Lee Valley Regional Park Authority	Agenda Item No:
LEE VALLEY REGIONAL PARK AUTHORITY	6
AUTHORITY MEETING	Report No:
20 OCTOBER 2022 AT 14:00	**A/4323/22**

BUSINESS CONTINUITY POLICY

Presented by the Corporate Director

SUMMARY

The purpose of this report is to seek Member approval for the Business Continuity Policy and associated procedures which has been created as a result of review of the Authority's Risk Management processes and procedures after the Risk Register Workshop held earlier in the year.

The Executive Committee considered the updated Business Continuity Policy/Procedures at a meeting held on 22 September 2022 (Paper E/773/22) and an oral update will be given at the Authority meeting.

RECOMMENDATION

Members Approve: (1) the Business Continuity Policy and associated procedures attached as Appendix A to Paper E/773/22 for adoption.

BACKGROUND

1 The Authority has a register of Policies that ensure the organisation works efficiently and consistently towards delivering its Business Strategy. As required, new policies are introduced to safeguard the Authority and make sure that all staff are conforming to current legislation and best practice.

2 Business Continuity management arrangements have been developed for implementation in a safe, prioritised and structured manner with the commitment of the Senior Management Team (SMT) for all of the services and sites within the Authority's control.

3 As part of a review of all processes involved with the management of risk and business continuity, a Business Continuity Policy has been written, along with accompanying procedures and guidance documentation.

BUSINESS CONTINUITY POLICY

4 The Executive Committee considered the Business Continuity Policy/Procedures at a meeting on 22 September 2022 (Paper E/773/22 – see

Annex A to this report) and an oral update will be given at the Authority meeting.

5 Any environmental, financial, human resource, legal and risk management implications are covered in paper E/773/22 attached as Annex A to this report.

Author: Vince Donaldson 01992 709 816, vdonaldson@leevalleypark.org.uk

PREVIOUS COMMITTEE REPORTS

Executive	E/773/22	Business Continuity Policy	22 September 2022

ANNEX ATTACHED

Annex A	Paper E/773/22

LIST OF ABBREVIATIONS

GLL	Greenwich Leisure Ltd. (trading as Better)

Lee Valley Regional Park Authority **LEE VALLEY REGIONAL PARK AUTHORITY** **EXECUTIVE COMMITTEE** **22 SEPTEMBER 2022 AT 10:30**	**Agenda Item No:** **Report No:** **E/773/22**

BUSINESS CONTINUITY POLICY

Presented by Corporate Director

EXECUTIVE SUMMARY

The purpose of this report is to seek Member approval for the draft Business Continuity Policy and associated procedures and the recommendation to the Authority for its adoption. The Policy has been created as a result of review of the Authority's Risk Management processes and procedures after the Risk Register workshop held earlier in the year.

RECOMMENDATION

Members Approve: (1) the recommendation of the draft Business Continuity Policy and associated procedures to the Authority for adoption.

BACKGROUND

1 The Authority has a register of Policies that ensure the organisation works efficiently and consistently towards delivering its Business Strategy. As required, new policies are introduced to safeguard the Authority and make sure that all staff are conforming within current legislation and best practice.

2 Business Continuity Management arrangements have been developed for implementation in a safe, prioritised and structured manner with the commitment of the Senior Management Team (SMT) for all of the services and sites within the Authority's control.

3 As part of a review of all processes involved with the management of risk and business continuity, a Business Continuity Policy has been written, along with accompanying procedures and guidance documentation.

BUSINESS CONTINUITY POLICY

4 A draft of the Business Continuity Policy is attached at Appendix A of this report for Members consideration and approval and the Business Continuity Plan Procedure, Risk Register Procedure and Business Continuity Risk Assessment are an annex to this policy.

5 The Business Continuity Policy is to set out the principles and practices that the Authority will adopt to meet with its legal obligations and its commitment to

ensure the safety of both customers and staff when within the Authority's Facilities or outside spaces and to ensure that, in the event of any business continuity incident, the initial response to a threat to the Authority's normal business is appropriate, robust and as coherent and effective as possible in the circumstances.

6 The aim of the proposed policy is to ensure that the Authority complies with the relevant legislation and that any associated procedures safeguard both customers and staff at all times with a business impact and disaster recovery process to be followed in the event of any incident.

ENVIRONMENTAL IMPLICATIONS

7 There are no environmental implications arising directly from the recommendations in this report.

FINANCIAL IMPLICATIONS

8 There are no financial implications arising directly out of the recommendations in this report.

HUMAN RESOURCE IMPLICATIONS

9 There are no human resource implications arising directly out of the recommendations in this report.

LEGAL IMPLICATIONS

10 There are no legal implications arising directly from the recommendations in this report.

RISK MANAGEMENT IMPLICATIONS

11 There will need to be regular training of relevant levels of staff in processes and monitoring as outlined within the attached procedures.

EQUALITIES IMPLICATIONS

12 There are no equalities implications arising directly from the recommendations in this report.

Author: Vince Donaldson, 01992 709 816, vdonaldson@leevalleypark.org.uk

APPENDICES ATTACHED

Appendix A	Business Continuity Policy
Appendix B	Business Continuity Plan Procedure
Appendix C	Risk Register Procedure
Appendix D	Business Continuity Risk Assessment

LIST OF ABBREVIATIONS

the Authority	Lee Valley Regional Park Authority
SMT	Senior Management Team

Lee Valley Regional Park Authority

Business Continuity Policy

September 2022

Reference: [Version 0.3]

This document is controlled by Lee Valley Regional Park Authority.

Lee Valley Regional Park Authority,
Myddelton House, Bulls Cross,
Enfield, Middlesex, EN2 9HG

This page is blank

i Document Information

Title: **Business Continuity Policy**

Status: Draft

Current Version: v0.3 (01 September 2022)

Author	Vince Donaldson – Senior Contracts and Quality Manager Sport and Leisure vdonaldson@leevalleypark.org.uk ☎ (01992) 709816
Sponsor	Dan Buck – Corporate Director (Sport and Leisure) Sport and Leisure Department dbuck@leevalleypark.org.uk ☎ (01992) 709896
Consultation:	Corporate Directors H&S Contractor Heads of Service Facility Managers Policy and Procedure Review Group
Approved	**Approved by:** XXXX **Approval Date:** XX September 2022 **Review Frequency:** Every Five Years **Next Review:** September 2027

Version History		
Version	**Date**	**Description**
0.1	22 July 2020	Initial draft, circulated to SMT, RDHS
0.2	3 September 2020	Revision after circulation to SMT, RDHS
0.3	1 September 2022	Further revision after commencement of Leisure Service Contract

II Contents

1. Introduction

1.1 Definition of Business Continuity Management

According to the Business Continuity Institute, business continuity management is "an holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities".

1.2 Business Continuity Policy - Operational

This policy ensures that the Authority's Business Continuity Management arrangements are developed and implemented in a safe, prioritised and structured manner with the commitment of the senior management team.

1.3 Business Continuity Objectives at LVRPA

The objectives of the Authority's business continuity policy are to ensure as far as practicable that:

- the initial response to a threat to the Authority's normal business is appropriate, robust and as coherent and effective as possible in the circumstances;
- the impacts of the threat are kept within acceptable levels as pre-defined by the relevant Corporate Directors and Senior Management Team (SMT) on initial threat analysis;

- in recovery to business as normal , priority is given to maintaining or restoring activities or services that are regarded as business critical in the circumstances; and
- relevant staff within the Authority are trained, advised and supported in order to achieve the above, in cooperation with others as appropriate; the process is not centrally directed

It is not an objective of business continuity planning within the Authority to ensure that, in the worst cases such as prolonged loss of use of an entire facility or service, full recovery to business as normal can be achieved quickly, or indeed in any particular timeframe. To guarantee any such recovery to any pre-determined specific deadline would be unrealistic and require prohibitively expensive resilience measures.

2. LVRPA Business Continuity Policy

2.1. It is the policy of LVRPA to:

- maintain a strategy for reacting to, and recovering from, adverse situations which is in line with an agreed level of acceptable risk
- ensure that, whenever practical, action is taken to prevent the occurrence or recurrence of an adverse situation through adopting appropriate risk controls
- maintain a programme of activity and services which ensures the Authority has the ability to react appropriately to, and recover from, adverse situations in line with predefined business continuity objectives
- maintain appropriate corporate and facility response plans underpinned by a clear escalation process
- rehearse response and recovery plans at least annually
- maintain a level of resilience to operational failure in line with the risks faced
- maintain employee awareness of the Authority's expectations of them during an emergency or business continuity threatening situation
- take account of changing business needs and ensure that the response plans and business continuity strategies are revised where necessary
- remain aligned with good industry practice in business continuity management

3. Scope of Business Continuity Planning

3.1 Business Continuity Planning at LVRPA concentrates on the following priorities:

- personal safety of all in Authority Facilities, Open Spaces and its Services.
- initial/emergency response
- communications
- safeguarding of assets
- recovery/continuity of key business activities
- recovery/continuity of revenue streams

4. Responsibility for Business Continuity

4.1 Responsibility for Business Continuity within the Authority is delegated by the Chief Executive to the Corporate Director (Sport and Leisure). This responsibility is in turn cascaded through the Authority's management structure and assured and overseen by the Business Continuity Planning Team. The Planning Team meets four times a year and is composed of;

Role	Responsible Officer
Planning Team Chair	Corporate Director (Sport & Leisure)
Co-ordination of open spaces and other facility requirements and group deputy	Corporate Director
Business Continuity Co-ordinator	Senior Contracts and Quality Manager
Co-ordination of IT requirements	Head of IT
Co-ordination of Special Project requirements	Head of Project and Funding Delivery
Co-ordination of Procurement	Senior Sport, Leisure and Projects Manager
Co-ordination of Communication requirements	Head of Communications
Co-ordination of Events	Senior Events Manager
Co-ordination of H & S requirements	H & S Contractor – Lead Officer
Co-ordination of APMD requirements	Head of Asset Maintenance
Co-ordination of Property requirements	Head of Property
Co-ordination of HR Training requirements	Head of HR

The Planning Team reports to the SMT.

4.2. Responsibility for localised business continuity matters and planning lies with the Heads of Service group incorporating heads of departments, the heads of divisions/service areas and this will feed into facility/service managers. The Facility/Service managers are accountable for the undertaking and implementation of business continuity measures in their areas. As a minimum the Authority expects each facility/service to have its own, fit for purpose, business continuity plan and for that plan to be reviewed and updated at least annually with sign off by the by the Business Continuity Planning team. Each business continuity plan must be submitted to the Business Continuity Co-ordinator annually for ratification by the Business Continuity Steering Group. Failure to comply at this level will be noted in the Authority's operational risk register.

5. Additional Roles & Responsibilities

5.1 The Roles and Responsibilities listed below will be revised annually to ensure that they fit the strategic objectives of the Authority.

Authority Members

- Understand and support awareness of business continuity;

- Support Authority staff with business continuity roles, within areas of responsibility, to demonstrate leadership and commitment;
- Ensure Corporate Directors and Heads of Service meet the business continuity targets;
- Discuss quarterly reports within Audit Committee meetings and act on any issues identified, as required.

Corporate Directors and Heads of Service

- If the department has experienced significant disruption due to a recent incident, discuss operational risk and business continuity in the senior management team/HoS meetings to identify controls and plans to mitigate disruption.
- Agree a primary and alternate business continuity champion, responsible for business continuity within their department as outlined in the Business Continuity Management Procedure.
- Ensure staff assigned the champion role complete their actions (Operational risk assessment, Business Impact Analysis, Business Continuity Plan development, exercises);
- Ensure the department has robust business continuity plan(s) which are signed-off;
- Ensure all members of the management team are aware of their responsibilities in each department's business continuity plan;
- Monitor results of plan reviews and exercises.

Business Continuity Champions

Under the guidance of the Business Continuity Co-Ordinator (through provision of templates and assistance with completion), the business continuity champions will over the course of the year complete and maintain the facility or service;

- Business Continuity Plan;
- Business Continuity Risk Assessment;
- Business Impact Analysis;
- Disaster Recovery Plan;
- Update the Call cascade outlined in the Facility Incident Management Plan;
- Plan exercise timetable with two exercises per year.

In addition:

- Respond to major operational incidents when required. This will involve the Corporate Director (Sport & Leisure) implementing a response structure to;
    - Bringing department situation reports to Business Continuity Steering Group meetings and implementing, communicating and coordinating updates to the facility or service Business Continuity Plan.
    - Attend quarterly meetings held by the Business Continuity Co-ordinator.
    - Generally raise awareness of business continuity in the department, including the department continuity plan and staff roles and responsibilities in the plan.

Business Continuity Co-ordinator

- Establish and maintain a business continuity management framework and agree business continuity champions for each department;
- Schedule and chair quarterly meetings with champions;
- Ensure the business continuity programme aligns with standards and best practice;
- Provide quarterly reports to the Corporate Director (Sport and Leisure) and the Audit Committee.

6. Management of Business Continuity

6.1. The following are the main processes and procedures through which the Authority implements its business continuity policy:

- Emergency Action Plans this is the first stage in the emergency response/business continuity process
- the Facility Incident Management Plans (FIMP) this is the next stage in the emergency response/business continuity process
- the Corporate Incident Management Plan (CIMP); this uses a command structure in line with that used by the emergency services following a Gold/Silver/Bronze hierarchy. Separate Event specific incident management plans will be specifically used during all events and link in with the CIMP.
- Business Continuity Plans for all facilities/services within the Authority, submitted for review yearly and tested regularly
- Annual Business Impact Analyses to help define recovery priorities for the Authority
- the Business Critical Calendar
- Authority-wide training and support facilitated by RDHS and HR (Authority Responsible Officer)

7. Business Continuity Framework

7.1 The standard management method Plan, Do, Check, Act (PDCA) used by organisations such as HSE will be applied to the design and implementation of the business continuity process.

Plan (establish)

- Documented business continuity policy, objectives, targets, controls, processes and procedures, relevant to improving business continuity in order to deliver results that align with the corporate strategy.

Do (implement and operate)

- Implementation of the policy, controls, processes and procedures through:
  - Documented business impact analysis and operational risk assessment;
  - Identification of appropriate business continuity strategies;
  - Establishing incident response structures and processes;
  - Documenting business continuity plans for key products and services and areas key to the delivery of the corporate strategy;
  - Implementation of exercises to validate the effectiveness of plans.

Check (monitor and review)

- Programme performance evaluation through methods of monitoring, measurement, analysis and evaluation of processes, including audits of plans and management reviews.

Act (maintain and improve)

- Implementation and follow-up of lessons learnt, as identified from incidents and exercises.
- Continual improvement through identification of nonconformity and corrective action plans.

8. Maintenance & Continual Improvement

8.1 In order to comply with the Business Continuity Framework, it is essential that both the Policy and Business Continuity Management Procedure are reviewed annually or after a major incident as defined in the Business Continuity Management Procedure.

Maintenance

Business continuity plans will go through a formal review at least once annually.
All facilities and services will be responsible for regularly updating their business continuity plans between reviews
All contact details held in the plans will be updated no less than once quarterly or on change of staff by the facility or service manager. *Contact details stored by departments for Business Continuity purposes must comply with data protection.*

Continual Improvement

To ensure continual improvement the Business Continuity Co-ordinator will:

- Ensure the business continuity programme achieves its intended outcomes, directing and supporting individuals as necessary.
- Ensure the resources needed are available (with support from the SMT where necessary).
- Follow-up recommendations from lessons learnt from exercises to ensure they are implemented.
- Ensure internal audits of the programme are conducted and the improvements identified are implemented.

8.2 Quarterly performance reports on the implementation of the business continuity programme and a summary of incidents will be collated by the Business Continuity Manager and provided to the Audit Committee so they are aware of any actions taken to improve resilience and reduce Corporate Risk.

9. Appendices

Appendix A – Supporting Document Index

APPENDIX A – SUPPORTING DOCUMENT INDEX

Document	Location	Version	Author
Emergency Action Plan Template	QMS System	9.0	Facility
Facility Incident Management Plan	QMS System	9.0	Facility
Facility Incident Response Flowchart	QMS System	9.0	H&S
Corporate Incident Management Plan	QMS System	7.0	H&S
Corporate Incident Response Reporting Flow Chart	QMS System	7.0	H&S
GLL and LVRPA Critical Incident Media Protocol	QMS System	1.0	H&S
Business Continuity Management	QMS System	2.0	Activation
Business Continuity Plan	QMS System	2.0	Activation
Business Continuity Risk Assessment	QMS System	2.0	Activation
Risk Register Procedure	QMS System	3.0	Activation

Lee Valley Regional Park Authority

Lee Valley Quality Management System Procedure

Detail

Procedure name:	Business Continuity Plan
Issue Number:	2
Date Created:	September 2020
Date updated:	September 2021
Review Date:	September 2023
Author (job title):	Senior Contracts and Quality Manager
Responsibilities:	A Business Continuity Planning Team has been established to deliver the objectives. This team will be responsible for establishing and supporting an on-going process to evaluate the impact of events that may adversely affect LVRPA, customers, assets or employees. The focus of the team is to assist Facility/Service managers develop and maintain a plan designed to ensure that the organisation as a whole and their facilities/service in particular, can restore business critical functions, and meet responsibilities to our customers and other stakeholders in a manner consistent with our recovery goals.

Contents

This procedure covers the following points:

Objective

It is the objective of Lee Valley Park Regional Authority to ensure that all facilities/services remain operational in the event of a major failure of areas/equipment, by means of a Business Continuity planning process.

Scope

The Business Continuity Planning Team will lead in identifying potential risks to Authority business and to the safety and well-being of our employees. Once risks are identified, the team will suggest and develop strategies that should minimise the impact the event may have on our operations both for facilities and services.

Business Continuity Plan Process

During the initial phased set up of any site and annually thereafter, the facility/service manager and their team, with support from the Business Continuity Planning Team, will analyse all processes that could affect the management and operational functions of the facility/service.

Once these items have been collated, the facility/service manager will then carry out the following processes;

1) Risk Assessment - The purpose of this assessment is to identify those events that have a higher likelihood (higher grade) of adversely impacting operations, so as to help prioritise the prevention and mitigation strategies.

2) Business Impact Analysis (BIA) – this will decide how quickly the function must be resumed before the facility/service is significantly impacted in terms of products, services, reputation and customer base.

3) Prevention/mitigation/recovery (Disaster Recovery Plan – DRP) – the facility/service manager can build an action plan to resume operations in the event of a business interruption and to set planning priorities based on how important these functions are to their operations based on their Business Impact Analysis.

4) Implementation, testing and exercises - To ensure that the recovery plan is effective after an event, periodic review coupled with testing is required. There are many types of tests that can be conducted to help ensure that the plan is adequate and these will be listed.

5) Training and education – with the assistance of the Business Continuity Planning Team, a training/education programme will be introduced ensuring a comprehensive and holistic approach for all staff to the Business Continuity process.

6) Testing and Exercises – The Authority will test the Business Continuity plans by means of tests (desktop) and exercises (real time) to ensure the plans are robust and have been updated, where necessary, to reduce risk, mitigate any further impacts on the business and confirm the disaster recovery process is fit for use. Tests will be conducted by external advisors, such as the Authority's Health and Safety support contractor or insurers.

Business Continuity programme schedule

	Estimated completion date	Planning team member/s responsible	Facility/Service
1) Risk Assessment	End December 2021	Vince Donaldson, Simon Clark, Jon Carney, Paul Roper	All
2) Business Impact Analysis	End January 2022	Vince Donaldson, Simon Clark, Dan Buck, Jon Carney	All
3) Prevention/Mitigation Disaster Recovery Plan	End January 2022	Vince Donaldson, Jack Bernard	All Authority
4) Implementation	End February 2022	All	All Authority
5) Training and Education	End February 2022	Vince Donaldson, Simon Clark, Jack Bernard	All Authority
Testing and exercises	End March 2022 then six monthly	Vince Donaldson, Jack Bernard	All Authority

Business Continuity Planning Team

The Business Continuity Planning Team for the Authority will meet on a quarterly basis to ensure that all processes required for Business Continuity are monitored to ensure they are updated as and when required.

The team will;

- Establish a work schedule and programme deadlines. Timelines can be modified as priorities become defined.

- Consider any specific budget requirements for research, documents, seminars, consulting services and other expenses that may be considered necessary during the plan development process.
- The Business Continuity Planning Team will be comprised of the following officers:

Name	Job Title	Specialism	Telephone	email
Dan Buck	Corporate Director	Sport and Leisure	01992 709896 07956 898619	dbuck@leevalleypark.org.uk
Jon Carney	Corporate Director	Open Spaces, Campsites, Marinas	01992 709804 07715 449325	jcarney@leevalleypark.org.uk
Vince Donaldson	Senior Contracts and Quality Manager	Quality Management Systemm	01992 709816 07920 495390	vdonaldson@leevalleypark.org.uk
Simon Clark	Head of IT	Information Technology	01992 709893 07734 021746	sclark@leevalleypark.org.uk
Paul Roper	Head of Project and Funding Delivery	Project management	01992 709845 07917 647552	proper@leevalleypark.org.uk
Justin Baker	Senior Sport, Leisure and Projects Manager	Procurement and project planning	01992 709938 07909 000302	jbaker@leevalleypark.org.uk
Stephen Bromberg	Head of Communications	Communications and PR	01992 709881 07793 773540	Sbromberg@leevalleypark.org.uk
Sophie Stone	Senior Events Manager	Events	01992 709913 07770 315973	sstone@leevalleypark.org.uk
Joe Ryan	Managing Director, RDHS Ltd.	Health and Safety	01458 241661 07919 214396	joe@rdhs-ltd.co.uk
Jack Bernard	Health and Event Safety Consultant, RDHS Ltd.	Health and Safety	01458 241661 07919 047389	jack@rdhs-ltd.co.uk
Michael Stevens	Head of Asset Maintenance	Asset Maintenance	01992 709861 07909 000320	mstevens@leevalleypark.org.uk
Marigold Wilberforce	Head of Property	Property and Allotments	01992 709883 07825 033510	mwilberforce@leevalleypark.org.uk
Victoria Yates	Head of HR	Human Resources	01992 709915 07739 852235	vyates@leevalleypark.org.uk
Alison Sackett	Management Support Officer	Administration	01992 709844 07920 825515	asackett@leevalleypark.org.uk

Business Continuity Champion

Each facility/service will nominate a Business Continuity Champion who will be responsible for the BCP, the BC Risk Assessment, Business Impact Analysis and Disaster Recovery Plan. This person will normally be the Facility/Service Managers who would be accountable for undertaking, implementing and ongoing training of staff in relation to Business Continuity measures.

Business Continuity Risk Assessment Process

Once all of the processes that could affect the management and operational functions of the facility/service have been collated, a Business Continuity Risk Assessment looking at the risk of specific items, implications of that risk, potential impact and risk mitigation will be completed and forwarded to the relevant Head of Service. This will be used to ensure that any high probability or high impact items are listed on the Authority's Risk Register and also the Asset Register for the facility/service. The Business Continuity Risk Assessment procedure will form

part of the Normal Operating Procedures for each facility/service which is a responsibility of the facility/service manager.

Specific Business Continuity Areas

The range of items for consideration will only be those which impinge directly on the ability of the site to provide the services/facilities required by both paying customers and staff. These will include areas such as:

IT – Hardware/Software failure, Data loss, phones etc.
Finance – ELMS (or replacement)/till failure, cash security, purchase orders
IM (Information Management) – Booking Systems, research
Health and Safety – Serious accident/incident, pandemic
Technical – Electrical failure, pump failure, contamination (chemical or bacteriological)

This list is not exhaustive and should be amended to meet the needs of each facility/service.

Updating the Business Continuity Plan

It will be the responsibility of the facility/site/service manager to update/review their Business Continuity Plan on an annual basis or as required. This will be the case where there have been changes to systems, equipment infrastructure etc. and will need to cover all changes to the current Business Continuity Risk Assessment that will be required to ensure continuity of the business of the site. Separate Business Continuity Risk Assessment and Business Impact Analysis procedures will be available with templates for completion by the facility/service manager.

Internal Forms

- SIP
- Asset Register
- Business Continuity Risk Assessment

External Forms

- N/A

Sources of Information

- Authority Risk Register
- LFA Targets

This page is blank

Lee Valley Regional Park Authority

Lee Valley Quality Management System Procedure

Detail

Procedure name:	Risk Register
Issue Number:	2
Date Created:	September 2020
Date updated:	April 2022
Review Date:	April 2024
Author (job title):	Senior Contracts and Quality Manager
Responsibilities:	In order to carry out these objectives the Business Continuity Co-ordinator assisted by all the Heads of Service will maintain and update the Authority's Risk Register along with any sub-Risk Register created to meet specific business risks and ensure they are regularly reviewed. The focus of these officers is to ensure that all foreseeable risks are fully considered and listed along with current controls and additional mitigations. For Risk Management to be an effective tool, it needs to be embedded throughout the organisation. It needs to be considered as part of the service planning process, as part of the budget setting process, as part of day to day decision making and as part of strategic level decision making by the Senior Management team and Members. It is also critical that management and Members are clear on the need to consider risks beyond their immediate operations, also focusing on risks in relation to partnerships with external bodies, risks in relation to projects and global risks both financial and medical, such as fuel shortages and pandemics. Organisation responsibilities are summarised as follows: • Members have overall responsibility for approving the Authority's Risk Management strategy and the content of the Risk Register. **They are not directly responsible for the management of risk, rather they must satisfy themselves that the Framework is operating effectively.** Specifically, they should be satisfied with the following: o the overall levels of Risk Appetite, o that all key risks have been identified within the Register on an ongoing basis, o that the inherent risk scores seem reasonable, o that the residual risk scores seem reasonable, given the existing controls identified and the potential causes of the risk, o that the decision as to whether to accept the residual risk score or to take further actions (including potentially terminating the operations relating to the risk) seems reasonable o that the deadlines set for any further actions seem reasonable, o that any further actions are being completed within the agreed deadlines and: o that the existing controls identified are indeed in place and continue to operate effectively – it is not for

Lee Valley Regional Park Authority

Risk Register
Issue 3

Members to check this for themselves, but to obtain assurances that this is the case (see Monitoring and Reporting below).

Contents

This procedure covers the following points:

Lee Valley Regional Park Authority

Risk Register
Issue 3

Objective

It is the objective of Lee Valley Regional Park Authority to record the details of all risks that have been identified along with their analysis and plans for how those risks will be treated. The Authority must remain functional in the event of any areas of business failure. All risks will be monitored by Authority officers and Members to ensure they are robust, updated and revised when required.

Scope

Risk Management applies to all aspects of the Authority's operations, including existing activities, those relating to planned developments and other risks that transpire due to unforeseen events such as national/international pandemics.

Risk is not just about the finances of the Authority. Whilst direct financial loss may result, the potential impacts if a risk is realised also include service disruption, reputational damage, environmental damage, personal injury, litigation and regulatory sanctions.

What Is the Purpose of a Risk Register?

The purpose of a risk register is to record the details of all risks that have been identified along with their current controls and plans for how those risks will be treated.
It takes the form of a spreadsheet that identifies:

- risks along with their severity;
- controls in place and the actions taken;
- steps to be taken to further mitigate the risk.

The risk register should be viewed by managers as a management tool for monitoring the risk management processes within the Authority. It is the responsibility of the Business Continuity Co-ordinator to ensure that the risk register is updated whenever necessary.

The list of risks that are identified and recorded in the Authority Corporate Risk Register are derived from the individual facility and service Risk Registers, however, generally only those risks that affect the Authority overall will sit within the Authority Corporate Risk Register.

Management of Risk

Management of risk is a constant ongoing process with the Business Continuity Co-ordinator/Heads of Service raising risks with the Corporate Directors who agree the necessity of adding the risk to the Authority Corporate Risk Register and identify actions that can be taken to mitigate the risk. To properly respond to a risk there may be a need to bring in experts to understand the actions that can be taken to reduce the likelihood of the risk occurring or the impact if the risk does occur.

The aim in general is to reduce risks to an acceptable level. There are times when the risk will remain "red". This is not a reflection that the risk is not being managed, more that SMT in conjunction with the Members feel that the risk has been controlled to the most acceptable level. It is not an efficient use of resources or practical for individual risks to be completely and

absolutely eliminated. A decision has to be made in each case as to what is a cost effective response, as set against the Authority's risk appetite.

If a decision is made to implement controls to help manage a risk, then the design of those controls needs to take account of the potential causes of the risk. It is only through taking action to control these causes that a risk can be managed.

How do we use Risk Management?

The Authority Risk Register and Sub-Registers are used for two main purposes:

- To determine those risks where further actions are needed in order to reduce the residual risk exposure to an acceptable level, i.e. within the Authority's risk appetite. These further actions need to be assigned responsible officers and deadlines for completion and progress towards implementing them needs to be monitored
- To determine those risks where the residual risk exposure has already been reduced to an acceptable level and hence where reliance is being placed on existing controls. Both SMT and Members need to be assured that these controls are operating as intended on an ongoing basis so as to confirm that the actual residual exposure remains at this level.

Both elements are of high importance and hence form the basis of the regular review by Management Team and Members. The Authority Corporate Risk Register and Sub-Registers will be an agenda item for each Heads of Service meeting and any changes are to be communicated by the chair to the Business Continuity Co-ordinator who will update the Authority Corporate Risk Register/Sub-Registers in question.

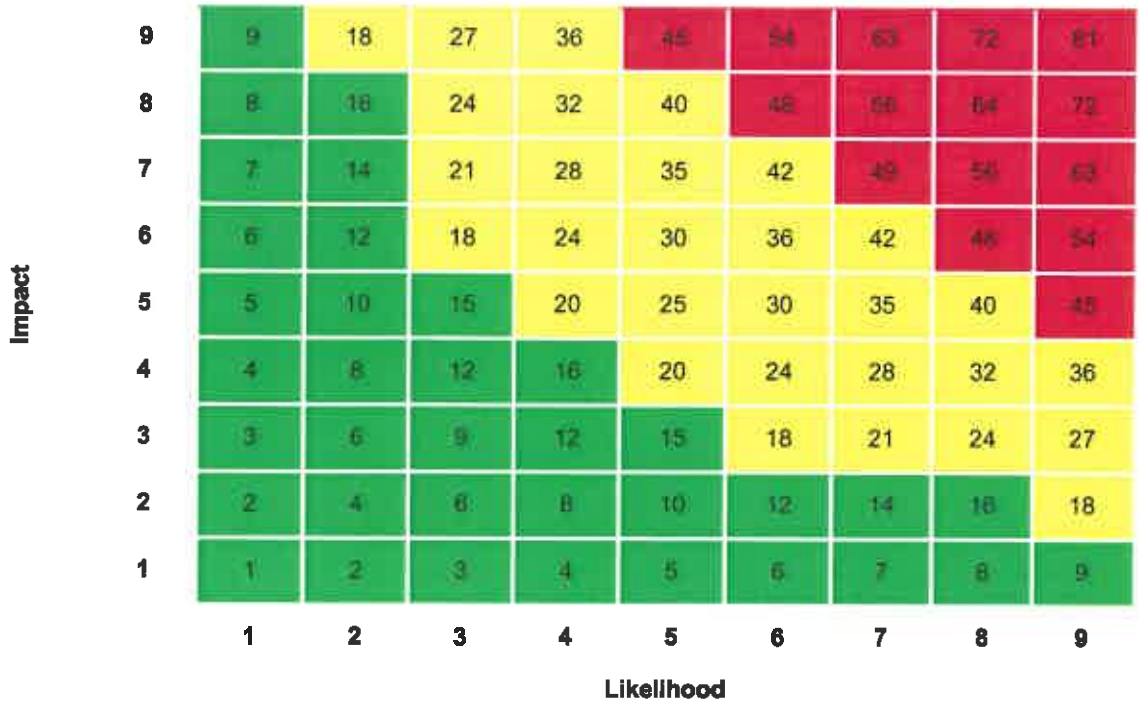
Risk Appetite

As it is not an efficient use of resources, nor is it necessarily practical for individual risks to be completely and absolutely eliminated, an important issue in considering the response to risk is the determination of the risk appetite of the Authority.

Risks are currently assessed using a 1-9 scale for both impact and likelihood. The Authority's risk appetite is then defined using the scoring matrix below.

Lee Valley Regional Park Authority

Risk Register
Issue 3



Those risks with a residual score in the green zone are generally considered to be managed to an acceptable level and hence limited or no further actions would be expected.

For those risks with a residual score in the amber zone, the exposure is considered to be partially acceptable. Further actions would be needed to lower this into the green zone, although a decision has to be made as to whether this is cost effective, given that resources are constrained.

Those risks with a residual score in the red zone are considered to have an exposure that is at an unacceptable level and hence further actions are needed to lower this.

On some occasions a decision may be made to accept a higher level of residual risk, although this will be subject to ongoing review and consideration at both Senior Management Team and Member level.

Scoring Criteria

Each risk is scored on the basis of the following criteria for impact and likelihood, both for inherent and residual risk. While the assessment remains subjective, these criteria serve as a guide and used to help ensure consistency in scoring against each of the risks identified.

	Impact	Likelihood
1	No impact	< 1% likely to occur in next 12 months
2	Financial loss up to £1,000 or no impact outside single objective or no adverse publicity	1% - 5% likely to occur in next 12 months
3	Financial loss between £1,000 and £5,000 or no impact outside single objective or no adverse publicity	5% - 10% likely to occur in next 12 months

4	Financial loss between £5,000 and £20,000 or minor regulatory consequence or some impact on other objectives	10% - 20% likely to occur in next 12 months
5	Financial loss between £20,000 and £50,000 or impact on other objectives or local adverse publicity or strong regulatory criticism	20% - 30% likely to occur in next 12 months
6	Financial loss between £50,000 to £250,000 or impact on many other processes or local adverse publicity or regulatory sanctions (such as intervention, public interest reports)	30% - 40% likely to occur in next 12 months
7	Financial loss between £250,000 to £500,000 or impact on strategic level objectives or national adverse publicity or strong regulatory sanctions	40% - 60% likely to occur in next 12 months
8	Financial loss between £500,000 to £1 million or impact on strategic level objectives or national adverse publicity or Central Government takes over administration	60% - 80% likely to occur in next 12 months
9	Financial loss above £1 million or major impact on strategic level objectives or closure/transfer of business	>80% likely to occur in next 12 months

Which Risks do we focus on?

All risks within the Authority Corporate Risk Register and Sub-Registers are focused upon, either because they have further actions against them to help lower the residual risk exposure, or because they are believed to be managed to an acceptable level of residual exposure and hence assurance is needed to confirm that this continues to be the case.

With regard to the initial inclusion of a risk on either the Authority Corporate Risk Register or any of the Sub-Registers, this is determined through the inherent risk assessment. If the inherent risk score falls within the green zone of the scoring matrix, then it will not be included as this suggests that the exposure is acceptable, even without taking any steps to manage it.

Risks will only be added to the Authority Corporate Risk Register if the inherent risk falls within the red zone or the amber zone.

How do we determine how to manage each Risk?

As noted above, it is not an efficient use of resources nor is it necessarily practical for individual risks to be completely and absolutely eliminated. A decision therefore has to be made in each case as to what is a cost effective response, as set against the Authority's risk appetite.

The response to each risk can be categorised into one of the following;

Treat	Controls are put in place to help reduce the likelihood of a risk being realised.
Transfer	Action is taken to transfer the potential impact to another party, e.g. through an insurance arrangement.

Terminate	A decision is made to end the area of activity with which the activity is associated.
Tolerate	A decision is made to accept the current level of exposure without taking any further action.

If a decision is made to implement controls to help manage a risk, then the design of those controls needs to take account of the potential causes of the risk. It is only through taking action to control these causes that a risk can be managed.

Different risks will have different causes and it is likely that there may be more than one potential cause per risk. However, the following categories are used as a guide to identify the causes in each case;

Lack of awareness/understanding of what's needed	Lack of resources/information needed to deliver	Lack of skills/competency needed to deliver
Errors in performance/compliance	Intentional non-compliance	Incompatible duties (lack of segregation)
Duplication of effort	Lack of awareness of poor performance/non-compliance	Lack of resource/competency to address issues

For each risk, the aim is also to have a mix of both preventative and detective controls. A preventative control seeks to stop the risk from being realised, whilst a detective control seeks to identify any instances where this does still occur. A balance is needed given that preventative controls may not always be successful.

How do we assess Residual Risk?

The residual risk exposure is assessed through a consideration of the extent to which the existing controls adequately mitigate the causes of each individual risk. A risk can only be managed through taking action to control the causes.

It is also important to recognise that the controls in place are generally focused more on reducing the likelihood of a risk occurring as opposed to the impact. In many cases, if the risk does still occur then the impact will be unchanged from the inherent scoring. There are exceptions to this, for example purchasing some form of insurance helps to reduce the potential impact rather than lowering the likelihood. In addition, in some cases, the controls may help to reduce the potential impact as well as the likelihood through a mix of both preventative and detective type controls.

What if the Residual Risk is not low enough?

The residual risk score is compared against the Risk Appetite to determine whether this is acceptable. As covered under the section titled 'Risk Appetite', if the score is outside the green zone then a decision needs to be made as to how to address this. Such a decision will be based on the specific nature and potential impacts of the risk in question, as well as the costs and practicalities involved with managing it.

The decision will be to 'Tolerate' the existing level of exposure, to 'Treat' it, or to 'Terminate' it through ending the operations to which the risk relates. If a decision is made to 'Treat' the

residual exposure, the further action(s) will be identified to do so. For each further action, a deadline for completion and a responsible officer are agreed.

Once completed the existing controls recorded in the Authority Risk Register are updated to reflect the strengthening of the control environment and the residual risk score is re-assessed.

How does the Risk Register fit within the Business Continuity Process?

The facility/service manager will carry out the following processes;

1) Risk Assessment Process and Regular Review of Risk Register - The purpose of this assessment is to help them identify those events that have a higher likelihood (higher score) of adversely impacting their specific operations so as to help them prioritise their prevention and mitigation strategies. Any significant risk that could affect the Authority overall and not just their specific operations will be added to the Authority Corporate Risk Register.

2) Business Impact Analysis (BIA) – this will help decide how quickly the function must be resumed before the facility/service is significantly impacted in terms of products, services, reputation and customer base.

3) Prevention/mitigation – the facility/service manager can build an action plan to help resume operations in the event of a business interruption and to set planning priorities based on how important these functions are to their operations based on their Business Impact Analysis. This will take the form of a Disaster Recovery Plan to ensure that their aspect of the Authority's function can return to normal operation in the earliest possible time taking costs into consideration.

These are discussed with the Head of Service and those items that are of a sufficiently high level of risk to the Authority as a whole are added to the Risk Register.

Lee Valley Regional Park Authority

Monitoring, Updating and Reporting the Authority Corporate Risk Register – Internal Process

Risk management needs to be consistently on the 'agenda' at all levels and the Authority Corporate Risk Register and Sub-Registers need to be treated as 'live' documents. The Authority Corporate Risk Register is reviewed quarterly by the SMT and is an agenda item for the Heads of Service meetings which take place on a monthly basis. The Sub-Registers are also subject to review by the SMT/HoS. The Authority Corporate Risk Register and any Sub-Registers are reviewed by the Audit Committee (Members) at their meetings on a minimum of three occasions annually.

Key elements covered by the review process as linked to the responsibilities include the following:

- consideration as to whether there are any new or emerging risks to be added to the Authority Corporate Risk Register;
- consideration as to whether the significance of any existing risks has changed;
- consideration as to whether a risk is no longer relevant/of concern and should be removed from the Authority Corporate Risk Register;
- monitoring and reporting on the extent to which the controls currently in place are adequately and effectively managing the risks identified;
- determining the extent to which any future actions are needed to strengthen the existing controls; and
- monitoring the progress on the implementation of further actions.

The Business Continuity Co-ordinator will ensure that the Authority Corporate Risk Register is updated quarterly in conjunction with the SMT and will supply the HoS chair copies of the current Authority Corporate Risk Register for them to discuss and, if required update at their monthly meetings.

Any emerging risks that need to be added to the Authority Corporate Risk Register should be confirmed by the relevant lead and communicated to the Business Continuity Co-ordinator who will add these within the relevant section of either the Authority Corporate Risk Register or any sub-register.

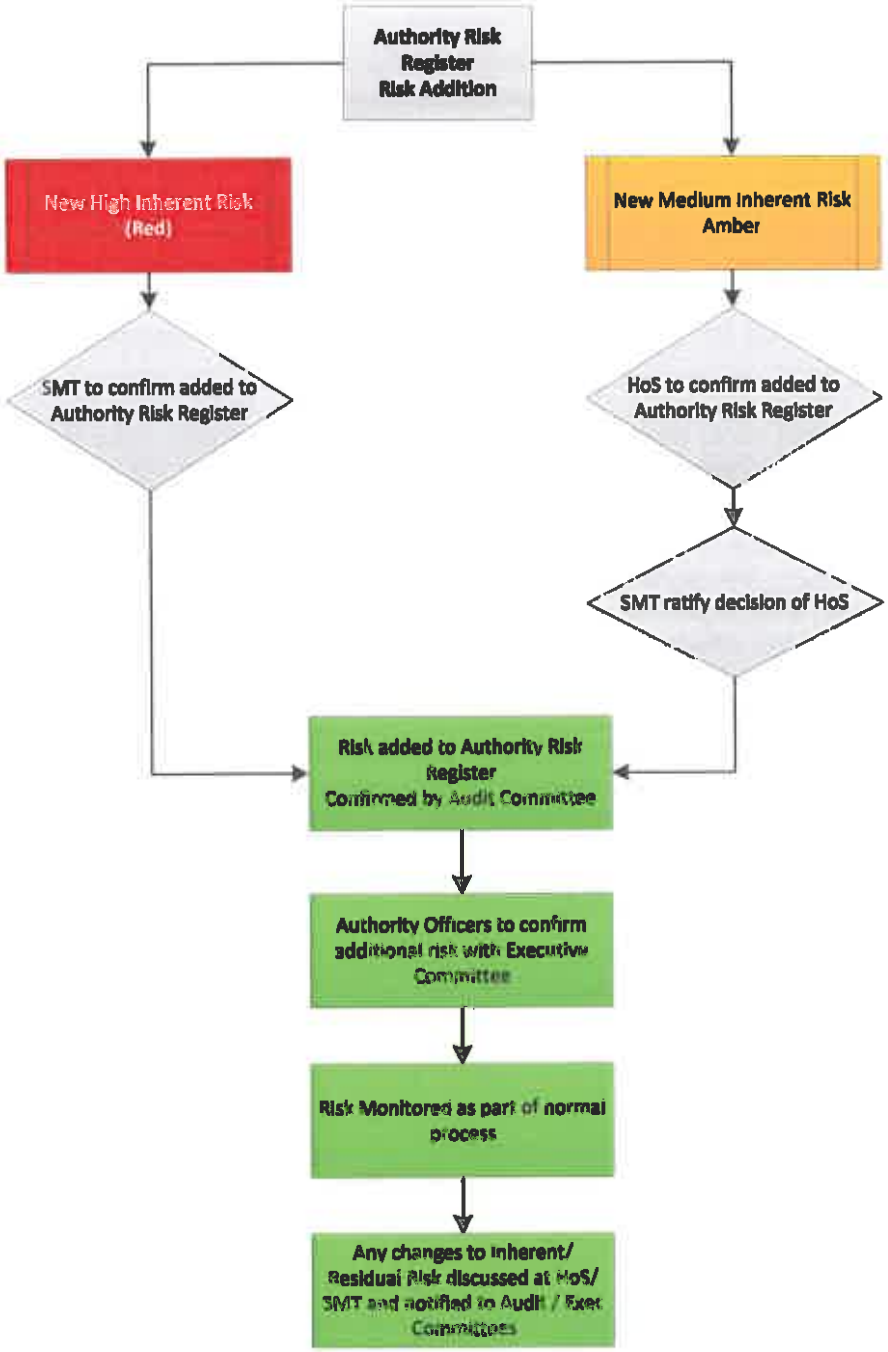
Any risks that increase in severity from amber to red should be confirmed by the relevant lead and communicated to the Business Continuity Co-ordinator. These would be flagged up at the next available Executive Committee meeting by Authority Officers, with the chair of the Audit Committee present and Audit Committee Members copied in.

Any risks that have become no longer relevant due to changes in conditions or removal of the specific risk (e.g. due to the end of a process such as procuring a large contract) can be removed at the instigation of the risk lead if the Inherent risk is now within the green zone.

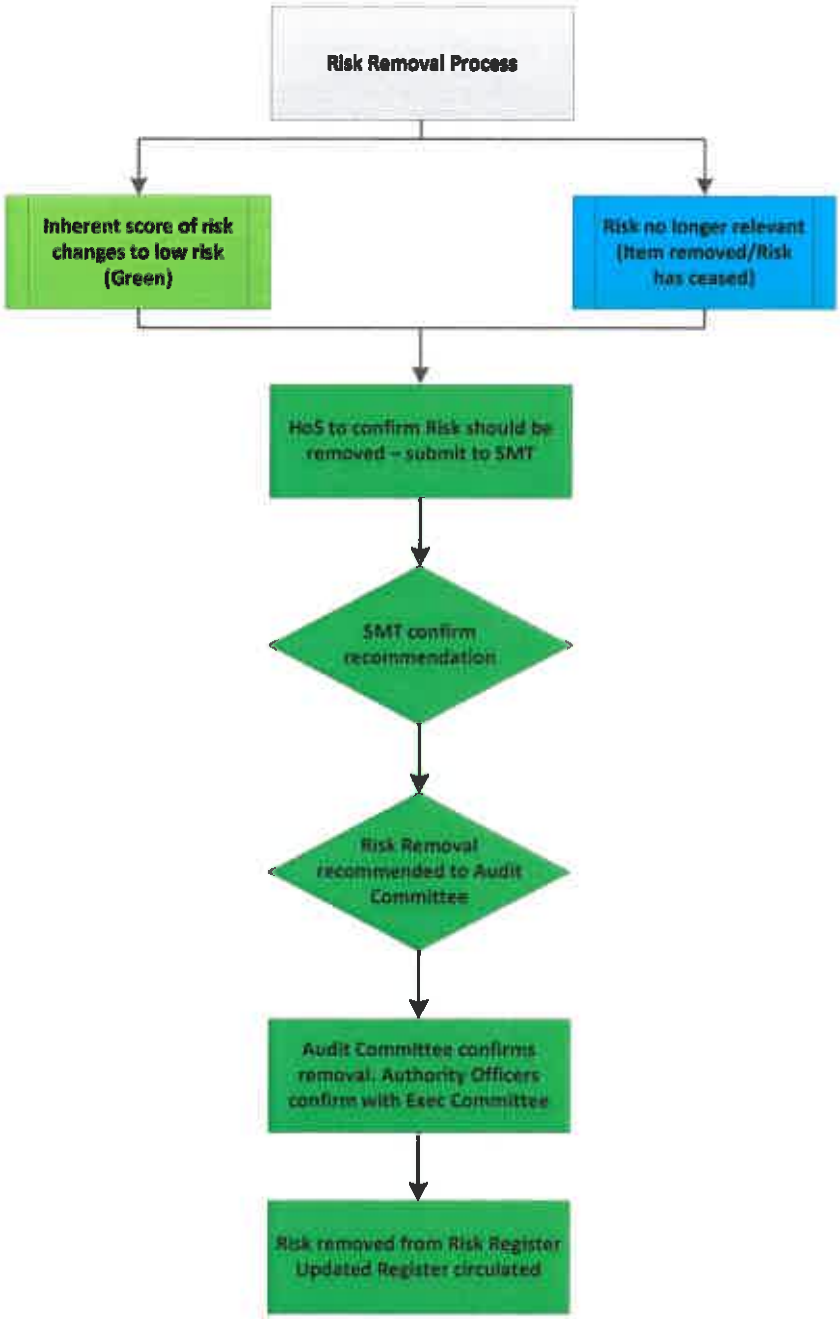
Lee Valley Regional Park Authority

Risk Register
Issue 3

Risk Addition Flowchart



Risk Removal Flowchart



Reviewing, Reporting and Updating the Authority Corporate Risk Register – Member Committees

It will be the responsibility of the Audit Committee to review the Authority Corporate Risk Register (and any sub-Risk Registers) at their programmed meetings. On completion of the meeting, the Audit Committee will recommend to the Executive Committee any changes or areas of medium to high risk that are of concern. The relevant Authority Officers (supported by

the Chair of the Audit Committee) will present these areas within a report to enable the Executive Committee to understand the ramifications of any areas of concern and enable them to assume ownership of the risks.

Once the Executive Committee have agreed the status of the risks, a report will be taken to the next full Authority Meeting for information/awareness.

In the event of any additional risks that emerge in the interim or changes to the severity of the risk, the Authority Corporate Risk Register will be amended. These amendments would be flagged up at the next available Executive Committee meeting by Authority Officers with the chair of the Audit Committee present and Audit Committee Members copied in for information. Once the Executive Committee have agreed the addition, this confirmation will be forwarded to the Audit Committee for ratification of the amended Risk Register.

Internal Forms

- Service Improvement Plan (SIP)
- Asset Register
- Facility/Service Specific Risk Register
- Business Continuity Risk Assessment
- Business Impact Analysis Template
- Disaster Recovery Plan Template

External Forms

- N/A

Sources of Information

- Authority Risk Register
- LFA Targets

Lee Valley Regional Park Authority

Business Continuity Risk Assessment

Issue 2

Objective

It is the objective of Lee Valley Park Regional Authority to ensure that all facilities open to the public and other users are managed to ensure they remain operational despite failure of areas/equipment.

Responsibilities

It is the responsibility of the (Facility/Service) manager to ensure that a Business Continuity Risk Assessment (BCRA) process is followed and that the assessment for the Facility is completed and forwarded to their relevant Head of Service for inclusion in the overall BCRA and Risk Register. This Risk Assessment will form part of the Business Continuity Plan for the facility/service.

Scope

This procedure covers the production of the Business Continuity Risk Assessment and the range of requirements for the site in operational state.

This procedure covers the following points:

Lee Valley Regional Park Authority

Business Continuity Risk Assessment

Issue 2

Detail

Business Continuity Risk Assessment Process

During the initial phased set up of any site and annually thereafter, the site manager, their team and support staff from head office will analyse all processes that could affect the management and operational functions of the site.

Once these items have been collated, a Business Continuity Risk Assessment (BCRA) looking at the risk of specific items, implications of that risk, potential impact and risk mitigation will be completed and forwarded to their Head of Service. This will be used to ensure that any high probability or high impact items are listed on the Risk Register and also the Asset Register for the facility. The Business Continuity Risk Assessment procedure will form part of the Normal Operating Procedures for each facility/service.

An example assessment of risk based on event type begins on page 8. The purpose of this assessment is to help officers identify those events that have a higher likelihood of adversely impacting their operations so as to help them prioritise their prevention and mitigation strategies. With the impact of the Covid-19 pandemic, officers should ensure they factor in all the additional assessments this has generated for their facility/service.

Department
In the first column of the form, list the department the Risk Assessment applies to.

Risk Area
This column covers the specific areas of risk within the department. These areas can be greater or lesser dependant on the department they apply to and is for the specific risks to be outlined which could affect the facility and the community.

Inherent Risk Score
In these columns list the impact and likelihood (both on a scale of 1 to 9). Potential risk events to consider include, but are not limited to, those listed below and how likely they are to happen, combined with what the impact could be:

Natural hazards	Man-made events	Technology-caused events
Tornadoes/Hurricanes Floods Earthquakes Lightning Snow, ice, hail Landslides Wildfires Biological (pandemic viral	Explosion/fire Transportation accidents Vandalism Terrorism/bomb threats Industrial accidents Financial	Computer systems failures/compromise Electronic data loss/corruption Software or application corruption Ancillary support equipment breakdown Telecoms/internet disruptions

Lee Valley Regional Park Authority

Business Continuity Risk Assessment

Issue 2

infections)		Energy/power/utility failures/outages

This list is not exhaustive and should be amended to meet the needs of each facility/service.

Lead

This is to indicate the relevant lead officer responsible for the Facility/Service and who will normally be the person completing the Risk Assessment.

Impact

In the Impact column, rate how each event's impact on the business/staff/customers. Facilities/services should consider the human, property, operations and environmental impact of any event. These are scored on a scale of 1 to 9 and should consider both internal and external resources.

Impacted area	Comments and considerations
Human impact	Analyse the possibility of death or injury. Consider the need for staff to work from home if self-isolating from a pandemic and their mental health.
Property impact	Consider the potential for loss or damage to property. Property includes buildings, machinery, equipment, electronic equipment, raw materials and finished products/goods. Considerations include: Cost to replace Cost to set up temporary replacement Cost to clean or repair Cost for additional safeguards (screens, signage etc.)
Operations impact	Consider the potential loss of market share factoring in areas such as; Business interruption Employees unable to report to work Customers unable to reach the facility Closure of the facility due to government edict Interruption of critical supplies Interruption of product distribution Company's potential breach or violation of contractual agreements Imposition of fines, penalties or legal costs
Environmental impact	Considerations include: Chemical or hazardous materials spill Damage to water resources Air pollution Ground contamination

Lee Valley Regional Park Authority

Business Continuity Risk Assessment

Issue 2

Likelihood
This is how likely such an event may happen. Also scored on a scale of 1 to 9 , in combination with the Impact, this will create the Inherent Risk Score.

Existing Controls
Assess the controls currently in place to manage these risks.

Residual Risk Score
In these columns again list the impact and likelihood (both on a scale of 1 to 9). However, these scores may be lower that the inherent risk score due to additional risk mitigations put in place to reduce the risk.

Source of Assurance
This will be the department/team/officer that will supply the necessary support/back up to ensure that any additional controls required can be put in place and monitored.

Impact
In the Impact column, rate how each event's impact on the business/staff/customers after mitigation/additional controls are put in place. These are scored on a scale of 1 to 9 and should consider both internal and external resources.

Likelihood
This is how likely such an event may happen after mitigation/additional controls are put in place. Also scored on a scale of 1 to 9, in combination with the Impact, this will create the Residual Risk Score.

For each of the risks the response in the column 'Treat, Transfer, Terminate, Tolerate' can be categorised into one of the following;

Treat	Controls are put in place to help reduce the likelihood of a risk being realised.
Transfer	Action is taken to transfer the potential impact to another party, e.g. through an insurance arrangement.
Terminate	A decision is made to end the area of activity with which the activity is associated.
Tolerate	A decision is made to accept the current level of exposure without taking any further action.

Further actions needed to reduce Risk
This column is used to add in the additional mitigation/control measures that can reduce the Residual Risk Score.

Lee Valley Regional Park Authority

Business Continuity Risk Assessment

Issue 2

Deadline for completion of actions
This column is used to note the deadline that the further actions must be completed/checked by to ensure the Residual Risk Scored is maintained or improved.

Officers Responsible
This will normally be the Facility/Service manager unless any specific actions require this to be another HoS.

Comments
This column is for any additional comments that may be pertinent to the specific risk e.g. a temporary situation that has a limited time scope.

Internal/External Resources
When reviewing each risk, officers should factor in both internal and external resources when considering how each risk can be managed.

Internal resources
Assess the facility/services ability to respond to the event based on internal resources. Consider each potential event from beginning to end and each resource that would be needed to respond. For each event, ask "Do we have the required resources and capabilities to respond?"

External resources
Similarly, assess the facility/services ability to respond to the event based on external resources. Consider each potential event from beginning to end and each resource that would be needed to respond. For each event, ask "Will external resources be able to respond to this event as quickly as we may need them, or will they have other response priorities?"

Risk Mitigation
Finally, evaluating the impacts of the hazards and comparing the probability, document if there are adequate strategies to prevent the hazard from occurring or if there are strategies in place to mitigate the impacts from the hazard. For example, you may need to:

- Develop additional emergency procedures
- Conduct additional training
- Acquire additional equipment
- Establish mutual aid agreements
- Establish agreements with specialised contractors

Example Risks and Mitigations

Department	Risk	Potential Impact	Risk Mitigation	Additional Requirements/Comments
Finance/IT	Booking system Failure – unable to process	Loss of trade, PR fallout, loss of return business, loss of income	Back up sheets printed, manual till operation	Reserve till to be purchased. Officers to confirm vendors have placed print option on system and arranged training for managers on print outs

Lee Valley Regional Park Authority

Business Continuity Risk Assessment

Issue 2

	bookings			
Finance	Security Firm does not attend to collect banking	Safe limits exceeded – insurance risk	Emergency call out numbers for Security firm.	Look at limits for all safes, purchase an additional 'day' safe. Safe make and model to be sent to Finance for Insurers to agree safe limits
Finance	Chip & Pin machine failure	Loss of income, loss of trade	Take cash only?	Knowledge of local cash machines in the area. Direct customers to online booking system
Finance	Finance	Failure of Purchase Order System	Inability to order stock, consumables, loss of income	Site manager to have use of authority credit card
IT	Booking System Failure	Loss of trade, PR fallout, loss of return business, loss of income	List of call out numbers available for vendor/IT support, system reboot procedures in place.	IT support available for non-IT staff to ensure they can be talked through system re-boot if required.
IT	Phone system fails	Loss of trade, PR fallout, loss of return business, loss of income	IT to supply BT emergency contact details, system engineer details	Consider backup issuing a mobile number on website that can be available in emergency
Health and Safety	Serious Incident or Accident	PR fallout, legal issues, insurance costs	Emergency Action Plan in place, Risk Assessments completed, staff training records. Accident/Incident forms. Contact details listed as per FIMP – copy kept in Incident Management Pack at reception along with other places as listed on FIMP	Accidents/Incidents reported as per 'Accident/Incident Reporting Procedure on LVQMS, Serious Incidents reported/dealt with as per Facility Incident Management Plan procedure on LVQMS (FIMP)
Health and Safety	Pandemic or other contagious illness reducing staffing levels	Loss of site cover, inability to safely staff site, inability to offer booked or other facilities	Use of large pool of 'Casual' employees for customer critical operations, multi trained staff available from other sites	Need to increase levels of staff trained in ELMS for reception cover. 'Pandemic Viral or Infectious Disease Planning' procedure available on LVQMS when required

Updating the Business Continuity Risk Assessment

It will be the responsibility of the facility/site manager to update/review the Business Continuity Risk Assessment on an annual basis or as required. This will be in the case where there have been changes to systems, equipment infrastructure etc. and will need to cover all changes to

the current Business Continuity Risk Assessment that will be required to ensure continuity of the business of the site. The Business Continuity Risk Assessment will be fully re-assessed every two years.

Review

September 2022

Site Specific Forms

- SIP
- Asset Register
- Business Continuity Risk Assessment

Sources of Information/External forms

- Authority Risk Register
- LFA Targets

Changes from Last Issue

Responsibilities, Scope and Detail all revised

Lee Valley Regional Park Authority

Business Continuity Risk Assessment

Issue 2

Appendix A: Business Continuity for IT (Example RA)

September 2020

RISK REGISTER Section: ICT Date: Updated 15 Jan 2022

Ref	Risk	Dept	Inherent Risk Score: Impact	Likelihood	Total Score		Existing Controls	Source of Assurance	Residual Risk Score: Impact	Likelihood	Total Score		Progress	Action	Further Actions Needed to reduce Risk	Deadline for Completion Actions	Officer(s) Responsible	Comments (Date)
ICT1	Server Failure (Core Systems)	IT Dept	9	4	36	36	All local App servers are backed up to a backup server; which is replicated to another server off site (Currently at VeloPark). Majority of systems have been moved to SAS; which are hosted externally. Vendors provide backups as part of SAS contract	Head of IT	7	2	14	14	>	Tolerate	Back up Data as per 'Backup Procedure' on LVQMS. Ensure that there is a 'backup' schedule as part of any SAS contract	Annual Check Whenever contract is started or renewed		eFin (Finance system), is in need of replacing. New system due to be procured, which should be a SAS system.
ICT2	Server Failure (Data Servers)	IT Dept	9	4	36	36	All data is backed up to a backup server; which is replicated to another server off site (Currently at VeloPark).	Head of IT	7	2	14	14	<>	Tolerate	Back up Data as per 'Backup Procedure' on LVQMS.	Annual Check		Backup servers being moved from VeloPark to a data centre in Hoddesdon as GLL will be taking over VeloPark.
ICT3	Core System failure - Booking systems	IT Dept	9	4	36	36	Different systems are used across the Authority, meaning that a failure of one system, would not result in a total loss SLA's in place with vendors	Head of IT	9	2	18	18	<>	Tolerate	Cash only transactions to be made Venues have an 'Offline' procedure in place Transactions can still be taken via the website or at another venue	Annually		
ICT4	Core System provider stops trading or goes into administration	IT Dept	9	2	18	18	Trading history checked during procurement process	Head of Finance	9	1	9	9	<>	Tolerate	Regular contractor meetings with vendors	Quarterly		
ICT5	Intranet Failure	IT Dept	5	4	20	20	IT support, system reboot procedures in place.	Head of IT	5	2	10	10	-	Tolerate	Print hard copy of LVQMS and other vital documents. Look at other ways of providing an Intranet i.e. Office 365	Quarterly		There is a hard copy of the LVQMS file on site. Documents are also saved on LV Servers.
ICT6	Data Loss through Theft or malicious intent to destroy. Data loss through lack of in house knowledge or skills in order to access databases	IT Dept	9	2	18	18	All data is backed up to a backup server; which is replicated to another server off site (Currently at VeloPark). Staff are asked to complete a DBS check before appointed Authority has Information Officer Micrsoft databases are no longer to be used for storing data	Head of IT	9	2	18	18	<>	Tolerate	Staff put on Garden leave if they are leaving under duress Remove access rights if under investigation or on garden leave Take equipment from staff that are on garden leave Public to be informed of any data breech All customer data stored on MS Access to be moved to CRM system	Monthly		Policy may be needed to address this. Potential DP risk if data is stolen
ICT7	Data Breach through cyber attack or malicious intent	IT Dept	9	5	45	45	Authority has Information Officer Access to data is restricted to authorised staff Access to CRM system restricted Firewalls in place Anti-Virus installed on all Authority computers Firewalls in place at edge of network Mimecast Email filtering in place to block threats via email	Head of IT	9	3	27	27	<>	Tolerate	Public to be informed of any data breech CRM system to be replaced as current one is over complex for Authority needs There is a lack of in-house knowlegde of the system. Further training is required on CRM	Monthly		New CRM system that matches business requirements needs to be procurred Staff across organisation need to be trained
ICT8	Cyber Attack	IT Dept	9	5	45	45	Anti-Virus installed on all Authority computers Firewalls in place at edge of network Mimecast Email filtering in place to block threats via email Patch management Cyber training provided by IT every six months IT Usage Policy and procedures No unauthorised devices allowd on network External Audits Default passwords changed Users do not admin rights IT supplied call out numbers	Head of IT	7	5	35	35	<>	Treat	Prevent personal email accounts from being accessed on Authority devices. Implement Two Factor Athentication. Ensure software updates are rolled out and installed. Stop staff from connecting own devices onto network. Stop use of out of date software such as old versions of Java required for eFin to work	Quarterly		Cyber-attacks are unpredicatable and the main risk is staff accidently or purposely initiating an attack
ICT9	Photocopiers failure	IT Dept	8	5	40	40	IT supplied call out numbers, sufficient forms printed out, some venues have multiple MFD's, print to another MFD an next nearest venue and collect	Head of IT	6	2	12	12	<>	Tolerate	Site staff to list relevant forms that are vital to ensure sufficient printed out. Print off blank forms as a back-up.	Quarterly		Some MFD's are with a different provider in preperation for transfer to GLL. Surplus MFD's if venues are outsourced i.e Hayes Hill Farm, as under contract until 2022. Will relocate or try to novate to new operator
ICT10	Phone system fails (Hardware)	IT Dept	8	5	40	40	List of call out numbers available for IT, support contract in place	Head of IT	5	3	15	15	<>	Tolerate	Phones can be diverted to mobiles by IT department.	Quarterly		Migrate all numbers to SIP; which gives extra level of resiliance on phones
ICT11	Telecomunications Failure (Daisy / BT Infrastructure)	IT Dept	8	4	32	32	IT to supply emergency contact details of telecoms providers (Daisy, Voiceflex and Zen). Support levels in place on lines, with important lines having higher level of support than others	Head of IT	6	2	12	12	<>	Tolerate	Type of cover means there is a 48 hour response time from service provider. Phones can be diverted to mobiles by provider, but there is a delay in the service going live of upto 24 hours	Six monthly Check		Migrate all numbers to SIP; which gives extra level of resiliance on phones
ICT12	MPLS Circuits Failure	IT Dept	8	4	32	32	IT to supply emergency contact details of telecoms provider (GTT). SLA on circuits Velo, HTC, WWC and MH have backup circuits	Head of IT	5	3	15	15	<>	Tolerate	4G Wi-Fi hotspots to be used as a back-up. ADSL used for public Wi-Fi to be used until main circuit is restored	Six monthly Check		
ICT13	User account locks out	IT Dept	8	6	48	48	IT supplied call out numbers	Head of IT	6	3	18	18	<>	Tolerate	Accounts can be unlocked remotely by any Member of the IT department	Quarterly		IT Staff must have a mobile phone that can handle the software to do this remotely. Phones are generally high spec and cost more then standard phones issued to staff

ICT14	Hardware is not maintained or replaced when becomes end of life or is no longer supported	IT Dept	8	4	32	32	Capital budget Rolling replacement of computers IT monitoring and repalcement of equipment	Head of IT	7	3	21	21	<>	Tolerate	Computers currently being replaced to keep equipment working Some hardware being replaced Quantity of equipment issued to staff to be reduced to reduce overheads of replacements	Annually		Hardware upgrades will be going to GLL. Do not want to pay for new hardware and then give it away to GLL. Sometimes hardware upgrades are enforced by vendors i.e. Apple stop support of
ICT15	Website not working meaning customers cannot book online	IT Dept	9	2	18	18	Staff training on how to use CMS Restricated access to CMS	Head of IT	8	2	16	16	<>	Tolerate	Website is built on a hosted CMS with a vendor who's reputation relies on it being up 99.99% of time	Annually		
ICT16	Public Wi-Fi not woking or used to access illicit data	IT Dept	5	5	25	25	SLA in place with supplier of Wi-Fi Filters applied to prevent accessing illicit data EUA in place that has to be agreed to before being used	Head of IT	5	5	25	25	<	Treat	Upgrading bandwith for campsites	Mar-21		Wi-fi equipment is now almost 10 years old and needs to be upgraded in order to guarantee good customer experience Will require capital budget to do this. Do we only do Non LSC venues
ICT17	Loss of Hardware due to theft, being lost or damaged or not returned when staff leave	IT Dept	6	6	36	36	Hardware is security marked IT Policy states not to leave equipment unattended CCTV at venues IT has an inventory of equipment	Head of IT	6	6	36	36	<>	Tolerate	Purchase MDM platform to disible stolen or lost phones Install tracking software on Laptops Staff should be accountable for any loss or damage Final salary to be deducted for any equipment not returned or has been returned in a damaged state	Annually		An MDM will require a budget Tracking software requires a budget and will become invalid if Hard Drive is removed IT Budgets should be centralised to prevent unauthroised purchase of replacement equipment and to prevent equipment being bought to use up budget at end of financial year
	Financial Management																		
ICT18	Core System failure – eFin (Financial System). eFin system is currently end of life and no longer supported by Vendor	Hoff	9	7	63	63	System is backed up, but uses an old version of Windows and is on an old server Spacial support purchased from vendor for support until system can be upgraded	Head of IT	9	5	45	45	>	Treat	Procurement or upgrade Finance system to a SAS system or at minimum one that can run on a virtual server	01/12/2021	Keith Kellard Simon Clark	eFin (Finance system), is in need of replacing. New system due to be procurred, which should be a SAS system. EFin requires old and unsecure version of Java to run Efin will only run on Server 2008; which is no longer supported by Microsoft Efin is on a server that is out of warranty and is very old
ICT19	Failure of Purchase Order System	Facility Manager	9	4	36	36	Finance supplied call out number	HoF	8	2	16	16	<>	Tolerate	Site manager to have use of Authority credit card	Quarterly	DCEO/ HoF	Other problems covered in 'Cash Handling and Financial Admin' on LVQMS
	Health and Safety																		
ICT20	Serious Incident or Accident	Facility Manager	9	5	45	45	Emergency Action Plan in place, Risk Assessments completed, staff training records. Accident/incident forms. Contact details listed as per FIMP – copy kept in Incident Management file	H&S Contract Lead	8	4	32	32	<>	Tolerate	Accidents/Incidents reported as per 'Accident/Incident Reporting Procedure on LVQMS. 24hr phone/email support available from RDHS.	Six monthly Check		Serious incidents reported/dealt with as per Facility Incident Management Procedure on LVQMS (FIMP)
ICT21	Pandemic or illness causes department to be absent	HoIT	9	5	45	45	Staff follow government guidelines when in Pandemic Avoid where possible, team being in same place at same time Policies and procedures in place Support contract in place with support company	Head of IT	9	4	36	36	<>	Tolerate	iQual have knowledge and experience of Authority systems and could provide interim support	Six monthly Check		
	Site Technical Risk Assessment																		
ICT22	Power Failure at Mydd House	HoIT	9	5	45	45	IT supplied call out numbers in case equipment does not reboot MH has been setup to be able to be connected to a generator in event of prolonged power failure	Head of APMD	8	4	32	32	<>	Tolerate	All equipment should reboot once power is restored. APMD to have a list of companies that can provide generators	Six monthly Check		If equipment is damaged, it will need to be replaced, which will take 3-5 working days.
ICT23	Power Failure at Venue	Facility Manager	9	5	45	45	IT supplied call out numbers in case equipment does not reboot UPS at venues, but have limited 'uptime' Batteries backup at Velo (where backup servers are) are expensive to replace	Head of IT	8	4	32	32	<>	Tolerate	All equipment should reboot once power is restored. APMD to have a list of companies that can provide generators	Six monthly Check		If equipment is damaged, it will need to be replaced, which will take 3-5 working days. Backup and data servers being moved to data centre
ICT24	Power Failure at Data centre	IT Dept	9	5	45	45	IT supplied call out numbers in case equipment does not reboot UPS at Data centre Network will go down until power is restored Backup of the backup will restart once power is restored Some folders stored on Data server will be inaccessable until power is restored	Head of IT	8	4	32	32	<>	Tolerate	All equipment should reboot once power is restored. APMD to have a list of companies that can provide generators Services outside network will continue to be available (email, Genesis)	Six monthly Check		If equipment is damaged, it will need to be replaced, which will take 3-5 working days.
					861						540		—						

Score 45-81 High Risk
Score 18-42 Moderate risk
Score 1- 16 Low risk

> Progress in a positive direction i.e. reducing the risk
< Progress is negative and risk is getting worse.
<> Progress static subject to actions or as risk is "tolerated"

Actions
Tolerate
Transfer
Treat
Terminate

If Treat, further actions needed