



**Northampton Borough Council**

**Risk and Business Continuity Management Handbook**

## Document Control

<b>Author (Post holder title)</b>	Risk and Business Continuity Manager
<b>Type of document</b>	Handbook
<b>Version Number</b>	V2
<b>Document File Name</b>	Risk and Business Continuity Handbook Final v2
<b>Issue date</b>	
<b>Approval date and by who</b>	
<b>Document held by (name/section)</b>	Sue Morrell/Risk Management
<b>For internal publication only or external also?</b>	Internal
<b>Document stored on Council website?</b>	No
<b>Next review date</b>	Bi-annually

### Change History

<b>Issue</b>	<b>Date</b>	<b>Comments</b>
Version 1	13/01/09	
Version 2	12/02/10	

# Contents

1. Purpose of this document
  2. Risk Management Methodology
    - 2.1 Risk Identification, Assessment and Management
      - 2.1.1 Stage One – Identify
      - 2.1.2 Stage Two – Assess
      - 2.1.3 Stage Three – Manage
      - 2.1.4 Risk Appetite
      - 2.1.5 Stage Four – Monitor and Review
  3. Business Continuity
    - 3.1 Introduction to Business Continuity Management
    - 3.2 Identification of Critical Functions
    - 3.3 Risk and Impact Identification
    - 3.4 Business Continuity Plan
    - 3.5 Testing and exercising
  4. Glossary of Terms
  5. References
- Appendix A – Example Risk Register  
Appendix B – Risk Management in Partnerships  
Appendix C – Risk Management in Projects.  
Appendix D - Approved Business Continuity Critical Functions  
Appendix E – Business Continuity Plan Template

## **1. Purpose of this document**

The purpose of this handbook is to assist Managers and those with specific Risk and Business Continuity responsibilities in undertaking both routine and non-routine risk management activities by providing guidance notes.

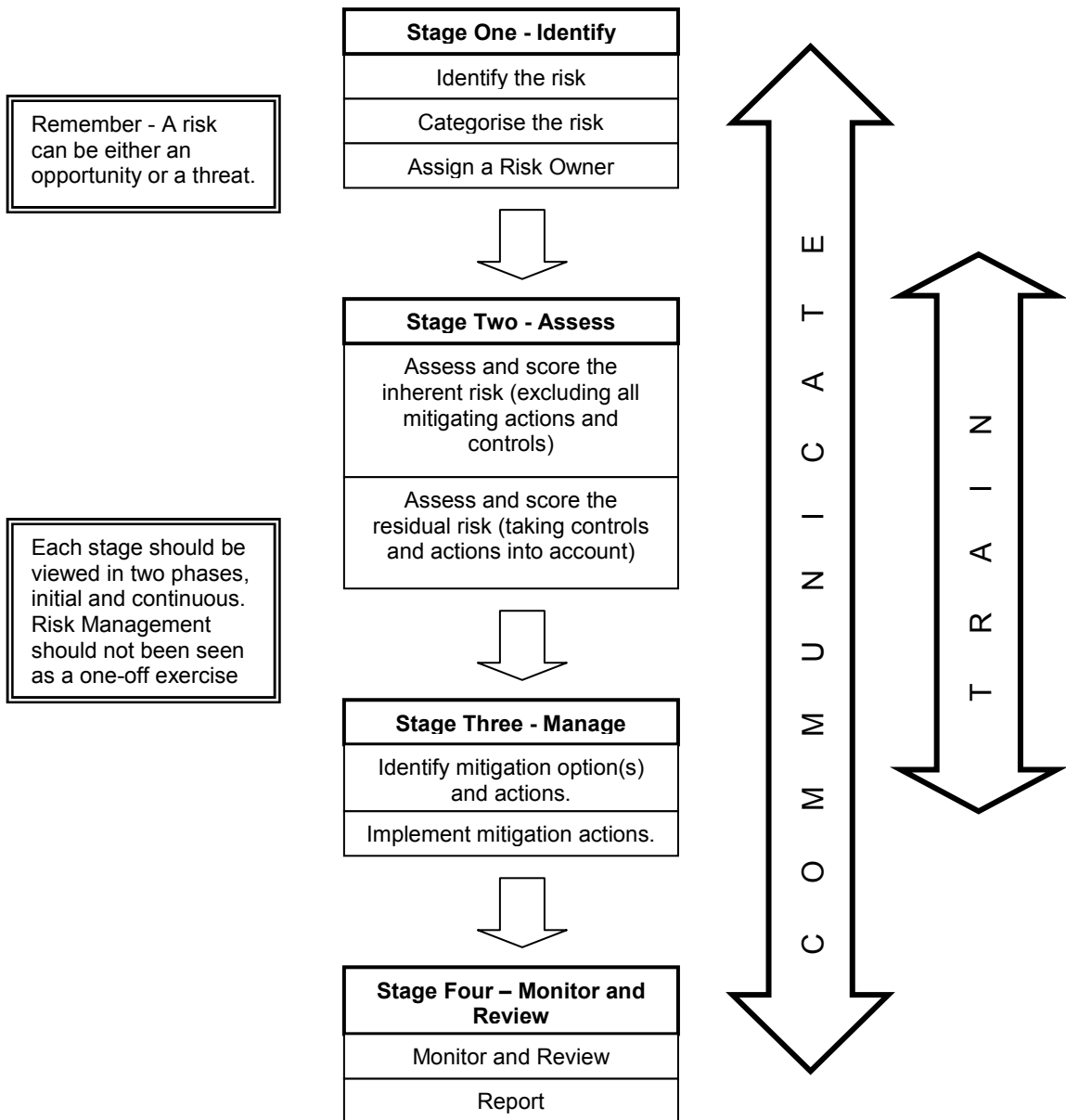
This handbook will evolve and develop over time, allowing for views and suggestions to be incorporated and processes adapted.

A copy of this handbook can be found on the Council's intranet site and is also available from the Risk and Business Continuity Manager on extension 8420.

If you require further support on your risk and business continuity activities or if you have any queries or comments relating to the handbook please contact the Risk and Business Continuity Manager on extension 8420.

## 2. Risk Management Methodology

There are four generic stages to the management of risk. The Council's approach to each of these stages is set out below.



## **2.1 Risk Identification, Assessment and Management**

### **2.1.1 Stage One - Identify**

The first key step in managing risk is to identify the threats, opportunities and barriers to achieving strategic, service, operational, partnership or project objectives(see appendix B and C for partnership and project management). Risks should be assessed and prioritised in relation to objectives. It is important for the Council's aims and objectives to be clearly defined to enable managers to understand the role their service has in delivering these objectives and to identify any potential barriers.

There are three steps to completing the identification stage:

1. A systematic approach should be taken when identifying risks. Brainstorm all potential risk causes, events and impacts.

Please contact the Risk and Business Continuity Manager if you would like help facilitating workshops or risk sessions.

The following tools can be used to assist in risk identification:

- Brainstorming
- Workshops
- Checklists
- Questionnaires
- SWOT analysis (strengths, weaknesses, opportunities and threats)
- Lessons learned reports

Remember that risks can be opportunities as well as threats. An opportunity is an uncertain event that could have a **favourable** impact on objectives or benefits, whereas a threat is an uncertain event that could have a **negative** impact on objectives or benefits.

It should be noted that if a risk has more than one impact, each impact should be recorded and scored independently. If a risk is too broad or generic, identifying impacts, mitigation actions and tracking progress can become problematical.

The following statement can be helpful when identifying risks - *As a result of (the cause) there is a risk that (the event) which may result in (the impact).*

A common error made when identifying risks is confusing a risk with an issue. An issue is an event or situation that has already occurred and needs managing now.

2. Northampton Borough Council, along with other local authorities, manages a diverse range of complex services and activities and the categorisation of each risk at the identification stage assists the reporting, review and monitoring of risks.

Categorise the risks using the categories listed below. Risks can be grouped by Risk Owner, Service Area or category i.e. financial, legal.

- Customers/citizens
- Communication
- Environmental
- Financial
- Health and Safety
- Human Resources
- IT
- Legal
- Partnership
- Political
- Property and Assets
- Reputation
- Service Delivery/business interruption
- Suppliers/contractors

3. At the identification and categorisation stage a Risk Owner, a single accountable officer, must be assigned to each risk. The Risk Owner must have adequate decision-making abilities in relation to the risk and be the individual best placed to monitor and manage the risk.

The Council's Risk Management process is supported by a specialist software package that simplifies the recording, reviewing and reporting on the Council's risks, whilst aligning the risks to corporate and service objectives. Training on the risk management software is available to Risk Owners and Risk Coordinators. Please contact the Risk and Business Continuity Manager on extension 8420.

### **2.1.2 Stage Two – Assess**

Each risk should be scored using the 5x5 scoring matrix below, taking into account the probability of the risk occurring and the severity of impact. The Strategic Scorecard can be used for guidance (Table 2). In the first instance risks should be assessed without taking any control measures or mitigations into account. This provides us with an ***inherent risk*** score. Understanding the inherent risk is important to the Council as it enables us to understand the true extent of our exposure if mitigating actions and controls are not implemented or maintained.

Now taking into account the controls and mitigation actions, re-score the risk. Risk Owners should consider how the controls and mitigating actions reduce the probability of the risk occurring and reduce the impact the risk may have. This provides us with a ***residual risk*** score.

**Table 1 - Scoring Matrix**

<b>Impact</b>	<b>5</b> <i>Catastrophic</i>	<b>5</b>	<b>10</b>	<b>15</b>	<b>20</b>	<b>25</b>
	<b>4</b> <i>Major</i>	<b>4</b>	<b>8</b>	<b>12</b>	<b>16</b>	<b>20</b>
	<b>3</b> <i>Moderate</i>	<b>3</b>	<b>6</b>	<b>9</b>	<b>12</b>	<b>15</b>
	<b>2</b> <i>Minor</i>	<b>2</b>	<b>4</b>	<b>6</b>	<b>8</b>	<b>10</b>
	<b>1</b> <i>Insignificant</i>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
		<b>1</b> <i>Rare</i>	<b>2</b> <i>Unlikely</i>	<b>3</b> <i>Possible</i>	<b>4</b> <i>Likely</i>	<b>5</b> <i>Almost certain</i>
		<b>Probability</b>				

**Probability Guideline**

- Rare <5%
- Unlikely 6 – 20%
- Possible 21 - 50%
- Likely 51 – 80%
- Almost Certain >81%



**Table 2 – Strategic Scorecard**

The scorecard below provides a consistent approach to determining the level of impact, recognising that terms can mean different things to different people.

**Impact Guideline**

	<b>Insignificant (Very Low)</b>	<b>Minor (Low)</b>	<b>Moderate (Medium)</b>	<b>Major (High)</b>	<b>Catastrophic (Very High)</b>
<b>Financial Cost</b>	£1 - £50k	£51K - £250K	£251K -£500K	Over £501K up to £1M	£1M +
<b>Service Provision</b>	Quality maintained some minor issues	Slightly Reduced – deadlines not achieved / some Local PIs poor	Severely Reduced – majority of targets not achieved. KPI's poor	Service Suspended Short Term	Service Suspended Long Term Statutory duties not delivered
<b>Objectives</b>	Objectives broadly achieved	Objectives of Section not met	Service Objectives not met	Directorate Objectives not met	Strategic objectives not met
<b>Government/Inspectorate relations</b>	Minor issues	Areas for improved Options curtailed Freedoms not granted	Overall Poor Assessment(s) – Funding impact	Service taken over temporarily	Service taken over permanently
<b>Employee Relations</b>	Localised Issue Distraction	Issue in a number of departments Losing goodwill	Hostile working relations/non cooperation Major distraction	Industrial action Long term relationship “sourer”	Mass staff leaving/ long term grievance / Unable to attract staff
<b>Reputation</b>	Letters in local press	Adverse “one off” reports in local media	Long term adverse reports Regional TV reports	Adverse national publicity Fewer partners	High profile national bad publicity. Becomes difficult to attract any partners
<b>Mgmt Team</b>	Minor issues	Seen as poor	Misconduct / seen as failing	Potential loss of job	Imprisonment
<b>Health &amp; Safety</b>	First Aider	Broken bones/illness	Loss of Limb/Long Term illness	Loss of Life/Major illness	Large scale loss of life/major epidemic

### 2.1.3 Stage Three - Manage

The primary goal of this stage is to identify and prepare specific responses to the threats or opportunities identified in the identification stage above. If the responses and mitigation actions are fully considered at this stage it should prevent the Council being taken by surprise should a risk occur.

There are a number of ways to respond to a risk. Table 3 describes the potential responses available to threats and Table 4 describes the potential responses available to opportunities.

**Table 3 Response to Threats**

<b>Reduction</b>	Proactive actions taken to reduce: <ul style="list-style-type: none"> <li>➤ The probability of the event occurring, by performing some form of control</li> <li>➤ The impact of the event should it occur e.g. Business Continuity Plans.</li> </ul>
<b>Removal</b>	Typically involves changing one aspect of the activity i.e. changing the scope, procurement route, supplier or sequence of activities.
<b>Transfer</b>	A third party takes on responsibility for an aspect of the threat e.g. insurance.
<b>Retention</b>	A conscious and deliberate decision is taken to retain the threat, having decided that it is more cost effective to do so than attempt a mitigation action.
<b>Share</b>	Procurement methods that entail a form of risk sharing through the application of sharing pain or gain formula.

The list of definitions is taken from the OGC Management of Risk: Guidance for Practitioners.

**Table 4 Response to Opportunities**

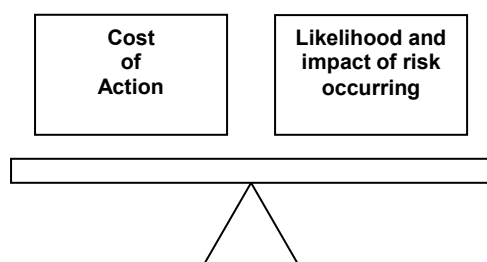
<b>Realise</b>	Identifying and seizing an opportunity. Ensures that potential improvements to an organisational activity are delivered.
<b>Enhance</b>	Seizing and improving on an identified opportunity. Refers to both the realisation of an opportunity and achieving additional gains over and above the opportunity.
<b>Exploit</b>	Identifying and seizing multiple benefits. Refers to changing an activity's scope, supplier or specification to achieve a beneficial outcome.
<b>Share</b>	Procurement methods entailing a form of risk sharing through application of pain/gain formula.

The list of definitions is taken from the OGC Management of Risk: Guidance for Practitioners.

One consideration available under the 'reduce' response is the development of Business Continuity arrangements and plans to reduce the impact if an event occurs. This is a key requirement for Local Authorities under the Civil Contingencies Act 2004, as described in Section 3.1 below.

Once a Risk Owner has decided which is the best response to take, the Risk Owner then has to decide on the controls and actions to put in place to manage the risk.

### **Balancing the risk**



It is important for Risk Owners to ensure the mitigation actions put in place are proportional to the risk. The Council's Risk Appetite is a useful tool when deciding on the best way to manage a risk.

#### **2.1.4 Risk Appetite**

Recognising that the Council should not manage all risks to the same extent, scoring helps to prioritise each risk enabling the Council to understand where time and resources should be focussed.

One of the key stages for the successful implementation of a risk management framework is the need to define the Council's 'risk appetite'. Risk appetite refers to the Council's attitude to taking risk and defines the amount of risk the Council considers acceptable in order to achieve its objectives.

The Council's risk appetite can be defined as set out in Table 5 below. Any residual risk scoring more than 12 is above the acceptable tolerance level and further work needs to be done to effectively manage this risk.

Actively using the information provided in Table 5 below can significantly help Risk Owners balance the level of resource and time taken to manage the risks on their risk registers, many risks will require no action to be taken with only periodic monitoring required.

**Table 5: Risk appetite as it relates to residual risk score**

Overall Residual Risk Score	RISK APPETITE	
<b>20-25</b>	Unacceptable level of risk exposure which requires <i>immediate corrective action to be taken or referral to next level</i>	<b>EXCEEDS OUR RISK APPETITE</b>
<b>12-16</b>	Unacceptable level of risk exposure which requires <i>constant active monitoring, and measures to be put in place to reduce exposure and/or referral to next level</i>	
<b>5-10</b>	Acceptable level of risk exposure subject to <i>regular active monitoring measures</i>	<b>WITHIN OUR RISK APPETITE</b>
<b>3-4</b>	Acceptable level of risk exposure subject to <i>regular passive monitoring measures</i>	
<b>1-2</b>	Acceptable level of risk exposure subject to <i>periodic passive monitoring measures</i>	

**2.1.5 Stage Four - Monitor and Review** All risks will be reviewed and updated at least monthly by the Risk Owner involving team members as required. Changes to the risk profile, updated information on mitigating actions and progress will be recorded on the Council’s electronic risk register with the support of the Risk Coordinators.

When undertaking a risk review, Risk Owners should consider:

1. Any new risks to be added or expired risks to be removed
2. Reassessment of current risk scores
3. Review of actions completed and outstanding
4. Any additional mitigating actions required
5. The need for escalation

There are several reasons why a risk may need to be escalated to the next level of management:

- Requires higher management level awareness or decision
- Request for additional resources to assist mitigation
- Potential transfer of risk to another level, ownership or register
- A more strategic or tactical, rather than operational approach

Risk escalation does not necessarily mean a transfer of Risk Ownership. Often Risk Ownership will stay the same whilst being supported by the next level of management.

### 3. Business Continuity

#### 3.1 Introduction into Business Continuity Management

Business Continuity Management is about identifying those services that the Council cannot afford to lose (in terms of vulnerable residents, financial loss, loss of reputation) and planning how to maintain those services if an incident or major disruption should occur.

Under the Civil Contingencies Act 2004 the Council has a responsibility to; *“maintain plans to ensure that they can continue to perform their functions in the event of an emergency, so far as is reasonably practicable”*.

Business continuity is not about managing the emergency, this is covered under emergency planning, but is concerned with the delivery of critical functions immediately following an emergency or disruption.

#### 3.2 Identification of Critical Functions

A two-staged, Council-wide, Business Impact Assessment has been undertaken to identify critical functions. A copy of the Council’s Critical Functions is included (Appendix D).

The first step in the process is to identify which functions are critical to the Council i.e. those that need to be up and running within a short period of time immediately following an incident. This stage helps to identify which services/activities need to have a Business Continuity Plan developed.

It can be undertaken as a workshop or as part of a team meeting. The outputs from this stage need to be recorded. Using a table can be a useful way of recording the outcomes. See Table 6 below.

**Table 6**

<b>SERVICE DESCRIPTION</b>	<b>IMPACT OF NOT DELIVERING THE SERVICE</b>	<b>LENGTH OF TIME REQUIRED (0-24 HRS, 1-3 DAYS, 3-7 DAYS, MORE THAN 1 WEEK)</b>	<b>TYPE OF RESOURCES REQUIRED (PEOPLE, TRANSPORT, PREMISES)</b>	<b>LEVEL OF RESOURCES REQUIRED (6 PEOPLE, 4 WORK AREAS WITH PC’S)</b>

**Task 1** - List all the services your service area/team delivers.

**Task 2** - Consider the impacts on all service stakeholders of not delivering that service, the extent and severity of the impact.

- Considering what is provided to whom, how, when, where and why.

**Task 3** - Identify how quickly each service needs to be up and running again in order to limit significant impacts on stakeholders.

- **Remember** – *we are not looking to resume all services to their normal operating standards.*
- For consistency please use the following timings:
  - 0 – 24 hours - Critical Function 1 (CF1)
  - 1 – 3 days - Critical Function 2 (CF2)
  - 3 – 7 days - Critical Function 3 (CF3)
  - > 1 week – not a Critical Function (NCF)

*Those services falling within the Critical Function classifications above are the key services that need a Business Continuity Plan in place and are the services that should be focused on in the remaining stages of the process.*

**Task 4** - Consider the type and level of resources required to maintain the critical activities within the timescales specified above i.e. premises, people, technology, communications, suppliers, information, transportation. Table 7 provides a useful series of questions to be used as a prompt.

**Table 7 – Questions to consider when quantifying the resources you require to maintain your critical activities.**

<p><b>People</b></p> <ul style="list-style-type: none"> <li>• What is the optimum number of staff you require to carry out your critical service?</li> <li>• What is the minimum staffing level with which you could provide some sort of service?</li> <li>• What skills/level of expertise is required to undertake these activities?</li> </ul>	<p><b>Technology</b></p> <ul style="list-style-type: none"> <li>• What IT is essential to carry out your critical activities?</li> <li>• What systems and means of voice and data communication are required to carry out your critical activities?</li> </ul> <p><b>Information</b></p> <ul style="list-style-type: none"> <li>• What information is essential to carry out your critical activities?</li> <li>• How is this information stored?</li> </ul>
<p><b>Premises</b></p> <ul style="list-style-type: none"> <li>• What locations do your critical activities operate from?</li> <li>• What alternative premises do you have?</li> <li>• What plant, machinery and other facilities are essential to carry out your critical activities?</li> </ul>	<p><b>Suppliers and Partners</b></p> <ul style="list-style-type: none"> <li>• Who are your priority suppliers/partners whom you depend on to undertake your critical activities?</li> <li>• Do you tender key services out to another organisation, to whom, for what?</li> <li>• Do you have any reciprocal arrangements with other organisations?</li> </ul>

HM Government, Business Continuity Management Toolkit.

### **3.3 Risk and Impact Identification**

To help us understand where we should focus our risk management activities, it is important for us to understand the type of risks that could occur, how probable they are and what the impact and disruption could be on your services.

The risk and impact identification stage in this process may have already been undertaken as part of your routine risk identification and management activities, please refer to section 2.4 of the Risk Management Strategy. However, detailed below are a few helpful points to consider.

- The Community Risk Register found on the following link is a useful document when considering the risks facing the authority.

<http://www.northamptonshire.gov.uk/en/councilservices/fire/eplan/Pages/CommRiskRegister.aspx>

- When considering the type of risk that could affect your services e.g. flood, flu pandemic, fire and the impact that risk could have, bear in mind that most risks will result in one or more of the following impacts to your service:
  - Loss of staff (flu pandemic, strike action)
  - Loss of premises (loss of utilities, fire, flood, within exclusion zone)
  - Loss of systems IT, telecommunications
  - Loss of transport (fuel shortage)
  - Loss of key supplier
- As with any risk management process, you now need to decide how the risk should be managed i.e.:
  - Reduce (manage it)
  - Remove (change, suspend or terminate a service)
  - Retain (live with it)
  - Transfer (insure it or get a 3<sup>rd</sup> party to manage it)
  - Share (share it with supplier or partner)

Decide what action should be taken and develop a strategy for meeting the recovery time as defined above. Please see Table 8 to assist in developing a strategy.

**Table 8 – Tactics you could adopt to protect your resources.**

<p><b>People</b></p> <ul style="list-style-type: none"> <li>• Inventory of staff skills not utilised within their existing roles – to enable redeployment.</li> <li>• Process mapping and documentation – to allow staff to undertake roles with which they are unfamiliar.</li> <li>• Multi-skill training of each individual.</li> <li>• Cross training of skills across a number of individuals.</li> <li>• Succession planning.</li> <li>• Use of third party support, backed by contractual agreements.</li> <li>• Geographical separation of individuals with core skills can reduce the likelihood of losing all those capable of undertaking a specific role.</li> </ul>	<p><b>Premises</b></p> <ul style="list-style-type: none"> <li>• Relocation of staff to other accommodation owned by NBC.</li> <li>• Displacement of staff performing less urgent business processes with staff performing a higher priority activity. Care must be taken when using this option that backlogs of the less urgent work do not become unmanageable.</li> <li>• Remote working – this can be working from home or working from other locations.</li> <li>• Use premises provided by other organisations.</li> <li>• Alternative sources of plant, machinery and other equipment.</li> </ul>
<p><b>Technology</b></p> <ul style="list-style-type: none"> <li>• Maintaining the same technology at different locations that will not be affected by the same business disruption.</li> <li>• Holding older equipment as emergency replacement or spares.</li> </ul>	<p><b>Suppliers and Partners</b></p> <ul style="list-style-type: none"> <li>• Storage of additional supplies at another location.</li> <li>• Dual or multi-sourcing of materials.</li> <li>• Identification of alternative suppliers.</li> <li>• Encouraging or requiring suppliers/partners to have a validated business continuity capability.</li> <li>• Significant penalty clauses on supply contracts.</li> </ul>
<p><b>Information</b></p> <ul style="list-style-type: none"> <li>• Ensure data is backed up and it is kept off site.</li> <li>• Essential documentation is stored securely (e.g. fire proof safe).</li> <li>• Copies of essential documentation are kept elsewhere.</li> </ul>	<p><b>Stakeholders</b></p> <ul style="list-style-type: none"> <li>• Mechanisms in place to provide information to stakeholders.</li> <li>• Arrangements to ensure vulnerable groups are accommodated.</li> </ul>

HM Government, Business Continuity Management Toolkit.



### **3.4 Business Continuity Plan**

Develop a Business Continuity Plan for each Critical Function that sets out how you will deliver the strategy above. Decide whether your plans should be developed by Service or Critical Function. Start with the most critical services first i.e. those defined as a CF1 or CF2.

Standard components of a Business Continuity Plan. Please use the template included in Appendix E.

- Document control – distribution list, version control
  - Document owner and maintainer.
  - Purpose and scope – relationship to other plans, services to be included.
  - Plan invocation – set out who has the responsibility to invoke the plan, circumstances for invocation.
  - Roles and responsibilities – individuals with a role in the implementation of the plan.
  - Location from which an incident will be managed.
  - Communication arrangements – plans for communicating with staff, stakeholders.
  - Set out critical activities and recovery times
  - Resource requirements and arrangements
  - Contact details – for all key stakeholders and staff involved in the plan.
- A Business Continuity Plan should be short and simple; if the information is not required during the immediate response then it should not be included in the plan.

### **3.5 Testing and exercising**

A Business Continuity Plan cannot be considered reliable until it has been exercised and tested. Valuable lessons will be learnt during an exercise drill that can be recorded as lessons learnt and changes incorporated within the plan. Exercises can be desktop based or a live exercise.

Assistance and support with testing and exercising Business Continuity Plans is available from the Risk and Business Continuity Manager.

All Business Continuity Plans will be reviewed at least annually, unless service activities or locations change.

## 4. Glossary of terms

<b>Business Continuity Plan</b>	A documented set of procedures and information intended to deliver continuity of critical functions in the event of a disruption.
<b>Business Impact Assessment</b>	Identifies and documents the key services and activities; the critical functions required to deliver these; the impact that a disruption of these activities would have on the Council and it's customers and the resources required to resume the activities.
<b>Category 1 Responder</b>	A person or body listed in Part 1 of Schedule 1 to the Civil Contingencies Act. Those in Category 1, are those organisations at the core of the response to most emergencies (e.g. emergency services, local authorities, NHS bodies). Category 1 responders are subject to the full set of civil protection duties.
<b>Civil Contingencies Act</b>	The Civil Contingencies Act 2004 establishes 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 modernises the emergency powers framework in the United Kingdom.
<b>Critical Function</b>	The functions which must be kept going or rapidly reinstated, at least in part, in the event of any disruption
<b>Enhance</b>	A risk response for an opportunity. The realisation of an opportunity and achieving additional gains over and above the opportunity.
<b>Exploit</b>	A risk response for an opportunity. Changing an activity's scope, suppliers or specification in order to achieve a beneficial outcome.
<b>Impact</b>	Impact is the result of a particular threat or opportunity actually occurring.
<b>Inherent Risk</b>	The exposure arising from a specific risk before any action has been taken to manage it.
<b>Issue</b>	A relevant event that has happened, was not planned and requires management action.
<b>Opportunity</b>	An uncertain event that could have a positive impact on objectives or benefits.
<b>Probability</b>	The evaluated likelihood of a particular threat or opportunity actually happening.
<b>Realise</b>	A risk response for an opportunity. Ensures that potential improvements to an organisational activity are delivered.

<b>Reduction</b>	A risk response for a threat. Proactive actions are taken to reduce the probability of the event occurring or the impact of the threat should it occur.
<b>Removal</b>	A risk response for a threat. Typically involves changing an aspect of the organisational activity.
<b>Residual Risk</b>	The risk remaining after the risk response has been applied.
<b>Retention</b>	A risk response for a threat. A conscious and deliberate decision is taken to retain the threat.
<b>Risk</b>	An uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives.
<b>Risk Appetite</b>	An organisation's unique attitude to risk taking.
<b>Risk Cause</b>	A description of the source of the risk.
<b>Risk Event</b>	A description of the area of uncertainty in terms of the threat or opportunity.
<b>Risk Identification</b>	Determination of what could pose a risk.
<b>Risk Management</b>	Systematic application of principles, approach and processes to the tasks of identifying and assessing risks.
<b>Risk Owner</b>	An individual responsible for the management and control of all aspects of individual risks.
<b>Risk Register</b>	A record of all identified risks.
<b>Risk Response</b>	Actions that may be taken to bring the situation to a level where the exposure to risk is acceptable to the organisation.
<b>Share</b>	A risk response for a threat or opportunity. Procurement methods entailing a form of risk sharing through application of pain/gain formula.
<b>Strategic risk</b>	Risk concerned with where the organisation wants to go, how it plans to get there, and how it can ensure survival.
<b>Threat</b>	An uncertain event that could have a negative impact on objectives or benefits.
<b>Transfer</b>	A risk response for a threat. Whereby a third party takes on responsibility for an aspect of the threat.

## **5. References**

A Guide to Business Continuity Management in Gloucestershire County Council, 2006.

A Guide to the Corporate Manslaughter and Corporate Homicide Act 2007, Ministry of Justice.

Business Continuity Management Good Practice Guidelines 2008, The Business Continuity Institute.

Cambridge City Council Risk Management Strategy 2007.

How prepared are you? Business Continuity Management Toolkit version 1– HM Government.

Milton Keynes Council Risk Management Process – A Guide 2008.

Management of Risk: Guidance for Practitioners, Office of Government Commerce.

Managing Successful Projects with PRINCE2, Office of Government Commerce.

Northamptonshire County Council Risk Management Protocol May 2008.

Solihull Metropolitan Borough Council Risk Management Strategy March 2008

The Accounts and Audit Regulations 2006.

The Orange Book, Management of Risk – Principles and Concepts.

## Appendix A – Example Risk Register

The Council's risk register corresponds to the entry fields in the risk management software.

ID	Category	Risk Owner	Risk Cause (as a result of)	Risk Event (there is a risk that)	Risk Impact (which may result in)	Inherent Risk Scores (assume no controls)			Mitigation Actions and Controls	Residual Risk Scores			Action Owner	Action Completion Date	Progress update	
						Impact (1-5)	Probability (1-5)	Score I x P		Impact (1-5)	Probability (1-5)	Score I x P				

## **Appendix B – Guidance on Risk Management in Partnerships**

One element of good partnership governance is risk management. Risk management helps to ensure partnerships succeed in achieving the objectives they set out to deliver whilst protecting the interests of the individual partners and stakeholders. Prior to entering into a Partnership arrangement, the risks associated should be assessed to ensure the level of exposure is acceptable to the Council.

In a partnership environment, risks should be managed both from the perspective of the partnership and of each partner.

### ***Partnership Approach***

At the commencement of any partnership the following steps should be undertaken by the Partnership Manager:

1. Using the partnership's objectives, agreement, memorandum of understanding etc., undertake an initial risk identification exercise to understand both the barriers to achieving the objectives and any potential opportunities. Guidance can be found in the Council's Risk and Business Continuity Handbook.
2. Record the risks on a risk register, excel template attached.
3. For each risk identified, complete all sections of the register:
  - i. Cause, event and impact.
  - ii. Risk Owner.
  - iii. Inherent and residual risk scores.
  - iv. Mitigating actions and controls.
  - v. Action owners and estimated completion dates.
4. Routinely (depending on the partnership governance cycle and level of risk exposure) the Risk Owner should review and update the risk. The Action Owner should update progress on the actions.
5. In line with the partnership's governance approach, high risks or risks causing concern should be reported to the Partnership Board. Financial risks should be escalated to the Head of Service and service accountant.
6. Risk should be a standing agenda item at Board and Team Meetings.

The risk register should be available to all members of the partnership.

Any risks identified throughout the life of a partnership that relate to an individual partner should be escalated to the partner concerned.

### ***Approach for Individual Partners***

The individual partners involved in a partnership should undertake each of the steps above but should assess the risks from their own perspective. A risk can have a different impact depending on the organisation assessing it.

To ensure openness on the individual's risk approach, it may be prudent for the partner's own register to not be shared with the wider partnership.

## Notes

### Risk categories:

- Customers/citizens
  - Communication
  - Environmental
  - Financial
  - Health and Safety
  - Human Resources
  - IT
  - Legal
  - Partnership
  - Political
  - Property and Assets
  - Reputation
  - Service Delivery/business interruption
  - Suppliers/contractors
- The following statement can be helpful when identifying risks
    - As a result of **(the cause)** there is a risk that **(the event)** which may result in **(the impact)**.
  - Remember that risks can be opportunities as well as threats.
  - A common error made when identifying risks is confusing a **risk** with an **issue**. An **issue** is an event or situation that has already occurred and needs managing now.
  - Inherent risk score – the exposure from a risk before any action has been taken to manage it.
  - Residual risk score – the remaining risk once a risk response has been taken.

### Risk Matrix

<b>Impact</b>	<b>5</b> <i>Catastrophic</i>	5	10	15	20	25
	<b>4</b> <i>Major</i>	4	8	12	16	20
	<b>3</b> <i>Moderate</i>	3	6	9	12	15
	<b>2</b> <i>Minor</i>	2	4	6	8	10
	<b>1</b> <i>Insignificant</i>	1	2	3	4	5
		<b>1</b> <i>Rare</i>	<b>2</b> <i>Unlikely</i>	<b>3</b> <i>Possible</i>	<b>4</b> <i>Likely</i>	<b>5</b> <i>Almost certain</i>
		<b>Probability</b>				

## ***Appendix C – Risk Management in Projects***



## **Appendix D – Approved Business Continuity Critical Functions**

<b>Description</b>	<b>Critical Function Category</b>	<b>Service Area</b>	<b>Head of Service</b>
Co-ordination of instruction of urgent repair works to corporate properties (not performance of actual repair works)	CF1	Asset Management	Gavin Chambers
Leisure Centres – Danes Camp, Lings Forum - to be used as 'reception centres' in the event of an emergency.	CF1	Culture and Leisure	Ian Redfern
External communications - media	CF1	Communications	Cara Boden
External communications - partners	CF1	Communications	Cara Boden
Internal communications (Live News / All User email)	CF1	Communications	Cara Boden
Website / intranet home page updates	CF1	Communications	Cara Boden
Time sensitive Corporate marketing activities	CF1	Communications	Cara Boden
Switchboard	CF1	Customer Services	Marion Goodman
Automated Call Distribution configuration	CF1	Customer Services	Marion Goodman
Emergency Repairs Call Handling	CF1	Customer Services	Marion Goodman
One Stop Shop or face to face access	CF2	Customer Services	Marion Goodman
General Call Handling – Contact Centre (Housing, Streetscene, Revs and Bens)	CF2	Customer Services	Marion Goodman
Emergency Management Team	CF1	Emergency Planning	Thomas Hall
Payroll*	CF2	Finance	Gavin Chambers

Final accounts, budget and council tax setting, Rent setting*	CF2	Finance	Gavin Chambers
Transactional banking	CF3	Finance	Gavin Chambers
Treasury Management	CF3	Finance	Gavin Chambers
S151 officer	CF3	Finance	Gavin Chambers
Key Holding Opening of buildings	CF1	Facilities Management	Marion Goodman
Disarming of Intruder Alarm	CF1	Facilities Management	Marion Goodman
Access/Entry System	CF1	Facilities Management	Marion Goodman
Evacuations	CF1	Facilities Management	Marion Goodman
Supply of meeting rooms & refreshments for emergency planning teams and provision of halls/meeting rooms in the event of evacuation to Guildhall.	CF1	Facilities Management	Marion Goodman
Cleaning of Buildings – potentially harmful or infectious substances.	CF2	Facilities Management	Marion Goodman
Mail Delivery and Collection	CF3	Facilities Management	Marion Goodman
Provision management of temporary accommodation	CF1	Housing Needs and Support	Fran Rodgers
Emergency housing allocations**	CF1	Housing Needs and Support	Fran Rodgers
Social alarm for community	CF1	Housing Needs and Support	Fran Rodgers
Out of hours call – social services	CF1	Housing Needs and Support	Fran Rodgers
Daily visits – Level 3s	CF1	Housing Needs and Support	Fran Rodgers
Hospital discharge assessments	CF1	Housing Needs and Support	Fran Rodgers

Emergency response service – coordinators	CF1	Housing Needs and Support	Fran Rodgers
Gateway Assessments	CF2	Housing Needs and Support	Fran Rodgers
Homelessness Investigations	CF2	Housing Needs and Support	Fran Rodgers
Private sector housing - duty	CF2	Housing Needs and Support	Fran Rodgers
Daily visits – Level 2s	CF2	Housing Needs and Support	Fran Rodgers
Daily visits – Level 1s	CF2	Housing Needs and Support	Fran Rodgers
Installation of life line – hospital discharge	CF2	Housing Needs and Support	Fran Rodgers
Housing advice – telephone service	CF2	Housing Needs and Support	Fran Rodgers
Corporate Health and Safety	CF1	Human Resources	Catherine Wilson
Access to HR systems	CF1	Human Resources	Catherine Wilson
Data Network Infrastructure	CF1	ICT	Marion Goodman
Voice Network Infrastructure	CF1	ICT	Marion Goodman
Server and Storage Area Network Support	CF1	ICT	Marion Goodman
Geographical Information Systems	CF2	ICT	Marion Goodman
Operational Server Support / Environmental Control / Data Storage/ Security Backups	CF2	ICT	Marion Goodman
I.C.T. Helpdesk	CF3	ICT	Marion Goodman
PC Support	CF3	ICT	Marion Goodman
Email and Internet Access	CF3	ICT	Marion Goodman
Business Application Support	CF3	ICT	Marion Goodman

Internet and Intranet Support	CF3	ICT	Marion Goodman
Court and Tribunal attendance for planned and emergency hearings, and urgent service of Planning Enforcement Stop Notices.	CF1	Borough Solicitor	Francis Fernandes
Provision of general legal advice related to the event	CF1	Borough Solicitor	Francis Fernandes
Provision of Monitoring Officer advice in relation to the event	CF1	Borough Solicitor	Francis Fernandes
Elections*	CF1	Borough Solicitor	Francis Fernandes
Legal Administration supporting court etc attendance	CF3	Borough Solicitor	Francis Fernandes
Committee Administration	CF3	Borough Solicitor	Francis Fernandes
Emergency Repairs	CF1	Landlord Services	Christine Ansell
Urgent Repairs	CF2	Landlord Services	Christine Ansell
Burials	CF1	Neighbourhood Environmental Services	Simone Wade
Westbridge Gatehouse	CF1	Neighbourhood Environmental Services	Simone Wade
Fuel Supply for Council Vehicles	CF1	Neighbourhood Environmental Services	Simone Wade
Management of Waste Operations (Staff/Office)	CF2	Neighbourhood Environmental Services	Simone Wade
Weekly Collection Of Domestic Waste In Black Sacks	CF2	Neighbourhood Environmental Services	Simone Wade
Clinical Waste Collections	CF2	Neighbourhood Environmental	Simone Wade

		Services	
Town Centre Cleansing	CF2	Neighbourhood Environmental Services	Simone Wade
Alternate Weekly Domestic Waste Collections In The Black Wheelie Bins	CF3	Neighbourhood Environmental Services	Simone Wade
Business Waste Collections	CF3	Neighbourhood Environmental Services	Simone Wade
Dangerous Structures	CF1	Planning	Sue Bridge
Provisions of CCTV	CF1	Public Protection	Steve Elsey
Emergency Prohibitions for Food Hygiene and H & S	CF1	Public Protection	Steve Elsey
Immediate control measures of a serious infectious disease	CF1	Public Protection	Steve Elsey
Immediate control measures of a serious incident where LA is enforcer	CF1	Public Protection	Steve Elsey
General Public Health control measures	CF3	Public Protection	Steve Elsey
Control measures of less serious infectious diseases	CF3	Public Protection	Steve Elsey
Housing Benefit – rent allowances (Private tenants)	CF1	Revenues and Benefits	Robin Bates
Bus Station - Management	CF3	Town Centre Management	Derrick Simpson
Car Parking	CF3	Town Centre Management	Derrick Simpson
Markets	CF3	Town Centre Management	Derrick Simpson

\*Critical at particular time of month or year.

\*\*Added to list after approval by Management Board – approved by FR



**Appendix E –Business Continuity Plan Template**



**Northampton Borough Council**

***(Insert service/department)* Business Continuity Plan**

***(Template)***

**Controlled Circulation – document contains confidential information**

<b>File name:</b>	
<b>Version:</b>	
<b>Document Owner:</b>	
<b>Approved By:</b>	
<b>Signature:</b>	

## Contents Page



## 1. Document Control

*(name a document owner and maintainer)*

### Distribution List

<b>Name</b>	<b>Location Of Plan</b> <i>(copies must be kept offsite i.e. at home or alternative office)</i>

### Record of Amendments

<b>Date</b>	<b>Version number</b>	<b>Detail of amendment/revision</b>	<b>Amended/revised by</b>

This plan will be reviewed and updated at least annually, more frequently if service location or activities change.

## 2. Purpose and Scope

*Relationship to other plans across the authority, services to be included and excluded, brief description of services.*

### 3. Plan Invocation/Activation

*Who has the responsibility to invoke the plan, circumstances for invocation.*

*Include a quick activation checklist e.g. the first 5 – 10 things that must be done.*

### 4. Roles and Responsibilities

*Details of individuals with a specific role in plan and details of the role.*

Name	Role/Tasks

## **5. Location from which the incident will be managed.**

*Details of location and an alternative. Address, Contact name, telephone number, access details.*

## **6. Communication Arrangements**

*Plans for communicating with staff and stakeholders, call cascade, who needs to know what and when, standard messages.*

## 7. Critical Functions and Recovery Times

*Approved critical functions.*

<b>Critical Function 1 – Brief Description</b>	<b>Impact on NBC if service not delivered</b>	<b>Recovery time</b>

<b>Critical Function 2 - Brief Description</b>	<b>Impact on NBC if service not delivered</b>	<b>Recovery time</b>

<b>Critical Function 3 - Brief Description</b>	<b>Impact on NBC if service not delivered</b>	<b>Recovery time</b>

## 8. Resource Requirements for Critical Functions

*Minimum requirements to achieve recovery time for critical functions and alternative sources for requirements.*

### Critical Function 1s

<b>Function Description</b>	
<b>Staff</b>	<i>Minimum number of staff, knowledge and skills required, what are the alternative staffing arrangements.</i>
<b>Accommodation</b>	<i>Desk space. Home working etc.</i>
<b>Agreed Alternative Accommodation Arrangements</b>	<i>Address, contact name, telephone number, access restrictions, key holders.</i>
<b>Systems (IT and comms)</b>	<i>Back up/recovery processes. Network connection, telephone access required etc.</i>
<b>Hard Data</b>	<i>Files, paperwork, where are they stored, alternative locations for storage.</i>
<b>Key Suppliers</b>	<i>Check their continuity arrangements, alternative suppliers etc.</i>
<b>Other</b>	

### Critical Function 2s

<b>Function Description</b>	
<b>Staff</b>	<i>Minimum number of staff, knowledge and skills required, what are the alternative staffing arrangements.</i>
<b>Accommodation</b>	<i>Desk space. Home working etc.</i>
<b>Agreed Alternative Accommodation Arrangements</b>	<i>Address, contact name, telephone number, access restrictions, key holders.</i>
<b>Systems (IT and comms)</b>	<i>Back up/recovery processes. Network connection, telephone access required etc.</i>
<b>Hard Data</b>	<i>Files, paperwork, where are they stored, alternative locations for storage.</i>
<b>Key Suppliers</b>	<i>Check their continuity arrangements, alternative suppliers etc.</i>
<b>Other</b>	

### Critical Function 3s

<b>Function Description</b>	
<b>Staff</b>	<i>Minimum number of staff, knowledge and skills required, what are the alternative staffing arrangements.</i>

<b>Accommodation</b>	<i>Desk space. Home working etc.</i>
<b>Agreed Alternative Accommodation Arrangements</b>	<i>Address, contact name, telephone number, access restrictions, key holders.</i>
<b>Systems (IT and comms)</b>	<i>Back up/recovery processes. Network connection, telephone access required etc.</i>
<b>Hard Data</b>	<i>Files, paperwork, where are they stored, alternative locations for storage.</i>
<b>Key Suppliers</b>	<i>Check their continuity arrangements, alternative suppliers etc.</i>
<b>Other</b>	

## 8. Contact Details

*For all key stakeholders, staff and suppliers involved in the plan.*

### Staff

Name	Job Title	Contact Details	Home location/walk to work?

### Stakeholder

Name	Role	Contact Details

### Supplier Contacts

Name	Role	Contact Details

### Other Useful Contacts

Name	Role	Contact Details

*Appendix A – Damage Assessment Form*

<b>Description of Damage</b>	<b>Identified By</b>	<b>Time/Date Identified</b>	<b>Actions</b>