Final Distribution

Insurance and Risk Manager
Strategic Risk and Business Continuity Manager
Risk and Business Continuity Officers

cc: Corporate Director Finance & Risk Management
    Head of Audit and Risk Management

Geoff Barlow – Interim Audit Services Manager
Minashi Patel – Auditor

MAY 2009
EXECUTIVE SUMMARY

1 INTRODUCTION

1.1 Background
Milton Keynes Council's Risk and Business Continuity Team’s aim is to improve the effectiveness of risk management and business continuity management across the council.

Effective Risk and Business Continuity Management ensures that we are able to:

- closely analyse activities and behaviours and so discover solutions and improvements and achieve organisational learning.
- Focus on agreed priorities ensuring we get the right balance between rewards and risks.
- Manage uncertainty by constraining threats to acceptable levels and responsibly developing opportunities.
- Develop better information to support improved decision-making.

Under the Civil Contingencies Act 2004 Local Authorities (LAs) are ‘Category One Respondants’ which means that LAs have to be able to continue their essential services through and beyond a threatened disruption or disruptive incident by Business Continuity Planning.

Advice and assistance needs to be given to local businesses about possible threats to their organisations and the need for and how to plan for Business Continuity.

On 22nd April Strategic RISK awards announced the winners and finalists for the 2010 European Risk Management Awards. The awards focus on supporting the European risk management community by promoting best practice, excellence and innovation. Milton Keynes Council, Risk and Business Continuity Team were finalists in four categories including European Risk management Team of the Year and won the award for the Best Risk Communication of the Year.

The team was a finalist for CIR Business Continuity Team Award 2010.

1.2 Objectives and Scope
The objectives of the audit were to ensure that:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>Budgets are effectively monitored. (Finance)</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td>b)</td>
<td>Relevant legislation is adhered to. (Law)</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
c) Council policy/strategies are adhered to (Policy)  

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

d) Risks are continuously identified and managed (Risk)  

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

e) Service improvement is considered (Service Improvement)  

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Key: 1 = Poor, 3 = Good

ICT Disaster Recovery, Emergency Planning and Risk Management are separate audits.

2 **AUDIT OPINION**

**Satisfactory** – Controls are considered adequate with some areas of weakness that are not major risk areas.
3 CONCLUSIONS

3.1 Over the last 12 months the Risk and Business Continuity Team have been focused on achieving Basic Business Continuity plans across the council. Full Business Continuity Plans have been carried out for a number of services, however, not all Essential services have a Full Business Continuity Plan.

3.2 The main concern of the audit is that the some services do not have a Business Continuity plan and that some plans were not readily accessible to their staff.

3.3 Some Business Continuity plans are exercised and the feedback from staff has been positive. Over 90% of staff who attended the exercises have been pleased with the learning and were going to improve their plans in some way.

3.4 Only 2 directorates have a Business Continuity Planning Champion of which one is under review and one is proactive. All directorates should have a Business Continuity Planning Champion that would be responsible for co-ordinating plans across their Directorate.

4 WAY FORWARD

4.1 All recommendations are in the Management Action Plan (Page 6). Good controls are shown in section 5, overleaf.

4.2 Business Continuity Plan owners should ensure that their plans are up to date, and contacts are reviewed quarterly. The plan should be easily accessible and communicated to all members of staff on a regular basis. It should be agreed and signed off by the Director and Risk and Business Continuity team.

4.3 All staff members should be made aware of their Business Continuity Plans and be able to access and operate them with or without the presence of the plan owner.

4.4 Full Business Continuity Plans should be developed for all Essential Services.

4.5 Risks entered onto the corporate system Grace which are to be treated or have a high residual risk score should have clear documented actions to mitigate risks.

4.6 All directorates should have a Business Continuity Planning Champion.

4.7 Work should be undertaken to ensure that all critical suppliers are resilient.
FINDINGS SUMMARY

5 FINDINGS

5.1 Finance
Regular budget monitoring is undertaken.

5.3 Law
5.4 Civil Contingencies Act 2004 is mandatory for Local Authorities. We should promote Business Continuity internally and externally in the local community. The Council have set up the Milton Keynes Business Resilience Forum to help with their resilience.

5.5 The Forum exists to help local businesses and voluntary organisations to improve resilience. The forum is an informal association of people from local organisations, led by MK Council that provides a support network to the local community and runs events.

5.6 The Risk and Business Continuity Team have set up a tool kit website which also supports the business of the forum and promotes resilience.

5.7 Essential services have been identified across the council. All Essential services have Basic Business Continuity Plans and critical components of all services are being protected with Full service plans.

5.8 Core Plans are also being developed to cover key cross organisational services for example ICT, Facilities, Human Resources and Communications,

5.9 Policy
5.10 The Risk Management and Business Continuity Management Strategy was approved on the 23rd March 2010. A copy can be found on the intranet. Audit testing was carried out on the approved strategy as the previous one was dated 2006.

5.11 Training is offered by the Risk and Business Continuity team on an individual and team basis as required, to support the development of Business Continuity plans and to exercise Business Continuity Teams in the use of their plans.

5.12 4 Business continuity exercises have recently been held involving 13 plans. Attendees experienced an incident with interactive telephone calls from someone role playing for example a staff member outside the incident, reporters, staff panicking trying to make the incident as realistic as possible.
The exercises went down well with 95% of attendees feeding back that they would be improving their plans in some way.

5.13 Within the new strategy all directorates should have a Business Continuity Planning Champion who is responsible for acting as the conduit between the directorate and the Risk & Business Continuity Team. Only 2 out of 5 directorates have a Business Continuity Planning Champion, of which one is proactive.

5.14 Audit Testing was carried out unannounced visits to Business Plan owners explaining there was an incident and that we need to leave the building with their Business Continuity plans. 52% (13/25) of plans were not readily available, with some held on the system only, locked in draws etc.

5.15 Reports are presented to Corporate Leadership Team and the Audit Committee on a regular basis.

5.16 **Risk**

5.17 Business Continuity Management (BCM) risk like all work streams BCM has assessed its risks. The risks are reported on the corporate system Grace: Mitigations included but are not fully mitigated by some service plans.

5.18 The Risk and Business Continuity team attend regular training to ensure that they are kept up to date.

5.19 Risk & Business Continuity Team undertakes regular training with service users to ensure that their plans are developed.

5.20 Team have a professional relationship with other bodies for example BCI Partnership, Emergency Networks etc.

5.21 CCA requirement: Under the Civil Contingency Act 2004 the Council is obliged to conduct annual threats assessments. Threats have been assessed and entered onto the corporate system Grace as a reference.

5.22 **Service improvement**

5.23 The Business Continuity team issue a Risk and Reward newsletter on a regular basis to all staff.

5.24 Plans are exercised which are based on specific scenarios with the aid of providing the teams with opportunity to improve and validate their resilience plans. The exercises simulate the actions and decisions that would be experienced during a real incident.

5.25 Training is offered for Business Continuity as required.

5.26 BC Team are building a response structure which locates the primary response at operational plan level supported by BC Support Teams, and a corporate wide BC Coordination Group should a corporate wide incident occur.
# MANAGEMENT ACTION PLAN

The recommendations are categorised on the following basis:

- **Essential** - Implementation is required with immediate effect to address a weakness that fundamentally undermines the control/objective of that system.
- **Important** - Implementation is required within a short period of time to address weaknesses that seriously undermine the control/objective of that system.
- **Standard** - Management need to take recommended action within a reasonable period to address weaknesses that may undermine controls/objectives.

<table>
<thead>
<tr>
<th>Ref</th>
<th>Findings</th>
<th>Risk/ Implication</th>
<th>Agreed Actions</th>
<th>Management Comments</th>
<th>Manager Responsible &amp; Target Date</th>
</tr>
</thead>
</table>
| 1   | Risk     | Some services may not be effectively protected by Business Continuity plans. | **Essential**  
Outstanding core plans should be completed and where required exercised.  
ICT should evidence that the core Business Continuity Plan meets the requirement to mitigate the risk.  
Some critical components of other plans will need to be completed. | Agreed  
This is an on going process and one target date will not achieve the required actions. | ICT manager to be Coordinated by Strategic Risk and Business Continuity Manager  
To coordinate  
Reviewed by 1/9/10 and part exercised by 1/11/10  
Grace to be updated routinely. |
<table>
<thead>
<tr>
<th>Ref</th>
<th>Findings</th>
<th>Risk/ Implication</th>
<th>Agreed Actions</th>
<th>Management Comments</th>
<th>Manager Responsible &amp; Target Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Policy</strong>&lt;br&gt;A sample of Business Continuity plan owners were audit tested to see if they had access to their plans and if they were absent that another member of the team was aware and able to access it. The results of the testing revealed:-&lt;br&gt;52% (13/25) of BC plan owners could not find the plans or they were on the system only.&lt;br&gt;32% (8/25) of plans where information was missing/need to be completed.&lt;br&gt;28% (7/25) of BC plans for essential services seen, required further work for a full BC plan.&lt;br&gt;20% (5/25) of plans had been signed off by Directors.&lt;br&gt;With only 20% (5/25) of the BC owners having attended Business Continuity exercises.</td>
<td><strong>Important</strong>&lt;br&gt;Staff not aware of what is required if an incident was to occur.&lt;br&gt;Injury to staff&lt;br&gt;Loss of service.&lt;br&gt;Reputational loss of council.&lt;br&gt;Breach of Civil Contingency Act.</td>
<td>Agreed&lt;br&gt;Risk and Business Continuity Team to pro actively coordinate to all services across that :&lt;br&gt;Business Continuity Plan owners should make their plans easily accessible to their staff and communicate of its existence to all staff members on a regular basis.&lt;br&gt;All teams should have Basic Continuity Plans and Essential Services, and others with critical components should have Full Business Continuity Plans.&lt;br&gt;All plans should be agreed and signed off by their Director and a member of the Risk &amp; Business Continuity Team.&lt;br&gt;Plans should be reviewed annually, with contact details reviewed on a quarterly basis or following an exercise or live incident.&lt;br&gt;All plan owners should exercise their plans.</td>
<td>According to the table, the planning status is reviewed Monthly. The agreed actions are ongoing.</td>
<td><strong>Strategic Risk and Business Continuity Manager to co-ordinate across the council 30/11/10 all Essential Services BCP to have been exercised</strong>&lt;br&gt;Pro active intervention by Risk and Business Continuity Team 30/11/10</td>
</tr>
<tr>
<td>Ref</td>
<td>Findings</td>
<td>Risk/ Implication</td>
<td>Agreed Actions</td>
<td>Management Comments</td>
<td>Manager Responsible &amp; Target Date</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| 3   | **Policy**  
Only 40% (2/5) of directorates have a Business Continuity Planning Champion, of which one directorate has a temporary person and the other is proactive. | Management may have out of date information.  
Poor communication.  
Plans not effective.  
Slow development of Business Continuity Planning. | **Important**  
All directorates should have a Business Continuity Planning Champion as required by the agreed strategy. | Agreed | Strategic Risk and Business Continuity Manager 30/11/10 |
| 4   | **Policy**  
Business Continuity Plans have not been reviewed as required annually and staff contact details have not been updated quarterly. | Should an incident occur details may be incorrect.  
The correct person not contacted or incorrect action taken.  
Ineffective response. | **Important**  
Plans should be reviewed annually, with contact details reviewed on a quarterly basis or as an incident occur. | Agreed | Strategic Risk and Business Continuity Manager 31/8/10 bulletin to all plan owners and followed up by 30/11/10 |
<table>
<thead>
<tr>
<th>Ref</th>
<th>Findings</th>
<th>Risk/ Implication</th>
<th>Agreed Actions</th>
<th>Management Comments</th>
<th>Manager Responsible &amp; Target Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>Policy</strong>&lt;br&gt;There is little evidence that Business Continuity planning extends down the critical supply chain.&lt;br&gt;From a sample of audit testing carried out on our suppliers/contractors only 1/5 had Business Continuity plan in place which was verified. However further work was needed to make the plan more effective.&lt;br&gt;Another supplier confirmed they had a plan, however this was not verified as not provided to Internal audit.&lt;br&gt;2 other suppliers contacted however they failed to reply both to internal audit and the service users.&lt;br&gt;1 other supplier had given an action plan which was supposed to be the Business Continuity plan.&lt;br&gt;Not all contracts have a standard condition to include Business Continuity.</td>
<td><strong>Important</strong>&lt;br&gt;Reputational loss of council.&lt;br&gt;Loss of service to the council and customers.</td>
<td><strong>Agreed</strong>&lt;br&gt;Further work should be undertaken to ensure that our suppliers/contractors across the council have effective plans in place to mitigate any critical event.&lt;br&gt;Services should ensure that any new contract should provide for Business Continuity. Services should look to ensure that Business Continuity Plans are in place for existing contracts.&lt;br&gt;Risk and Business Continuity Team to liaise with the Legal Team to ensure that any new contracts include a clause relating to Business Continuity.</td>
<td><strong>Agreed</strong>&lt;br&gt;The requirement will be advised to Business Plan owners by email/newsletter and followed up on a priority basis.</td>
<td><strong>Strategy Risk and Business Continuity Manager</strong>&lt;br&gt;To coordinate across the council and liaise with Legal Team 30/11/10</td>
</tr>
<tr>
<td>Ref</td>
<td>Findings</td>
<td>Risk/ Implication</td>
<td>Agreed Actions</td>
<td>Management Comments</td>
<td>Manager Responsible &amp; Target Date</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>6</td>
<td><strong>Service Improvement</strong></td>
<td>Poor service provision. Performance is not effectively measured (and any under performance promptly identified and remedied)</td>
<td><strong>Standard</strong> Measures should be fully explored and exceptions examined to facilitate continuous improvement.</td>
<td>Agreed Measures are considered and discussed at regular team meetings.</td>
<td>Strategic Risk and Business Continuity Manager 30/11/10</td>
</tr>
<tr>
<td></td>
<td>At the moment the only measure in place is the feedback forms completed after an exercise. However, this is not followed through in terms of checking that plans have actually been changed. A debrief was undertaken and sent out after an exercise that was carried out in 2009.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><strong>Policy</strong></td>
<td>Lack of direction may lead to ineffective planning due to lack of engagement.</td>
<td><strong>Standard</strong> The strategy/policy should be reviewed on an annual basis. If no changes are needed it should be recorded that the review has taken place and that no changes are required.</td>
<td>Agreed</td>
<td>Strategic Risk and Business Continuity Manager 31/12/10 to begin reviewing the strategy.</td>
</tr>
<tr>
<td></td>
<td>Strategy/ policy approved recently prior to this the previous one was dated 2006.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB Any cost implications arising from implementation of the recommendations by Mouchel must be agreed in advance with the appropriate Client Officer and the Partnership Delivery Manager.