SLOUGH BOROUGH COUNCIL

Business Continuity

FINAL

Internal audit report: 1.16/17

30 June 2016

RSM

CONTENTS

Debrief held	10 June 2016	**Internal audit team**	Dan Harris – Head of Internal Audit
Draft report issued	21 June 2016		Chris Rising – Senior Manager
Responses received	30 June 2016		Amir Kapasi – Assistant Manager
			Habib Aidarus – Senior Auditor
Final report issued	30 June 2016	**Client sponsor**	Neil Aves – Assistant Director, Housing and Environment
		Distribution	Neil Aves – Assistant Director, Housing and Environment

1 EXECUTIVE SUMMARY

1.1 Background

An audit of Business Continuity was undertaken as part of the approved internal audit plan for 2016/17. The audit was designed to provide assurance over the Council's business continuity arrangements and whether business continuity plans were in place to facilitate the Council returning to business as usual in the event of an adverse incident, within appropriate and planned timescales.

Senior leadership responsibility for business continuity management rests with the Assistant Director, Housing and Environment. However, over the last couple of years, there has been a lack of dedicated business continuity resource within the Council, due to one member of staff leaving and another being on long-term sickness absence. As such, there has been a lack of consideration given to business continuity management, with arrangements last reviewed in July 2013 despite significant organisational changes in the interim.

1.2 Conclusion

Our audit has highlighted a lack of a robust framework for business continuity management within the Council. A lack of dedicated resource in this area over the last couple of years has resulted in a lack of attention being given to this important area. Business continuity arrangements have not been reviewed since July 2013 despite significant organisational changes. Furthermore, there were no arrangements for delivering business continuity management training to staff, while a formal group to continuously monitor and evaluate business continuity arrangements has not been in place for the last two years.

Internal Audit Opinion:

Taking account of the issues identified, the Council cannot take assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

Urgent action is needed to strengthen the control framework to manage the identified risk.
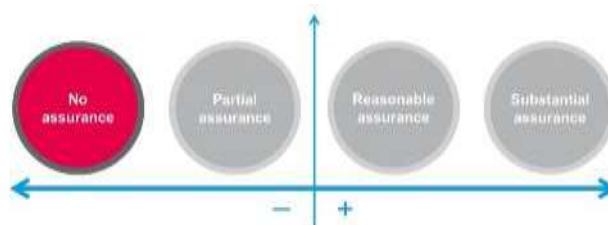
1.3 Key findings

The key findings from this review are as follows:

Business Continuity Management Policy

We identified that the Council did not have an overarching Business Continuity Management (BCM) Policy covering the framework for BCM in the organisation. While we noted elements of this had been covered in the Council's Business Continuity Plan (BCP), this was last reviewed in July 2013 and did not reflect current arrangements. As a result, the policy may not provide accurate and up to date guidance to staff on the BCM arrangements to be followed within the Council.

Without sufficient guidance on the Council's BCM framework being made accessible to staff, there is an increased risk of staff within the Council not preventing incidents or responding appropriately to incidents should they occur, potentially resulting in significant adverse effects on delivery of services. We have agreed a **high** priority management action in relation to this.

Business Impact Analysis (BIA) and Business Continuity Plans (BCP)

We noted business continuity arrangements were last reviewed in July 2013, and that the BIAs undertaken at the time and the Council's BCP no longer reflect the current arrangements, following significant structural changes within the Council. We also identified a lack of arrangements for testing the effectiveness of the BCP. Furthermore, there were also no separate Directorate or Service BCPs.

Without undertaking regular BIAs, which encompasses risk assessments, the Council may not be able to identify the arrangements and resources necessary to be able to appropriately respond to incidents which could impact on business continuity and the delivery of services. As a result, the lack of up-to-date BCPs, which are regularly tested for effectiveness, increases the risk of the Council not being able to respond appropriately to incidents impacting business continuity. This could potentially result in significant disruptions to delivery of services. We have agreed **two high** and one **medium** priority management actions to address these issues.

Roles and responsibilities

As we have already highlighted above, there has been a lack of dedicated business continuity resource within the Council over the last couple of years to oversee and coordinate the arrangements. As a result, there has been a lack of attention given to this area, resulting in significant control gaps as identified within this audit.

Without ensuring adequate resources are in place to support the business continuity agenda within the Council, a lack of sufficient attention being given to business continuity arrangements increases the risk of significant service disruption as a result of an inadequate response(s) to an incident, which could impact business continuity and services to the public. We have agreed one **high** priority management actions in relation to this issue.

Training

We confirmed that a formal programme of training for staff in relation to business continuity management had not been established. There is therefore a risk that staff will not attain the necessary knowledge and expertise to be able to appropriately respond to incidents which could have an impact on business continuity. A **medium** priority management action has been agreed in respect of this. The Council should consider the use of the Learning Pool software to enable the provision of this training.

Governance

We identified that a formal group with responsibility for continuously monitoring and evaluating business continuity arrangements within the Council has not been in place for the last two years. Without such a group, the Council is unable to ensure adequate monitoring and scrutiny of business continuity arrangements to assess its continuing suitability, adequacy and effectiveness. This increases the risk that adequate arrangements and resources may not be deployed to minimise disruption to services in the event of an incident impacting business continuity. We have agreed a **high** priority management action in respect of this.

1.4 Additional information to support our conclusion

The five high and two medium priority management actions agreed to address the issues identified are detailed within the action plan that follows in section two.

Risk	Control design*	Non-compliance with controls*	Agreed actions		
			Low	Medium	High
Failure to maintain a minimum level of service due to a major system failure.	6 (6)	0 (6)	-	2	5
Total			**-**	**2**	**5**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

2   ACTION PLAN

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The table below sets out the actions agreed by management to address the findings:

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
Risk: Failure to maintain a minimum level of service due to a major system failure.					
1	The Council did not have an overarching Business Continuity Management (BCM) Policy covering the framework for BCM in the organisation	High	The Council will develop an overarching Business Continuity Management (BCM) Policy covering the framework for BCM in the organisation. The policy will set out; • Scope, aims and objectives of BCM in the Council; • The Council's commitment to BCM; • The activities that will be required to deliver these; and • Roles and responsibilities of staff in relation to BCM. • Version control to state approval details and next planned review date. Once finalised, the policy will be subject to ratification by CMT and communicated to staff.	31August 2016	Neil Aves – Assistant Director, Housing and Environment

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
2	A Business Impact Analysis (BIA) was last undertaken in July 2013 and has not been reviewed and updated since.	High	The Council will establish and maintain a documented process for undertaking business impact analysis and risk assessments at Service, Directorate and Council-wide level that; • Establishes the context of the assessment and defines the criteria for evaluating the potential impact of a disruptive incident; • Takes into account legal and other commitments; • Includes systematic analysis and prioritisation of risk treatments; • Defines the required output from the business impact analysis and risk assessment; and • Specifies the requirements for this information to be kept up-to-date. The business impact analysis will include; • Identifying activities that support the provision of services; • Assessing the impacts over time of not performing these activities; • Setting prioritised timeframes for resuming these activities at a specified minimum acceptable level (RTO - Recovery Time Objective), taking into consideration the time within which the impacts of not resuming them would become unacceptable (MTPD - Maximum Tolerable Period of Disruption); and • Identifying dependencies and supporting resources for these activities, including suppliers and outsource partners. The risk assessment will include; • Identifying risks of disruption to the Council's prioritised activities and the processes, systems and resources that support them; • Systematically analysing risks in line with the Council's risk management methodology;	30 September 2016	Neil Aves – Assistant Director, Housing and Environment

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
			• Evaluating which risks require treatment/mitigation; and • Identifying treatments/mitigations in line with business continuity objectives and the Council's risk appetite. The processes will be documented within the Council's overarching Business Continuity Management Policy.		
3i	The Council's Business Continuity Plan (BCP) was last reviewed in July 2013 following the last BIA undertaken, and did not reflect current arrangements. In addition, there were also no separate Directorate or Service Business Continuity Plans.	High	Following finalisation of the Major Incident Plan, the document will be used to inform the development of the Council's Business Continuity Plan (BCP) as well as Directorate and Service BCPs. There will be a clear linkage between Directorate and Service BCPs and the Council's overall BCP. Each of these BCPs will define; • Purpose, scope and objectives; • Defined roles and responsibilities during and following an incident potential affecting business continuity; • The criteria and procedures for activating a response to such incidents; • The detailed procedures for implementing the response, including details to manage the immediate consequences; • The location(s) from which the response is to be coordinated; • Contents and storage location of the battlebox (response pack) and details of where vital backup computer data and any critical paper records are stored; • Communication requirements and procedures, including details of media response and how and under what circumstances the organisation will communicate with employees, key parties and emergency contacts; • Emergency contact arrangements, including list of key customers, suppliers, third parties and their contact details;	30 September 2016	Neil Aves – Assistant Director, Housing and Environment

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
			• Internal and external interdependencies and interactions between the Council and its stakeholders; • Resource requirements; • Information flows within the Council and processes for documenting actions taken as part of the response; and • Stand-down procedure once incident is resolved. Once finalised, the BCPs will be subject to formal approval by CMT and reviewed regularly thereafter. Version control will be included within each BCP to state approval details; next planned review date and the requirement to review these in the event of a major structure change or where lessons learnt are identified after an exercise or real event.		
3ii	We also identified a lack of arrangements for testing the effectiveness of the BCP.	Medium	A formal and documented process will be established, implemented and maintained for exercising and testing business continuity procedures in order to assess their effectiveness. This will be documented within the Council's overarching Business Continuity Management Policy. A testing schedule will be defined for the Council BCP as well as the Directorate and Service BCPs which details the intervals at which each element of these will be tested. Exercises/tests will; • Be based on appropriate scenarios with clearly defined aims and objectives to minimise the risk of disruptions; and • Produce formalised post exercise reports that contain outcomes and lessons learnt, recommendations and actions to implement improvements.	31 October 2016	Neil Aves – Assistant Director, Housing and Environment

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
4	There has been a lack of dedicated business continuity resource within the Council over the last couple of years to oversee and coordinate arrangements	High	The Council will review the current staffing resources in relation to business continuity to ensure sufficient resources are in place to appropriately oversee business continuity arrangements.	30 June 2016	Neil Aves – Assistant Director, Housing and Environment
5	A formal programme of training for staff in relation to business continuity management had not been established.	Medium	A formal programme of business continuity training will be developed and delivered to staff covering, but not limited to; • The Council's overarching Business Continuity Management (BCM) Policy; • The roles and contributions of staff to the effectiveness of BCM within the Council; and • The implications of non-conformance with the policy.	31 October 2016	Neil Aves – Assistant Director, Housing and Environment
6	We identified that a formal group with responsibility for continuously monitoring and evaluating business continuity arrangements within the Council has not been in place for the last two years.	High	A formal group will be established to oversee the Council's business continuity agenda. The group's remit will be defined within Terms of Reference which will include; • Responsibilities; • Membership and quoracy; • Meeting frequency; and • Accountability and reporting.	30 June 2016	Neil Aves – Assistant Director, Housing and Environment

3 DETAILED FINDINGS

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
Risk: Failure to maintain a minimum level of service due to a major system failure.						
1	The Council does not have a separate overarching Business Continuity Management (BCM) Policy covering the framework for BCM in the organisation. This is covered within the Council's Business Continuity Plan (BCP), however it was last reviewed in July 2013 and does not reflect current arrangements, and thus requires updating. It is therefore not accessible to staff.	No	N/A	In line with best practice guidance, organisations must agree and document a BCM policy which sets out; • Scope, aims and objectives of BCM in the organisation; • The organisation's commitment to BCM; • The activities that will be required to deliver these; and • Roles and responsibilities of staff in relation to BCM. We identified through discussion with the Assistant Director, Housing and Environment that the Council did not have a separate, overarching Business Continuity Management (BCM) Policy covering the above. We were provided with a copy of the Council's Business Continuity Plan (BCP), which was dated July 2013 and were informed by the Assistant Director, Housing and Environment that this was out-of-date and required updating. The document was therefore not accessible to staff. Through review of the BCP, while we confirmed it covered the above areas, it did	High	The Council will develop an overarching Business Continuity Management (BCM) Policy covering the framework for BCM in the organisation. The policy will set out; • Scope, aims and objectives of BCM in the Council; • The Council's commitment to BCM; • The activities that will be required to deliver these; and • Roles and responsibilities of staff in relation to BCM. • Version control to state approval details and next planned review date. Once finalised, the policy will be subject to ratification by CMT and communicated to staff.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
				not reflect current arrangements. Furthermore, there is a clear distinction between the BCP and BCM policy as the BCM policy sets out the overarching framework while the BCP details the arrangements for responding to and dealing with incidents affecting business continuity. The Council should therefore develop a separate, overarching policy which would cover the above areas in line with best practice, to ensure the Council's BCM framework is clearly signposted to staff. Without sufficient guidance on the Council's BCM framework being made accessible to staff, there is an increased risk of staff within the Council not responding appropriately to incidents, potentially resulting in significant adverse effects on delivery of services.		
2	A Business Impact Analysis (BIA) was last undertaken in July 2013 and has not been reviewed and updated since. A BIA report was produced for each of the four Council directorates, to identify those areas and services whose loss would have the greatest impact on the Council and would therefore need to be recovered quickest.	No	N/A	The Business Impact Analysis (BIA) is a key element of BCM and the foundation work from which the whole process is built. However, we confirmed through discussion with the Assistant Director, Housing and Environment that a BIA has not been undertaken since July 2013. We were provided with the BIA reports produced following the BIA undertaken in 2013, and were informed by the Assistant Director, Housing and Environment that these needed to be reviewed and updated following significant structural changes	High	The Council will establish, implement and maintain a formal and documented process for undertaking business impact analysis and risk assessments at Service, Directorate and Council-wide level that; • Establishes the context of the assessment and defines the criteria for evaluating the potential impact of a disruptive incident; • Takes into account legal and other commitments; • Includes systematic analysis and prioritisation of risk treatments; • Defines the required output from the business impact analysis and risk assessment; and

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
	The reports state that these are to be reviewed annually, where there is a major structure change or where lessons learnt are identified after an exercise or real event.			within the organisation. We reviewed the format of the reports to assess whether these captured the necessary information in line with guidance. While we found that overall, the report covered the relevant areas in respect of BIA, we noted it did not capture risk assessments of critical activities/services. We also noted the reports had not been fully completed. Without undertaking regular BIAs, which encompasses risk assessments, the Council may not be able to identify the arrangements and resources necessary to be able to appropriately respond to incidents which could impact on business continuity and the delivery of services.		• Specifies the requirements for this information to be kept up-to-date. The business impact analysis will include; • Identifying activities that support the provision of services; • Assessing the impacts over time of not performing these activities; • Setting prioritised timeframes for resuming these activities at a specified minimum acceptable level (RTO - Recovery Time Objective), taking into consideration the time within which the impacts of not resuming them would become unacceptable (MTPD - Maximum Tolerable Period of Disruption); and • Identifying dependencies and supporting resources for these activities, including suppliers and outsource partners. The risk assessment will include; • Identifying risks of disruption to the Council's prioritised activities and the processes, systems and resources that support them; • Systematically analysing risks in line with the Council's risk management methodology; • Evaluating which risks require treatment/mitigation; and • Identifying treatments/mitigations in line with business continuity objectives and the Council's risk appetite. The processes will be documented within the Council's overarching Business Continuity Management Policy.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
3	The Council's Business Continuity Plan (BCP) was last reviewed and updated in July 2013. The BCP needs to be reviewed and updated following significant structural changes within the organisation, and is therefore currently not accessible to staff. There are no separate Directorate or Service Business Continuity Plans. A Major Incident Plan is currently being developed in conjunction with an external facilitator, which will subsequently inform the updating and development of the Council's Business Continuity Plan.	No	N/A	We confirmed through discussion with the Assistant Director, Housing and Environment that the Council's BCP was last reviewed in July 2013 following the last BIA undertaken, and did not reflect current arrangements. We also identified a lack of arrangements for testing the effectiveness of the BCP. In addition, there were also no separate Directorate or Service Business Continuity Plans. We were informed that a Major Incident Plan was currently being developed in conjunction with an external facilitator, and once finalised, this would subsequently inform the development of the Council's BCP as well as Directorate and Service BCPs. Nevertheless, the lack of up-to-date BCPs, which are regularly tested for effectiveness, increases the risk of the Council not being able to respond appropriately to incidents impacting business continuity. This could potentially result in significant disruptions to delivery of services.	High	Following finalisation of the Major Incident Plan, the document will be used to inform the development of the Council's Business Continuity Plan (BCP) as well as Directorate and Service BCPs. There will be a clear linkage between Directorate and Service BCPs and the Council's overall BCP. Each of these BCPs will define; • Purpose, scope and objectives; • Defined roles and responsibilities during and following an incident potential affecting business continuity; • The criteria and procedures for activating a response to such incidents; • The detailed procedures for implementing the response, including details to manage the immediate consequences; • The location(s) from which the response is to be coordinated; • Contents and storage location of the battlebox (response pack) and details of where vital backup computer data and any critical paper records are stored; • Communication requirements and procedures, including details of media response and how and under what circumstances the organisation will communicate with employees, key parties and emergency contacts; • Emergency contact arrangements, including list of key customers, suppliers, third parties and their contact details; • Internal and external interdependencies and interactions between the Council and its

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
						• stakeholders;
						• Resource requirements;
						• Information flows within the Council and processes for documenting actions taken as part of the response; and
						• Stand-down procedure once incident is resolved.
						Once finalised, the BCPs will be subject to formal approval by CMT and reviewed regularly thereafter.
						Version control will be included within each BCP to state approval details; next planned review date and the requirement to review these in the event of a major structure change or where lessons learnt are identified after an exercise or real event.
					Medium	A formal and documented process will be established, implemented and maintained for exercising and testing business continuity procedures in order to assess their effectiveness. This will be documented within the Council's overarching Business Continuity Management Policy.
						A testing schedule will be defined for the Council BCP as well as the Directorate and Service BCPs which details the intervals at which each element of these will be tested.
						Exercises/tests will;
						• Be based on appropriate scenarios with clearly defined aims and objectives to minimise the risk of disruptions; and
						• Produce formalised post exercise reports that contain outcomes and lessons learnt, recommendations and actions to implement improvements.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
4	There is currently no dedicated business continuity resource within the Council.	No	N/A	We were informed by the Assistant Director, Housing and Environment that, due to the long-term absence of the Business Continuity and Response Manager since December 2014, there was currently no dedicated business continuity resource within the Council. Without ensuring adequate resources are in place to support the business continuity agenda within the Council, sufficient attention may not be given to business continuity arrangements. This increases the risk of significant service disruption as a result of an inadequate response to an incident impacting business continuity.	High	The Council will review the current staffing resources in relation to business continuity to ensure sufficient resources are in place to appropriately oversee business continuity arrangements.
5	The Council has not established a formal programme of training for staff in relation to business continuity management.	No	N/A	We were informed by the Assistant Director, Housing and Environment that a formal programme of training for staff in relation to business continuity management had not been established. There is therefore a risk that staff will not attain the necessary knowledge and expertise to be able to appropriately respond to incidents which could have an impact on business continuity.	Medium	A formal programme of business continuity training will be developed and delivered to staff covering, but not limited to; • The Council's overarching Business Continuity Management (BCM) Policy; • The roles and contributions of staff to the effectiveness of BCM within the Council; and • The implications of non-conformance with the policy.
6	A formal group to continuously monitor and evaluate business continuity arrangements within the Council is not in place.	No	N/A	We confirmed through discussion with the Assistant Director, Housing and Environment that a formal group with responsibility for continuously monitoring and evaluating business continuity arrangements within the Council was currently not in place.	High	A formal group will be established to oversee the Council's business continuity agenda. The group's remit will be defined within Terms of Reference which will include; • Responsibilities; • Membership and quoracy;

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
				Without such a group, the Council is unable to ensure adequate monitoring and scrutiny of business continuity arrangements to assess its continuing suitability, adequacy and effectiveness. This increases the risk that adequate arrangements and resources may not be deployed to minimise disruption to services in the event of an incident impacting business continuity.		• Meeting frequency; and • Accountability and reporting.

APPENDIX A: SCOPE

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risk:

Objective of the area under review	Risks relevant to the scope of the review	Risk source
To ensure Business Continuity arrangements are in place, regularly tested and effective.	Failure to maintain a minimum level of service due to a major system failure.	Corporate Risk Register (**Risk ORG0045)**

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

This audit aimed to provide assurance over the Council's Business Continuity arrangements and included consideration of:

- How Business Impact Assessments are completed and reviewed.

- Whether a Council-wide Business Continuity Plan has been developed that includes arrangements for responding to major incidents which could impact on business continuity, and how this has been communicated to all staff.

- Whether individual Business Continuity Plans have been developed at Directorate and Service level, and their approval and link to the Council's overall Business Continuity Plan.

- How Business Continuity Plans are monitored throughout the year.

- Whether the Business Continuity Plans are linked to the plans of Slough's other public sector providers such as the Police, Fire and NHS.

- Whether roles and responsibilities have been clearly documented within job descriptions in relation to business continuity.

- If leads have been identified at Directorate and Service level for co-ordinating the response of the Council.

- Whether a group has been established to review business continuity within the organisation and whether plans have been tested and the results reported to CMT or equivalent.

Limitations to the scope of the audit assignment:

- This review did not focus on the IT aspect of Business Continuity as this was covered as part of a separate review within the 2015/16 internal audit plan.

- The audit does not provide full assurance over the entire business continuity operations of the Council.

- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Neil Aves – Assistant Director, Housing and Environment

Benchmarking

We have included some comparative data to benchmark the number of management actions agreed, as shown in the table below. In the past year, we have undertaken a number of audits of a similar nature in the sector.

Level of assurance	Percentage of reviews	Results of the audit
Green (substantial assurance)	20%	
Amber (partial assurance)	30%	
Amber/Red (partial assurance)	40%	
Red (no assurance)	10%	X
Management actions	**Average number in similar audits**	**Number in this audit**
	5	7

FOR FURTHER INFORMATION CONTACT

Chris Rising

Senior Manager

Chris.Rising@rsmuk.com

Tel: 07768 952380

Amir Kapasi

Assistant Manager

Amir.Kapasi@rsmuk.com

Tel: 07528 970094

rsmuk.com