Internal Audit

Information Technology Disaster Recovery
March 2016

Distributed to:

Chief Operating Officer
Head of Information Management
Emergency Planning and Business Continuity Manager
Programme Director and Acting ICT Director (CSG)
Operations Director (CSG)
Service Delivery Manager (CSG)
Operations Manager (CSG)

	No	Limited	Satisfactory	Substantial
Audit Opinion				

1. Executive Summary

Introduction

As part of the 2015/16 Internal Audit Plan, agreed by the Audit Committee in April 2015, we have undertaken a review of the Information Technology Disaster Recovery (ITDR) programme.

Background & Context

An ITDR programme is the IT component of the wider Business Continuity Management (BCM) programme, which fulfills part of the Council's obligations to the public and Civil Contingencies Act in the event of a major incident. The purpose of the programme is to recover IT services that underpin Council activities, within an agreed time and to a point in time prior to the outage, to prevent an unacceptable business impact. ITDR in a modern IT environment has also to consider other supporting IT services, which whilst not directly important to the business, are essential to those that are.

At Barnet, the technical component of the ITDR programme has been outsourced to Capita as part of the Customer Support Group (CSG) contract. As part of the contract with Capita, IT services have, with the exception of the Council's internal telephone system, been migrated to a new data centre. As part of the migration, IT services were either replaced or re-platformed so they would be easier to maintain and be more resilient. With respect to ITDR, Capita were to implement a new capability at a secondary data centre that would meet the Council's recovery requirements. Prior to implementation, Capita were to maintain an interim ITDR solution which, whilst not capable of recovering services fully in line with requirements, would provide a fallback position.

Corporate objectives and risks

This audit supports all four of the strategic objectives in the Corporate Plan 2015 –2020:

The Council, working with local, regional and national partners, will strive to ensure that Barnet is a place:

1. of opportunity, where people can further their quality of life;
2. where people are helped to help themselves, recognising that prevention is better than cure;
3. where responsibility is shared, fairly; and
4. where services are delivered efficiently to get value for money for the taxpayer.

Scope

As part of our work, we performed a review of:

- The obligations of Capita with respect to ITDR provision;
- The scope of the ITDR project for the secondary data centre;
- The governance of the ITDR programme; and
- Existing ITDR capabilities.

Key Findings summary (informing the Audit opinion)

This audit has identified four priority 1 recommendations. We identified the following issues as part of the audit:

- **Governance -** There is a quarterly Business Continuity Management ("BCM") team meeting which governs BCM activities. It was noted that whilst Capita representatives do attend, those with the specific responsibility for ITDR have not been identified by Capita and consequently are not invited. We also noted that the meeting primarily deals with the BCM programme and ITDR is not routinely discussed. Finally, whilst Capita do provide a service report which includes high level ITDR status, it is primarily to demonstrate meeting KPI's and PI's and there is no detail with respect to ITDR capability, either planned or interim. We reviewed the format of the service report and noted that the report does not reflect the true ITDR risk exposure of the Council. The risk is that without including ITDR in BCM governance and having an accurate view of its status, management will not be able to address any shortfall in capability. **(Finding 2.1, priority 1)**

- **Alignment of BCM requirements with ITDR capability -** The Council's ITDR recovery requirements are described in the contract with Capita. It was noted that the requirements detailed in the contract are not those that are being delivered by the ITDR project. In particular, the Council applications are rated as platinum, gold, silver or bronze based on an assessment of the business impact. Applications rated as Silver and Bronze, are supposed to be recovered within 48 hours with a maximum of an hour of data loss. The current project is not delivering ITDR for Bronze applications and the current provision is to restore Silver rated applications within 96 hours with up to a day's worth of data loss. There are similar inconsistencies at Platinum and Gold level. **(Finding 2.2, priority 1)**

- **ITDR technical recovery capability -** Following on from the issue above, the technical provision will not cover the contractual requirements for ITDR. Additionally the technical approach has not considered interdependencies between IT applications. This means that there is a risk that an application may not function when other applications that it is dependent on are also not recovered. Finally, the recovery capability which would be provided through this arrangement would restore an infrastructure which may not be able to support the number of users the Council requires. **(Finding 2.3, priority 1)**

- **Interim ITDR capability -** Prior to the new ITDR capability being implemented at the secondary data centre, we confirmed that an Interim ITDR capability was in place. This was initially a ship to site "data-centre" that contained infrastructure for the Council's legacy systems. These services were procured from an external supplier by Capita but the contract for these services lapsed in early 2015 and was not renewed. Capita are currently replicating data to the secondary site and taking backups in preparation for the new full ITDR capability, now due in Q1 2016. However, these back- ups cannot be used to restore capability as they have not been tested and there are no documented ITDR plans in place. It was noted that there is currently no alternative interim capability. **(Finding 2.4, priority 1)**

For the detailed issues and recommendations please see section 2.

Limitation of scope

This review focused on Disaster Recovery Planning only. Business continuity planning (BCP) was the subject of a separate internal audit review earlier in the year and was not covered here. Emergency planning was also outside of the scope of this review.

Area of Scope	Adequacy of Controls	Effectiveness of Controls	Number of Recommendations Raised		
			Priority 1	Priority 2	Priority 3
Governance (see 2.1)			1	0	0
Business requirements (see 2.2)			1	0	0
Contract specification (see 2.2, 2.3, 2.4)			1	0	0
Proposed DR solution (see 2.3)			1	0	0

Acknowledgement	We would like to thank the CSG IT team and the Information Management team for their time and co-operation during the course of the internal audit.
To note	However, we would also like to note that during the course of the audit we encountered significant delays in receiving relevant information and being able to speak to the appropriate staff within CSG IT. The initial discussions around the audit were held in April 2015. The terms of reference for the review was not, however, agreed with CSG IT until September 2015. Delays were then suffered around gaining access to the right people and receiving the requested information. Ultimately a large amount of information was provided in late December 2015, hence this report has been issued in Quarter 4 as opposed to Quarter 1 as planned.

2. Detailed issues and recommendations

Note: the relevant Terms of Reference scope area is indicated in brackets after each aspect of the recommendation

2.1 ITDR Governance

P	Detailed finding	Risk	Recommendation
1	Whilst there is a quarterly Business Continuity Management ("BCM") team meeting which governs BCM activities and Capita staff do attend, those responsible for ITDR have not been identified and therefore do not attend. Additionally the meetings are primarily aimed at BCM programme issues and do not include ITDR status, which means that management are not necessarily aware of the extent of the capability or issues associated with it. Finally, whilst Capita do provide a service report which includes high level ITDR status, however it is primarily to demonstrate meeting KPI's and PI's and there is no detail with respect to ITDR capability, either planned or interim . We reviewed the format of the service report and noted that the report does not reflect the true ITDR risk exposure of the Council. As an example, the probability of an ITDR event is rated as low (less than 2%) with an impact of medium, giving the overall risk a green status. Whilst the probability rating is arguably correct, in our experience the impact of the Council losing its ITDR capability for an extended period of time would be high. The service report has no	• Appropriate governance arrangements may not have been established with regards to disaster recovery to ensure the ITDR capability can support the wider BCM programme. • Clear oversight and escalation may not be established which is supported by accurate, complete and timely management information resulting in issues not being identified, investigated and rectified. • The Council may not have a clear view of the ITDR capability and its residual risk.	**Recommendation 1** a) Governance of BCM should formally include Capita staff who are responsible for ITDR. These individuals should be identified by Capita and then invited on a standing basis (Governance) b) The BCM quarterly meeting should include formal ITDR discussion we with respect to a) business alignment b) capability c) status d) issues e) residual risk c) Capita should immediately engage the Council management and agree the level of reporting information required with respect to the ITDR capability. This should include as a minimum a) ITDR capability in terms of IT services in scope, Recovery Time Objective (RTO), Recovery Point Objective (RPO) and capacity, b) residual risk, c) planned tests, d) the test results and remedial actions and d) ITDR capability changes. (Governance) d) Management should update governance policies, terms of references and processes to reflect the above. (Governance)

	further detail with respect to scope, testing and gaps.		

Management Response	Responsible Officer	Deadline
Capita will nominate those people responsible for ITDR and the Council will invite them to the relevant BCM meetings. The governance documentation will be updated to reflect any changes. Capita will engage with the Council and internal audit and make sure the reporting gives the Council sufficient oversight of the delivery of the ITDR plan.	a) IS Security Manager (CSG) b) Emergency Planning and Business Continuity Manager (LBB) c) Operations Manager (CSG) d) Emergency Planning and Business Continuity Manager (LBB)	30 April 2016 30 April 2016 30 April 2016 30 April 2016

2.2 Alignment of BCM recovery requirements with ITDR capability

P	Detailed finding	Risk	Recommendation
1	The Council's initial ITDR recovery requirements were described in the Information Systems method statement (4 Mar 2013) which forms part of the contract with Capita. In line with the contractual obligations, on an annual basis, Capita and the Council should review the recovery requirements and update the relevant documentation as necessary. We reviewed the Capita contract and noted the ITDR recovery requirements which were initially	ITDR arrangements may be in place which are not aligned to contractual agreements which may result in significant business disruption where incidents occur and services cannot be restored in line with the Council's requirements.	**Recommendation 2** a) The programme teams should confirm who is responsible for reviewing the scope of the IT services included within ITDR. The responsible party should review the scope and the current ratings and engage Capita with respect to any required changes which should be provisioned as part of the ITDR project. (Business requirements) b) Capita should immediately engage the

	agreed. These were compared with the current arrangements being delivered in practice. It was noted that the requirements detailed in the contract are not those that are being delivered by the ITDR project. In particular, the Council applications are rated as platinum, gold, silver or bronze based on an assessment of the business impact. In line with the contract, applications rated as Silver and Bronze, are supposed to be recovered within 48 hours with a maximum of an hour of data loss. The current project is not delivering ITDR for Bronze applications and the current provision is to restore Silver rated applications within 96 hours with up to a day's worth of data loss. There are similar inconsistencies at Platinum and Gold level, however Capita have stated that the project document has been completed incorrectly and the technology being deployed will meet requirements (See Finding 2.3). Finally, the ITDR project did not engage the BCM team with respect to the intended ITDR capability. This means that the Council have not been able to incorporate any recovery requirement changes or be in a position to challenge the intended capability.		Council to ensure that the recovery bandings, i.e. platinum, gold, silver and bronze, are being delivered as per the contractual agreement. Where not, Capita should provision as part of the project. (Contract Specification) c) In line with the governance finding (Recommendation 1) above, the BCM programme should engage with those in Capita responsible for ITDR on a defined and regular basis to ensure changes in recovery requirements are provisioned for. (Business requirements)	
Management Response			**Responsible Officer**	**Deadline**

The current ITDR solution in operation is correct but the capacity document is incorrect and has been updated since the testing date. The last update was made on14/12/2015 but was not provided to audit. The method statement includes no implementation statement. This will be incorporated into the next version of the document. The Council and Capita will also engage to assess the appropriateness of the banding of each of the systems and applications in the method statement.	a) Emergency Planning and Business Continuity Manager (LBB) b) Operations Manager (CSG) Programme Director and Acting ICT Director (CSG) c) Emergency Planning and Business Continuity Manager (LBB)	a) With immediate effect b) With immediate effect c) 30 April 2016

2.3 ITDR planned technical recovery capability

P	Detailed finding	Risk	Recommendation
1	There is infrastructure technical recovery capability in place, for Platinum and Gold applications in scope that provides a good basis for recovery. Silver and bronze applications do not have recovery infrastructure immediately available. For silver, recovery infrastructure would be installed at the recovery site following ITDR invocation. There is currently no intent to do the same for bronze. Additionally, the recovery infrastructure for Platinum, Gold IT and Silver services is less capable than that enjoyed normally and is sized to support 2500 users. It is not clear if this is	Following an invocation, IT services that the Council requires from a business continuity perspective, will not function as expected or at all and may not be capable of supporting the required number of Council employees.	**Recommendation 3** a) In line with the recovery requirements recommendation above (Recommendation 2), Capita should immediately engage with the Council to ensure the required infrastructure is provided to meet recovery requirements and expected user numbers. (Contract specification) b) The ITDR project should identify end to end IT service dependencies that should be taken into account in provisioning and planning. This may mean that IT services that are not currently in scope have to be provisioned to support ones that are in

	sufficient to support the Council's operations and how long this limitation would be in place. Finally the current Capita approach has not taken IT application interdependencies into account, particularly between recovery tiers, for example, Silver and Gold. This means whilst individual applications may be recovered, they may not function as expected if supporting applications are not present. This gap was acknowledged during the review by Capita.		scope and have a critical dependency. It may also mean that IT services have to be promoted in terms of tiering to ensure successful recovery. (Proposed ITDR solution)

Management Response	Responsible Officer	Deadline
There is now infrastructure in place to support silver and bronze applications, although this has not been validated by the Council at the reporting date. It should be noted that the capability of the recovery arrangements to support 2500 users is the contractual requirement. An interdependency grid of platinum and gold systems has also been developed since the testing date. The responsibility for maintaining this as part of 'Business as Usual' will fall to the Applications team.	a) Operations Manager (CSG) Programme Director and Acting ICT Director (CSG) b) Applications team, CSG	a) With immediate effect b) 30 May 2016

2.4 Interim IT Disaster Recovery

P	Detailed finding	Risk	Recommendation
1	Prior to the new ITDR capability being implemented (now due Q1 2016) at the secondary data centre, we confirmed that an Interim ITDR capability was supposed to be in place. This was initially a ship to site "data-centre" that contained infrastructure for the Council's legacy systems. In the event of an incident, this would be plugged into the Council network and IT services would	In the event that the primary site was disabled, IT services could take multiple days or even weeks to recover, well outside of defined Council recovery requirements and causing significant service disruption.	**Recommendation 4** a) Capita should immediately engage the Council and propose the most effective way of mitigating the risk in the interim period prior to ITDR being fully deployed by the project. (Contract specification)

	have been recovered from a back-up. These services were procured by Capita from an external supplier. The contract for these services lapsed in early 2015 and was not renewed. As Capita have replaced some IT services and re-platformed others, the interim arrangement would not have been usable for recovery even if the contract had been renewed or extended. Capita are currently replicating data to the secondary site and taking backups in preparation for the new full capability. It was noted that there is currently no interim capability as: • There are no documented ITDR plans; • There have been no tests of the new capability; and • There is no recovery infrastructure in place or on contract to affect a successful recovery. NOTE: The reason for the gap in coverage is that the ITDR project was significantly delayed and the lapse of the contract should have coincided with the new capability going live.		

Management Response	Responsible Officer	Deadline
Agreed. It would be welcomed for audit to witness the preparation for the testing and the testing itself as part of their follow-up audit.	ICT Director (CSG) Head of Information Management (LBB)	With immediate effect

Timetable	
Terms of reference	14 August 2015
Fieldwork completed	23 December 2015
Draft report issued	2 February 2016
Management responses received	29 February 2016
Final Report Issued	22 March 2016

Appendix A: Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below:

- The matters raised in this report are only those which came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made.

- Recommendations for improvements should be assessed by you for their full impact before they are implemented.

- The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity.

- Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

- Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents.

- Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Appendix B: Guide to assurance and priority

The following is a guide to the assurance levels given:

	Substantial Assurance	There is a sound system of internal control designed to achieve the system objectives. The control processes tested are being consistently applied.
	Satisfactory Assurance	While there is a basically sound system of internal control, there are weaknesses, which put some of the client's objectives at risk. There is evidence that the level of non-compliance with some of the control processes may put some of the system objectives at risk.
	Limited Assurance	Weaknesses in the system of internal controls are such as to put the client's objectives at risk. The level of non-compliance puts the system objectives at risk.
	No Assurance	Control processes are generally weak leaving the processes/systems open to significant error or abuse. Significant non-compliance with basic control processes leaves the processes/systems open to error or abuse.

Priorities assigned to recommendations are based on the following criteria:

High – Fundamental issue where action is considered imperative to ensure that the Council is not exposed to high risks; also covers breaches of legislation and policies and procedures. Action to be effected within 1 to 3 months.

Medium – Significant issue where action is considered necessary to avoid exposure to significant risk. Action to be effected within 3 – 6 months.

Low – Issue that merits attention/where action is considered desirable. Action usually to be effected within 6 months to 1 year.