DRAFT - Internal Audit Report

IT Disaster Recovery
October 2016

To: Jenny Obee, Head of Information Management
Brett Holtom, ICT Director (CSG)
Kim Fletcher, Service Delivery Manager (CSG)

Copied to: Paul Williams, Enterprise Services (CSG)
Neal Silverstein, IT Contract Manager
Stephen Evans, Chief Operating Officer

From: Clair Green, Assurance Assistant Director

We would like to thank management and staff for their time and co-operation during the course of the internal audit.

Cross Council Assurance Service

Executive Summary

Assurance level	Number of recommendations by risk category				
	Critical	High	Medium	Low	Advisory
Reasonable	-	1	2	1	1

Scope

The scope of our work was to assess:

- The ITDR capability in place to meet Capita Customer Services Group (CSG) contractual requirements, in terms of the deployed technology and recovery processes in place.
- The method, process and controls employed to validate the ITDR capability through testing.
- The method process and controls employed in maintaining the ITDR capability as the Council adds new services and as existing ones are updated.

Summary of findings

Capita have recently completed an IT Disaster Recovery (ITDR) project, as part of a wider technology transformation project, aimed at meeting its contractual recovery obligations. The scope of the project included:

- The implementation of ITDR technical recovery capability at a secondary datacentre, that is capable of recovering operable contracted IT services within Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
- The testing of new capability to demonstrate that IT services under contract can be recovered.
- The development of comprehensive ITDR recovery plans and supporting documentation.
- Transferring the management of the capability into Business As Usual (BAU) IT operations.

The programme has been reviewed by Internal Audit twice previously and a number of observations were made that both Capita and council officers have committed to resolve.

Since the last update, CSG have undertaken a lot of work in preparing the ITDR capability in preparation to transfer it to Business As Usual (BAU) operation. Whilst this is yet to complete, the current technical capability, planning and project testing demonstrate that in the event of a disaster there is a high probability that services could be recovered within their designed capability.

Management have recently (September 2016) completed their ITDR re-baselining exercises to confirm the recovery Tier for all applications within scope. The output of this has been passed to CSG who are in the process of assessing the impact of moving IT services between recovery Tiers on the current technical provision.

Management are also engaged with CSG to resolve the issue raised in the last update with respect to the discrepancy between the contracted data recovery capability of Tier 2 IT services and capability that has actually been provisioned.

This audit has identified 1 high, 2 medium, 1 low risk and 1 advisory finding. The high risk finding is:

- **The CSG contract only supports IT service recovery during business hours** - The wider contract with CSG only covers business hours between 8am to 6pm in the working week, excluding bank holidays and weekends. If a disaster occurred out of hours CSG are not obliged to start recovery until 8am the next business day, even if the IT service has a 2 hour Recovery Time Objective (RTO). Additionally for those that have longer RTO's, i.e. the Tier 2 IT services with 48 hours, the recovery would potentially stop and start if the recovery actions exceeded the contracted hours, again taking longer than expected. From a business impact perspective, if a disaster happened out of hours, it would mean that critical Barnet functions would be without the services far longer than expected and may cause a material impact to the council as services to the public would be interrupted. This would particularly impact any function that work out of hours and that rely on a Tier 1 service with an RTO of 2 hours.

The medium risk findings are:

- **IT Disaster Recovery plans are not complete and its invocation and mobilisation processes are not defined sufficiently:** - Whilst technical ITDR plans are complete for Tier 1 IT services, the plans for Tier 2 are not complete. Instead there is generic guidance on how to recover a system from back-up, rather than the specifics on each Tier 2 system and the order they are supposed to be recovered in. Additionally the processes to invoke the ITDR capability are not clear, particularly with respect to the transition of responsibility from the business as usual major incident management process to the IT Business continuity plan and the mobilisation of central CSG resources, who are essential for the execution of the recovery. The impact is that without sufficiently detailed plans or clear mobilisation and invocation processes, the overall recovery may be delayed with IT services being recovered later than expected, which could cause a material impact to the business dependant on what council public services were affected.
- **A full ITDR test has not been carried out** - Whilst project testing has been executed, a full ITDR test has not been carried out. Management has agreed the scope of the test that will be executed following the transfer of the programme to business as usual, which whilst more comprehensive is not a full test. We understand, given the technical setup that executing a full test may not be feasible. The risk is that without a comprehensive testing programme that the recovery will not operate as planned when needed, which could lead to IT services being recovered later or in a state that cannot support the council. The impact would be that council functions would not be able to function and this could materially impact the provision of public services.

Appendix 6 contains updates from previous actions associated with ITDR. Progress has been made on the majority of outstanding observations.

2. Findings, Recommendations and Action Plan

Ref	Finding	Risks	Risk category	Agreed action
1.	**The CSG contract only supports IT service recovery during business hours. (Control design)** The current CSG contract for all IT services only covers the hours of 8am to 6pm during the week and excludes bank holidays. IT services with ITDR capability at Barnet are split into two tiers. Tier one services have an Recovery Time Objective (RTO, the time from invocation the IT service has operational) of two hours and hours and a 1 hour Recovery Point Objective (RPO, permanent data-loss, i.e. if a system with an RPO of 1 hour fails at 1300 it will be brought back the in state it was at 1200, with an hours permanent data loss). Tier two IT services have an RTO of 48 hours and an RPO of 24 hours. If an incident happens out of hours, CSG would not be obliged to start recovery until 8am the next day. Additionally, if recovery had started, for example, at 4.30pm, recovery would stop at 6pm and re-start at 8am. In a Tier two service case, as the RTO is 48 hours, this potentially could extend the recovery over several days. Whilst CSG may choose to conduct the recovery anyway, they are under no obligation to do so contractually and the central resources that the local team relies on may also be prioritised to clients who have 24 by 7 cover. It should be noted that whilst the general CSG contract does specify the support hours, the ITDR section	If a disaster occurs out of hours IT services will not be recovered to their RTO. The risk is that teams that work out of hours may not be able to operate and will not be able to provide the service are required to, to the public.	**High**	**Agreed Action:** a) Discussions have been taking place with CSG about extended out of hours support, and extended DR provision for critical services will be added into these proposal discussions. The target to resolve this is by the end of January 2017. The Council will undertake a risk assessment exercise to determine what services require out of hours DR support. **Responsible officer:** Jenny Obee, Head of Information Management Brett Holtom, ICT Director (CSG) **Target date:** 31 January 2017

Ref	Finding	Risks	Risk category	Agreed action
	where RTO's are stated does not have any commentary on the impact of support hours on recovery timelines. We understand that management and CSG are in discussion with respect to increasing some elements of support to 24 by 7 cover.			
2.	**IT Disaster Recovery plans are not complete and Invocation and mobilisation processes are not defined sufficiently (Control design)** IT services that have ITDR capability are now split into two tiers. Tier 1 IT services have an RTO of two hours and an RPO of one hour. Tier 1 ITDR technical recovery provision is based replicating data to the ITDR site and failing over the services using a tool called Site Recovery Manager (SRM) to prepared IT infrastructure, and is a relatively simple operation. Tier 2 IT services as provisioned have an RTO of 48 hours and an RPO of 24 hours. Tier 2 recovery technical provision is from the last available back-up, which may be up to 24 hours old, hence the RPO, which is then recovered to IT infrastructure in the recovery datacentre. The technical recovery plans currently only cover the Tier 1 IT service recovery steps in significant detail, which would allow for easy coordination and execution.	If sufficiently detailed plans are not in place to support the recovery of Tier 2 IT services then the risk is that they may not be recovered in time or in a suitable operable state. If the manner in which MIM passes over to ITDR and then the processes to invoke and secure resources are not clear then there is a risk that recovery will be delayed, which may lead to Tier 1 IT services, in particular, missing their recover times. In both cases there is a risk of material impact to the council as key IT services may not be available in the agreed recovery time to enable its	**Medium**	**Agreed Action:** a) The flight manual is to be updated to include a repeatable process for each Tier 2 IT service following an order of recovery. b) The IT Business Continuity plan will be updated so that it clearly reflects how MIM transfers responsibility to it with respect to the incident in terms of responsibility and managing any groups or communication that MIM may have setup or started. c) The IT Business Continuity plan will be updated so that it clearly states, how and when it stands up the recovery team detailed in the ITDR technical plan.

Ref	Finding	Risks	Risk category	Agreed action
	The recovery plans do not currently cover the specific steps or order that Tier 2 IT services will be recovered, in the event of a disaster. Instead there are generic instructions on how to apply a back-up. Management and CSG are aware of this issue and intend to address it once the revised list of Tier 2 IT services has been formally agreed. In the event of a major incident, including a disaster, the initial stages will be managed by CSG's Major Incident Management process (MIM). The objective of this process is to quickly understand the incident, mobilise the correct technical teams, which can be a mix of on-site and central CSG technical resources, and then manage the incident to conclusion within four hours. If the incident required requires the invocation of ITDR, the IT Business Continuity plan is then used to invoke recovery and then over manage the recovery detailed in the ITDR technical plan. Whilst there are links between the MIM process and the IT Business Continuity plan, they are not clear as to how one transitions into another, in terms of coordination. Additionally, whilst the ITDR technical plan specifies the types of resources it requires to execute the plan, it and the IT Business Continuity plan do not specify when and who secures them, as they come in the majority from the CSG central teams who are based off site and support multiple clients.	functions to operate key public services.		**Responsible officer:** Brett Holtom, ICT Director (CSG) **Target date:** 28th October 2016

Ref	Finding	Risks	Risk category	Agreed action
3.	**A full ITDR test has not been carried out (Control design)** As part of the ITDR project, CSG has carried out unit tests on different aspects of the technical recovery, most notably for SRM and demonstrating that virtual servers can be moved between sites. These tests were controlled adequately, with defects being identified and then scheduled for resolution. The Council and CSG have discussed the scope of the ITDR test, which currently involves moving a number of services to the secondary site and operating them there for its duration. Whilst this is useful test, it does not test an en-masse recovery (where everything is tested together), however we understand that as infrastructure is shared with other clients, isolating the second datacentre for a test is not possible.	If ITDR processes and technical capability are not tested sufficiently then there is a risk that if there is a disaster ITDR enabled services may not be recovered This could materially impact the council as IT services may not be available in the agreed recovery time to enable its functions to operate key public services.	**Medium**	**Agreed Action:** In absence of an en-masse test the test regime will consist of the following on an ongoing basis: a) Execute the agreed test. b) Run SRM tests on a quarterly basis. c) Conduct table table-top walkthroughs of the entire recovery, starting at the MIM process, through invocation and technical recovery on six monthly basis. The test approach has been agreed in principle, and the final Test Approach is to be produced by 28th October 2016 for sign-off by LBB. On sign-off a forward schedule of exercises will be agreed between both parties. **Responsible officer:** Jenny Obee, Head of Information Management Brett Holtom, ICT Director (CSG) **Target date:**

Ref	Finding	Risks	Risk category	Agreed action
				28th October
4	**IT service management processes are not fully developed to support the ITDR capability once it transfers to Business As Usual (BAU) (Control design)** The current IT change control process, does ask those raising the change to consider the impact on ITDR, so that it can be maintained effectively. Additionally all changes are submitted to the Change Advisory Board (CAB) for assessment. However, those raising the change currently have no point of reference to determine whether their change impacts an ITDR enables IT service. Management and CSG are aware of this and intend to develop a simple service catalogue that change raisers can access to improve their assessments and plans.	If production IT services are changed and the impact to ITDR provision is not updated in terms of technical process then there is a risk that if there is a disaster the ITDR enabled service may not be recovered as expected. This could materially impact the council as IT services may not be available in the agreed recovery time to enable its functions to operate key public services.	**Low**	**Agreed Action:** a) The IT service catalogue will be produced by the end of November 2016. An interim solution is in place to enable changes to be checked against a list of current DR services. b) The change process will be updated on implementation of the service catalogue. c) Prior to the roll out of the new process an awareness session to be held and updated change process to be issued all CAB members. **Responsible officer:** Brett Holtom, ICT Director (CSG) **Target date:** 30th November 2016

Ref	Finding	Risks	Risk category	Agreed action
5	**The SPIR process does not capture ITDR requirements (Design effectiveness)** The current SPIR process used to request new services from CSG does not currently consider ITDR as part of its requirements. This is mitigated in a limited fashion by the CSG receiving processes asking for the ITDR requirements when a SPIR is received. Management are currently in the process of updating the SPIR process to include ITDR requirements.	If requirements are not captured for a new IT service then there is a risk that ITDR provision may be insufficient and services either not recovered or recovered in time for council functions to resume service to the public with no impact.	**Advisory**	**Agreed Action:** This will be discussed with the Council's Programmes and Commercial Teams and the SPIR template will be updated. **Responsible officer:** Jenny Obee, Head of Information Management **Target date:** 31 December 2016

Appendix 1: Definition of risk categories and assurance levels in the Executive Summary

Risk rating	
Critical ●	Immediate and significant action required. A finding that could cause: • Life threatening or multiple serious injuries or prolonged work place stress. Severe impact on morale & service performance (eg mass strike actions); or • Critical impact on the reputation or brand of the organisation which could threaten its future viability. Intense political and media scrutiny (i.e. front-page headlines, TV). Possible criminal or high profile civil action against the Council, members or officers; or • Cessation of core activities, strategies not consistent with government's agenda, trends show service is degraded. Failure of major projects, elected Members & Senior Directors are required to intervene; or • Major financial loss, significant, material increase on project budget/cost. Statutory intervention triggered. Impact the whole Council. Critical breach in laws and regulations that could result in material fines or consequences.
High ●	Action required promptly and to commence as soon as practicable where significant changes are necessary. A finding that could cause: • Serious injuries or stressful experience requiring medical many workdays lost. Major impact on morale & performance of staff; or • Significant impact on the reputation or brand of the organisation. Scrutiny required by external agencies, inspectorates, regulators etc. Unfavourable external media coverage. Noticeable impact on public opinion; or • Significant disruption of core activities. Key targets missed, some services compromised. Management action required to overcome medium-term difficulties; or • High financial loss, significant increase on project budget/cost. Service budgets exceeded. Significant breach in laws and regulations resulting in significant fines and consequences.
Medium ●	A finding that could cause: • Injuries or stress level requiring some medical treatment, potentially some workdays lost. Some impact on morale & performance of staff; or • Moderate impact on the reputation or brand of the organisation. Scrutiny required by internal committees or internal audit to prevent escalation. Probable limited unfavourable media coverage; or • Significant short-term disruption of non-core activities. Standing orders occasionally not complied with, or services do not fully meet needs. Service action will be required; or • Medium financial loss, small increase on project budget/cost. Handled within the team. Moderate breach in laws and regulations resulting in fines and consequences.
Low ●	A finding that could cause: • Minor injuries or stress with no workdays lost or minimal medical treatment, no impact on staff morale; or • Minor impact on the reputation of the organisation; or • Minor errors in systems/operations or processes requiring action or minor delay without impact on overall schedule; or • Handled within normal day to day routines; or • Minimal financial loss, minimal effect on project budget/cost.
Level of assurance	
Substantial ●	There is a sound control environment with risks to key service objectives being reasonably managed. Any deficiencies identified are not cause for major concern. Recommendations will normally only be Advice and Best Practice.
Reasonable ●	An adequate control framework is in place but there are weaknesses which may put some service objectives at risk. There are Medium priority recommendations indicating weaknesses but these do not undermine the system's overall integrity. Any Critical recommendation will prevent this assessment, and any High recommendations would need to be mitigated by significant strengths elsewhere.
Limited ●	There are a number of significant control weaknesses which could put the achievement of key service objectives at risk and result in error, fraud, loss or reputational damage. There are High recommendations indicating significant failings. Any Critical recommendations would need to be mitigated by significant strengths elsewhere.
No ●	There are fundamental weaknesses in the control environment which jeopardise the achievement of key service objectives and could lead to significant risk of error, fraud, loss or reputational damage being suffered.

Appendix 2 – Analysis of findings

Area	Critical		High		Medium		Low		Total
	D	OE	D	OE	D	OE	D	OE	
ITDR Capability in line with requirements That the deployed ITDR capability, from both a technical and process perspective can recover in scope operable IT services in line with the CSG contract	-	-	1	-	1	-	-	-	**2**
ITDR Capability maintenance That effective processes and controls are in place to ensure the ITDR capability is maintained as the IT estate or council requirements change.	-	-	-	-	-	-	1	-	**1**
ITDR capability testing That the ITDR capability, from both a technical and process perspective, is demonstrated representatively through testing.	-	-	-	-	1	-		-	1
Total	**-**	**-**	**1**	**-**	**2**	**-**	**1**	**-**	**4**

**Includes two findings relating to control design and operating effectiveness*

Key:

- Control Design Issue (D) – There is no control in place or the design of the control in place is not sufficient to mitigate the potential risks in this area.
- Operating Effectiveness Issue (OE) – Control design is adequate, however the control is not operating as intended resulting in potential risks arising in this area.

Timetable					
Terms of reference agreed:	**Fieldwork commenced:**	**Fieldwork completed:**	**Draft report issued:**	**Management comments received:**	**Final report issued:**
20th September 2016	28th September 2016	6th October 2016	10th October 2016	14th October 2016	18th October 2016

Appendix 4 – Identified controls

Area	Objective	Risks	Identified Controls
ITDR Capability in line with requirements	That the deployed ITDR capability, from both a technical and process perspective is can recover in scope operable IT services in line with the CSG contract	The deployed ITDR capability does not meet the councils requirements and, in the event of real incident, fails to recover IT services in time or state, in line with the contract, impacting the Council materially.	Identified control • ITDR plans and processes used to coordinate and execute a recovery (Reference observation 2) • The CSG contract sections that detail what IT services are covered by ITDR and their contracted capabilities (Reference finding 1) • The technical solution in place that CSG have deployed and maintained to deliver ITDR
ITDR Capability maintenance	That effective processes and controls are in place to ensure the ITDR capability is maintained as the IT estate or council requirements change.	The deployed ITDR capability is not maintained effectively, and in the event of a major incident does not function as expected, materially impacting the Council.	Identified control • IT Change Management process, in an ITDR context, to ensure that the existing technical capability is maintained (Reference observation 4) • SPIR process used by the council to define new service requirements from CSG (Reference observation 5) • OASIS Process used to transfer new IT services into live support (Reference 5) • Work Package Process.
ITDR capability testing	That the ITDR capability, from both a technical and process perspective, is demonstrated representatively through testing.	The deployed ITDR capability is not tested effectively and the opportunity to resolve issues that have the potential to delay the effective recovery of IT services is lost, again with material impact to the council.	Identified control • Test approach as part of the project to representatively demonstrate the capability prior to deployment (Finding 3) • Proposed test approach to representatively demonstrate the ITDR capability after deployment (Finding 3)

Appendix 5 – Internal Audit roles and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken the review of *IT Disaster Recovery*, subject to the limitations outlined below.

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Specifically we will not:

- Provide assurance over the accuracy, validity or completeness of Purchase Card expenditure within the General Ledger, "Integra" system; and
- Investigate the results from the data analytics exercises. Results of this exercise will be presented to management to investigate and take further action as necessary.

Future periods

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.

Appendix 6 – Update on actions from the July 2016 follow on review

Status	Description	Total July 16	Total Oct 16
Implemented	Evidence provided to demonstrate that the action is complete	3	5
Partially Implemented	Evidence provided to show that progress has been made but the action is not yet complete	5	3
Not Implemented	No evidence seen of the action being progressed or completed	2	2

Detailed Status Updates

Audit finding, date and recommendation (March 2016)	Audit follow-up status (October 2016)
1. ITDR Governance	
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) **Action:** Recommendation accepted & completed **Responsible Officer:** Dennis Hunt, IS Security Manager (CSG) **Target date:** 30 April 2016	**Implemented (July 2016)** Capita staff, who are responsible for the ITDR programme have been identified for inclusion in the council's BCM steering committee.

Audit finding, date and recommendation (March 2016)	Audit follow-up status (October 2016)
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 **Action:** Recommendation accepted & completed **Responsible Officer:** Kate Solomon, Emergency Planning and Business Continuity Manager (LBB) **Target date:** 30 April 2016	**Implemented (October 2016)** BCM steering committee now discusses ITDR formally **Partly Implemented (July 2016)** Capita have invited and have attended the BCM steering committee. However the meeting did not include any formal ITDR programme discussion. BCM team should add a standing ITDR agenda item to the steering committee.
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) **Action:** Recommendation accepted & completed **Responsible Officer:** Ian Baker, Operations Manager (CSG)	**Not implemented (October 2016)** Final RTO's and RPO's have been submitted by the council (September 2016) for discussion with Capita. Until these are finalised Capita will not be able to report on them. **Not implemented (July 2016)** Please see 2b below. RTO's are still being reviewed with the council this cannot complete until they are agreed.
d) Management should update governance policies, terms of references and processes to reflect the above. (Governance)	**Implemented (October 2016)**

Audit finding, date and recommendation (March 2016)	Audit follow-up status (October 2016)
Action: Recommendation accepted & completed **Responsible Officer:** Kate Solomon, Emergency Planning and Business Continuity Manager (LBB) **Target date:** 30 April 2016	Management have changed the terms of reference for the BCMT to reflect that ITDR status will be discussed as part of governance. **Not implemented (July 2016)** No update received from management for this recommendation.
2. Alignment of BCM recovery requirements with ITDR capability	
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) **Action:** Recommendation accepted **Responsible Officer:** Kate Solomon, Emergency Planning and Business Continuity Manager (LBB) **Target date:** With immediate effect	**Implemented (July 2016)** For the purposes of this action Capita are engaging with Jenny Obee.

Audit finding, date and recommendation (March 2016)	Audit follow-up status (October 2016)
b) Capita should immediately engage the 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) **Action:** Recommendation accepted & completed **Responsible Officer:** Ian Baker, Operations Manager (CSG)) **Target date**: With immediate effect	**Partially implemented (October 2016)** Capita have, with management, agreed that Platinum and Gold are now Tier 1 and Silver and Bronze are Tier 2 based as their recover capabilities within Tier are identical. Capita have received an updated list of IT services from management (September 2016) and are in discussion with respect to moving them between tiers. **Partially implemented (July 2016)** Capita have recently (complete June 2016) an analysis of the original schedule against the systems currently provisioned for by the project. At the time of the update Capita had not discussed the outcomes with LBB. The Capita analysis shows the following for 2011: • 32 as Platinum • 16 as Gold • 23 as Silver • 66 as Bronze • 43 unclassified (i.e. in this case do not require ITDR) The above numbers are reflected in the contract. It was also noted that a number of these entries were erroneous as they were for service components (e.g. Oracle) as opposed to IT services. Additionally these numbers include a number of 3rd party services not provided directly by Capita The Capita analysis shows that what has actually been provisioned (excluding 3rd parties) is as part of the project is as follows: • 52 as Platinum and Gold • 27 as Silver and Bronze • 25 as Unclassified The analysis notes that since 2011 58 additional services have been decommissioned

Audit finding, date and recommendation (March 2016)	Audit follow-up status (October 2016)
	It was also noted on interview, that systems that were introduced since 2011, did not include a formal request for ITDR from the council, however in a number of cases (e.g. Mosaic), Capita have provisioned anyway. The analysis underlines the necessity for the council and Capita to re-baseline the recovery requirements of IT services.
c) In line with the governance finding (Recommendation 2.1d *per report*) 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) **Action:** Recommendation accepted & completed **Responsible Officer:** Kate Solomon, Emergency Planning and Business Continuity Manager (LBB) **Target date**: 30 April 2016	**Not implemented (October 2016)** As per 2(b) Tiering of applications is still on going. Once complete this activity can start. **Not implemented (July 2016)** As Capita and the council have not re-baselined this action is not possible.

Audit finding, date and recommendation (March 2016)	Audit follow-up status (October 2016)
3. ITDR planned technical recovery capability	
a) In line with the recovery requirements recommendation in the report (Recommendation 2.2b), Capita should immediately engage with the Council to ensure the required infrastructure is provided to meet recovery requirements and expected user numbers. (Contract specification). **Action:** Recommendation accepted & completed **Responsible Officer:** Ian Baker, Operations Manager (CSG) **Target date:** With immediate effect	**Partially Implemented (October 2016)** As per 2b, Capita and management have started (September 2016) which IT services will be moving recovery Tiers. Management are in discussion with Capita with respect to the gap between the Councils expectations for Silver and Bronze IT services (now Tier 2) with RPO and Capita provision. **Partially implemented (July 2016)** As per 2b, Capita have completed their initial analysis on what is currently covered by the ITDR programme against initial contract and are in the process of engaging the Council. As an update Capita have informed IA that the current ITDR project's provision for applications placed in silver and bronze categories cannot meet contractual recovery requirements with respect to Recovery Point Object (RPO, i.e data loss). The contractual requirements stands at 1 hour (i.e. if the system fails at 1200, it will be brought back to a state where it was at 1100, with an hours' worth of permanent data-loss), however the actual capability will lose up to 24 hours of data. It is recommended that the Council take this into account when re-baselining.
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 scope and have a critical dependency. It may also mean that IT services have to be	**Implemented (July 2016)** Capita have conducted an analysis of the applications in scope and identified interdependencies between applications.

Audit finding, date and recommendation (March 2016)	Audit follow-up status (October 2016)
promoted in terms of tiering to ensure successful recovery. (Proposed ITDR solution) **Action:** Recommendation accepted & completed **Responsible officer:** Applications team, CSG **Target date:** 30 May 2016	
4. Interim IT Disaster Recovery	
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). **Action:** Recommendation accepted & completed **Responsible Officer:** Brett Holtom, ICT Director (CSG) Jenny Obee, Head of Information Management (LBB) **Target date:** 4 April 2016	**Partially implemented (October 2016)** The technical recovery capability is in place for failover of central systems. The WAN project has a number of sites that are yet to be cut-over, however this only represents approximately 5% of users. As per the main report limited testing as part of the project has been carried out, however BAU testing has not and the current ITDR plans do not have detailed instructions for Tier 2 applications. **Partially implemented (July 2016)** Capita have continued with the rollout of the ITDR programme. In terms of recoverability the following stands: • Gold and Platinum IT services have recovery infrastructure and currently replicating their data. • Silver and Bronze IT services have recovery infrastructure in place, however it does not allow for the recovery of data within contractual requirements • Partial recovery plans have been developed.

Audit finding, date and recommendation (March 2016)	Audit follow-up status (October 2016)
	• The associated LAN/WAN project has not completed and the time of review would mean that approximately 40% of council users would not be able to access recovered services from their offices. • No testing has been carried out. In this position Capita would stand a reasonable chance of recovering services but there is a risk this may not occur within contractual requirements due to the lack of testing and documentation. However requirements do not come into force until the project has delivered. The project is currently on track to complete (i.e. hand over to Business As Usual) in mid-August.