Putting the Community First

BARNET LONDON BOROUGH

Internal Audit Report

IT Change Management Review
March 2016

To:	Chief Operating Officer
	Head of Information Management
	IT Director (CSG)
	Programme Director (CSG)
Copied to:	Enterprise Architect (CSG)
	Head of Service Delivery (CSG)
	External Audit
From:	Head of Internal Audit

We would like to thank management and staff of the London Borough of Barnet and the Customer Support Group (CSG) 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
Limited	0	2	3	1	0

Scope and limitations of scope

The Council use the Customer Support Group (CSG), part of Capita, who are an external IT service provider, to manage, support and deliver IT services that enable operation of the Council's services. Historical IT incidents/ outages have raised concerns regarding the operation of the IT Change Management process and whether CSG are following the standard for IT Service Management as defined within the contract.

The purpose of this audit is to review the appropriateness and effectiveness of the IT Change Management process, including related governance, policies, process, procedures and controls that are in place to manage changes to the IT applications and infrastructure that support Barnet Council's services. This review will not include a technical assessment or an opinion on any IT products or services chosen by the Council to deliver and implement its strategy.

Executive summary

Successful implementation of IT services to the live, Business as Usual (BAU) environment is reliant on effective control processes, including Service Asset and Configuration Management, Release and Deployment Management, Service Validation and Testing, Change Management and Change Evaluation. This review focused on Change Management specifically and while there is a draft IT Change Management process in place, it is not effective due to the lack of maturity in the supporting control processes.

This review was mainly scoped for the time period of January 2015 to December 2015. It is recognised that CSG have made significant improvements to the IT Change Management process during 2015 and have continued to make gradual improvements during 2016. However, it has been observed through this review that there are many examples of a reactive, rather than proactive approach to IT change management being implemented. This approach impacts the quality of service provided to Barnet Council.

The IT Change Management process is not yet effectively embedded into the organisation (due to it being relatively new) and it is not yet at the required level of maturity expected from an experienced IT Service Provider. This limits CSG's ability to effectively govern, manage, monitor and improve IT change and increases the likelihood of negative impact to services at Barnet Council.

Summary of observations

1. **Control Design – Process Lifecycle (High Priority)**

   - CSG use a static, standalone spreadsheet to manage configuration information and this is not linked to the existing toolset (ServiceNow) that is in place to manage the Change Management process. Auditor's view is that this approach is not suitable for an IT estate of the size and complexity of Barnet Council. The standalone spreadsheet approach and lack of update process has resulted in a backlog of outstanding configuration updates as well as an inaccurate baseline of configuration information. Without an effective Configuration Management Database (CMDB), accurate Configuration Items (CIs) and relationships linking the CIs to business processes, it is difficult to accurately assess the full impact to end-to-end business services when making technology changes. As a consequence, the configuration information cannot be relied upon for change, risk and impact assessments. Additionally, as CIs are not being updated, links between CIs in the live/ BAU and IT Disaster Recovery (ITDR) environments will not be current or accurate. This will impact CSG's ability to maintain an effective ITDR environment, which may then impact a successful recovery in the event of disaster **(see finding 1.1)**.

   - Post-change evaluations are not performed routinely for change records. This means that there is no process being consistently followed to determine whether or not a change has been successful and whether there are any lessons learned that would be useful to drive continuous improvement. Ad-hoc investigations into failed changes have been performed on request or when a major incident has occurred as a result of a change. This approach limits the evaluation process as not every failed change is going to result in an incident **(see finding 1.2)**.

   - There have been occasions where changes related to project implementations have been processed as Emergency Changes in order to achieve project deadlines. While the reasoning for this is to mitigate potential business impact, the use of Emergency Changes specifically by projects is not documented as an exception within the Change Management process. These exceptions are not reviewed or included in management reporting for trend analysis. Lack of appropriate planning for a project-related change should not automatically invoke the Emergency Change process as Emergency Changes carry an increased level of risk to the business. It is therefore important that the scope and exceptions for Emergency Changes are documented in detail **(see finding 1.3)**.

2. **Control Design – Change Testing & Validation (High Priority)**

   - Few applications had separate testing environments. For those applications with no testing environment, CSG stated that the risk has been accepted by Barnet Council, however formal documentation and evidence of this has not been seen. Where no testing environment exists, changes were implemented directly into the live environment without testing. Back-out plans are not always sufficiently detailed and are not usually tested prior to change implementation. This increases the likelihood of problems occurring during change implementation **(see findings 2.1 and 2.2)**.

3. **Operating Effectiveness - Result of Sample Records Testing (Medium Priority)**

   - We tested 25 sample changes to check the operating effectiveness of key controls in the IT Change Management process and found the following issues **(see findings 3.1 to 3.5)**:

     - 8 out of the 25 changes sampled (32%) were major changes, yet none of them had a full work plan document. This is not in line with the Change

Management procedure.

- 4 out of the 25 changes (16%) lacked a back out plan.
- 3 out of the 25 changes (12%) lacked a test plan.
- 1 of the 25 changes (4%) was raised as a normal change, but was approved by the Emergency Change Advisory Board (ECAB).
- 24 of the 25 changes (96%) have not yet been closed out. The remaining change had been marked as "rejected". Good practice, such as post-change review and change evaluation are not formally performed if a change record is not completed and closed out. It is also difficult to assess, measure and report on the performance of the IT Change Process and how successful it is.

4. Operating Effectiveness – Continuous Service Improvement (Medium Priority)

- Upon reviewing two failed change reports and one security incident report, it was found that the reports were not conclusive in identifying the root cause. The reports were produced while the investigation was still in progress and were not updated following completion of the investigation **(see finding 4.1)**.

- A Service Improvement Plan exists, however there are no formalised processes or triggers for its use, for example, lessons learned reviews. Information is gathered on an ad-hoc basis and lacks appropriate analysis, ownership or a formal action plan **(see finding 4.2)**.

- There is no mandatory process to investigate failed changes or to use this information to drive continuous improvement and lessons learned **(see finding 4.2).**

5. Control Design – Governance of IT Change Management (Medium Priority)

- The IT Change Management process design documentation was updated immediately prior to our review and was supplied as a draft version. The documentation had yet to be approved through CSG's internal approval process. The document is not at the level of maturity expected from an experienced IT Service Provider and requires inclusion of the findings from this review **(see finding 5.1)**.

- There was a lack of documented evidence to show effective governance of the IT Change Management process and associated sub-processes. The Change Management process lacks a documented owner and there is confusion with who is responsible and accountable for the policy, process and procedure documents. The Technical Change Advisory Board (CAB) meetings and the Customer CAB meetings lacked documented terms of reference to explain their purpose, who should be invited and the roles and responsibilities of the attendees. Lack of effective governance means reduced control and increased risk to Barnet Council **(see findings 5.1 and 5.2**).

6. Control Design – Expectations Management (Low Priority)

- The Service Level Agreements (SLAs) for CSG's IT services are not adequately visible and accessible. As a result, there are different expectations of the IT service, such as Core Service Hours **(see finding 6.1)**.

Findings, Recommendations and Action Plan

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
1.	**<u>Process Lifecycle</u>** ***Control design***			**HIGH**	
1.1	IT Change Management is reliant on accurate configuration management information. The configuration of the system shows the status of assets that need to be managed in order to deliver an IT service and their dependencies. This can include applications, hardware or documentation. This is usually stored in a Configuration Management Database ("CMDB"). While CSG's IT Change Management process is supported by ServiceNow (a toolset used to manage the IT service management processes), CSG use a static, unlinked spreadsheet for managing configuration information. It is not appropriate or effective to manage configuration information for an IT estate of the size and complexity of Barnet Council's in a static spreadsheet. This approach restricts CSG's ability to capture and maintain accurate relationship information between Configuration Items (CIs), resulting in change-related decisions being made that are based on inaccurate information. There is a backlog of missing CI updates to the spreadsheet. We did not see evidence of	Configuration records are not updated in a timely manner after an IT change resulting in inaccurate IT configuration information available for future IT change impact assessment and dependency analysis. The lack of auditable updates to configuration information post change implementation, means that dependency and configuration information cannot be relied upon when assessing an IT change increasing the likelihood that future IT changes will fail.	a) Upgrade to a scalable relational Configuration Management Database (CMDB) tool to enable the auditable capture of CI dependencies and configuration information. b) Ensure that CIs are routinely updated into the CMDB through the IT Change Management process.	**HIGH**	**Action:** (a) Recommendations accepted **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 31st August 2016 **Action:** (b) Recommendation accepted **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 31st August 2016

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	a process to update the CIs into the Configuration Management Database (CMDB) spreadsheet, establish CI baselines (to provide an accurate snapshot of all CIs at specific points in time), manage existing CIs, add new CIs or update CIs following changes.				
1.2	Post-change evaluations on all change records are not performed routinely which means that there is no process to determine whether a change has been successful or identify any lessons learned that would be used to drive continuous improvement. Evaluations of failed changes are performed on an ad-hoc basis, only on request or if a major incident is caused by a failed change. At present not all change records are being captured to determine the failure rate – only the ones where there has been an incident as a result of a failed change. Not all change failures cause an incident. Change records are managed through the ServiceNow toolset but are not consistently closed after an IT Change is implemented, with the status of many historical change records left at 'Implement' or 'Update CMDB' (Configuration Management Database) stage	Changes are not reviewed to determine whether successful and identify lessons learned for continuous improvement. Change records are not completed in a timely manner, resulting in inaccurate status reporting, potential inaccuracies to IT configuration information available for future IT change impact assessment and dependency analysis and lack of triggering the post-change review process.	a) Update the IT Change Management policy to include a mandatory review of all failed Request for Change (RFCs) to identify the cause of failure. b) Where Council services are affected, inform and update in a timely manner, explaining which services are unavailable, what work-arounds are available and the estimated time until service is restored. c) Perform post-change evaluations and ensure change records are closed. d) Review IT Change Management service metrics and monitor on an ongoing basis. This will allow early identification of issues and inform proactive changes to the IT Change Management process, policy, design or procedure as well as identifying staff that require	**HIGH**	**Action:** (a) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016 **Action:** (b) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016 **Action:** (c) Recommendation accepted **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 31st August 2016 **Action:**

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
			additional change training and support.		(d) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 12 April 2016
1.3	Through the fieldwork interviews, it was discovered that **changes relating to project implementations** have been processed as Emergency Changes in order to achieve project deadlines. Criteria and controls for exceptions to the Emergency Change process are not explicitly documented and included in the IT Change Management process. These exceptions are not reviewed or included in management reporting for trend analysis.	Emergency Changes carry an increased risk to the business as this type of change does not go through the same level of assessment and approval as a normal change.	a) Define the project-related criteria and controls required for acceptance into the Emergency Change process. b) Incorporate project-related changes to the existing reports.	**HIGH**	**Action:** (a) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 12 April 2016 --- **Action:** (b) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 12 April 2016
2.	**<u>Change Testing & Validation</u>** ***Control design***			**HIGH**	
2.1	Through the fieldwork interviews, it was found that not all applications had separate testing environments due to lack of	A lack of testing environments for some Council IT services and	a) Identify which IT services could have an unacceptable impact to the Council's	**HIGH**	**Action:** (a) Recommendation accepted

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	investment. For those applications with no testing environment, changes were implemented into the live environment without testing.	a lack of testing of the change back-out procedures increases the likelihood of problems during release/ implementation.	services should there be a prolonged outage. b) Where the underpinning IT services do not have a test environment, or the existing test environment configuration differs from production, ensure proposed options for remediation have been presented to Council and Council's response recorded. c) Where proposed options are declined by Council, ensure that the risk of IT Change is formally accepted by Council and is reviewed regularly by CSG and Barnet Council management.		**Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 30 April 2016 **Action:** (b) Recommendation accepted & completed **Responsible Officer:** Programme Director (CSG) **Target date:** 12 April 2016 **Action:** (c) Recommendation accepted & completed **Responsible Officer:** Programme Director (CSG) **Target date:** 30th April 2016
2.2	A back-out plan is a procedure used to reverse a change and restore the original configuration, as if the change had not taken place. The steps required to carry out a controlled back-out of a change are required as part of the IT Change Management procedure, however it was found that the back-out plan was not always tested prior to change implementation and the details of the back-out plan attached to a change record were often documented only as "restore from	A lack of testing environments for some Council IT services and a lack of testing of the change back-out procedures increases the likelihood of problems during release/ implementation.	a) Where possible, test back-out plans. Testing may either be performed periodically (with an appropriate frequency schedule during the year) or in real-time, specifically as part of the change request to ensure confidence that the back-out plan will work as expected. Where back-out plans cannot be tested, this	**HIGH**	**Action:** (a) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 12 April 2016 **Action:**

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	backup". There can be a vast difference between reversing the steps for a change and implementing a full restore from back up, both in terms of time and risk and outcome. The level of detail noted within the back-out plan needs to be appropriate. Without testing the back-out plan, it is unknown whether changes can be successfully reversed and achieved within the agreed Change Management window.		risk should be made aware to the Technical and Customer CAB when presenting the RFC and formally documented in the change record. b) Specify under which conditions the back-out plan should be invoked. c) For back-out plans that are dependent upon data restoration from backup, CSG should ensure that the data restoration time is known and confirmed through testing.		(b) Recommendation accepted & completed **Responsible Officer:** , Head of Service Delivery (CSG) **Target date:** 12 April 2016 **Action:** (c) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016
3.	**Result of Sample Records Testing** ***Operating effectiveness***			**MEDIUM**	
3.1	The ServiceNow toolset is used to raise new IT changes and to coordinate and record the review, assessment and approval of IT change requests. All standard, normal and emergency changes are recorded in ServiceNow. 979 changes were raised during the period of 01/01/15 to 31/12/15 which gives an average change frequency of multiple change records per day which perhaps could have been grouped into releases.	A lack of work plan increases the likelihood of unforeseen IT incidents during the Change Management process, causing a prolonged impact to Council services.	a) The IT Change Manager must ensure that for all major changes, the full work plan is completed in line with Change Management procedures and attached to the change request ticket. b) Release Management is the process responsible for planning, scheduling and controlling the build, test and deployment of releases. It is also responsible for delivering new functionality required by	**MEDIUM**	**Action:** (a) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016 **Action:** (b) Recommendation accepted & completed **Responsible Officer:**

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	A sample of 25 changes were randomly chosen, covering all change types (normal, emergency, retrospective and standard) and all Request For Change (RFC) categories (major, significant, minor). 7 out of the 25 samples were emergency changes. Several findings emerged from the detailed testing: 8 out of the 25 changes (32%) were major changes, however none of these had a full work plan document attached to the change record (as required in the IT Change Management procedure). The work plan document ensures that all pre-requisites for carrying out the change have been completed.		the business while protecting the integrity of existing services. The Release Manager should review Requests for Change (RFCs) to determine when these changes should be packaged as releases.		Head of Service Delivery (CSG) **Target date:** 4th April 2016
3.2	4 out of the 25 changes (16%) lacked a back-out plan (as required in the IT Change Management procedure), which means that if reversal of the change is required, there would not be any steps within the change record, for the technician to follow. 1 of the 4 exceptions is an emergency change request which carries increased risk to the Council. It is good practice to include a back-out plan for all emergency changes.	A lack of back-out plan and testing of the back-out plan increases the likelihood of unforeseen IT incidents during release/ implementation which may cause an impact to Council services.	The IT Change Manager must ensure that essential documentation such as back-out plans are in place for all standard and emergency change requests. Where not applicable, clear justification should be provided and documented in the change request ticket.	**MEDIUM**	**Action:** Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016
3.3	3 out of the 25 changes (12%) lacked a test plan (as required in the IT Change Management procedure), which means that appropriate testing was not agreed or performed before the change was made to	A lack of test plan increases the likelihood of unforeseen IT incidents during release/ implementation which	a) The IT Change Manager must ensure that essential documentation including test plans are in place for all standard and emergency	**MEDIUM**	**Action:** (a) Recommendation accepted & completed **Responsible Officer:**

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	the production environment. 1 of the 3 exceptions is an emergency change request which carries increased risk to the Council. It is good practice to include a test plan for all emergency changes.	may cause an impact to Council services.	change requests. Where not applicable, clear justification should be provided and documented in the change request ticket. b) Vital IT services must have like-for-like configuration environments to allow appropriate levels of testing for IT change. Where this is not possible, ensure that the risk is accepted by all stakeholders (refer to Recommendation 6.1 b).		Head of Service Delivery (CSG) **Target date:** 4th April 2016 **Action:** (b) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016
3.4	24 of the 25 change records (96%) had not yet been closed within the ServiceNow toolset. 1 exception had a status of "Rejected' and 3 out of the 24 samples were still marked as being at the "Implement" stage, which means that they appear as if they are still in progress, even though it is known that they have been completed. The remaining 21 samples were at "CMDB update" stage, which means that configuration information had not been captured or updated into the Configuration Management Database (spreadsheet).	Change records are not closed in a timely manner, resulting in inaccurate status reporting, potential inaccuracies to IT configuration information available for future IT change impact assessment and dependency analysis and lack of triggering the post-change review process.	a) The IT Change Manager must ensure that all change records are closed in a timely manner. b) The Configuration Management process requires maturity, to ensure all configuration information is captured and updated in a timely manner.	**MEDIUM**	**Action:** (a) Recommendation accepted **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 31st August 2016 **Action:** (b) Recommendation accepted **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 31st August 2016
3.5	1 of the 25 changes (4%) was raised as a normal change (CHG0050066), but was approved by the Emergency Change Advisory Board (ECAB). In line with good	Emergency changes may not be properly reviewed and approved if they are not sent to the	The IT Change Manager must ensure that all change records are routed to the correct Change Advisory Board or re-classified if	**LOW**	**Action:** Recommendation accepted & completed

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	practice, changes should be approved by the appropriate Change Advisory board (to ensure the correct people make the approval) or re-classified if the priority has changed. Evidence has been provided post-review, showing that this change record was miscategorised as a 'normal change' when raised, instead of being categorised as an 'emergency change'. Despite the miscategorisation, the change record was routed through the approval process for emergency changes.	correct approval group, resulting in an increased likelihood of unforeseen IT incidents causing an impact to Council services.	the priority has changed.		**Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016
4.	**Continuous Service Improvement** ***Operating effectiveness***			**MEDIUM**	
4.1	We requested a sample of IT incident reports where IT Change Management was identified as the root cause. Of the three reports sampled, two were failed change reports and one was a security incident report. We found that these reports were not conclusive in identifying the root cause of the incidents. The reports were produced while the investigation was still in progress and not completed or updated once the investigation was over. Specifically, the Tribal change failure report stated "*We need to understand why we lost the ARP config settings when the change was made*." as well as "*Investigations are on-going*". The root cause was not identified to	The root cause of incidents resulting from failed changes are not identified, resulting in opportunities for improvement not being identified and an increased likelihood of similar incidents occurring in the future. Not every failed change will result in an incident. Performing root cause analysis only in the event of a major incident is not effective in capturing the reasons behind failed changes.	Investigate all failed changes. Failed change investigation reports must identify the root cause of change failure and actions taken against the root cause to improve the process.	**MEDIUM**	**Action:** Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4 April 2016

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	establish why the ARP configuration setting was lost. Similarly, the report for the Citrix incident in 2014 stated "*The ensuing immediate investigation was inconclusive in attributing the root cause of the incident. The loss of permissions may have been caused by a glitch in the migration process, or may be attributable to an existing undiscovered 2003 software bug, as infrequent instances of permission issues have been experienced at Barnet before.*" Again, the root cause was not identified when the report was produced.	Design and operating deficiencies within the change management process cannot be effectively identified unless the cause of a failed change is known. Lack of understanding behind failed changes prohibits service improvement and can result in a repeat of incidents.			
4.2	There is a Service Improvement Plan in place, maintained by the Service Delivery Manager. Although the IT Change Manager performs ad-hoc reviews (upon request) to investigate specific failed changes, this is not standard practise for all failed changes. A failed change report is produced after an investigation, but the reports submitted for review were not conclusive in identifying a root cause and had not been completed. Upon reviewing the Service Improvement Plan, two items related to change management were listed. Neither of them were triggered by lessons learned from previous incidents and appear to have been added on an un-related, ad-hoc basis.	Actions identified from post change reviews are not input into a service improvement plan resulting in a repeat of incidents that could have been prevented.	Review all failed changes for root cause analysis and lessons learned. Routinely review and consolidate the lessons learned into the Service Improvement Plan, to prevent similar incidents repeating in the future	**MEDIUM**	**Action:** Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
5.	**<u>Governance of IT Change Management</u>** ***Control design***			**MEDIUM**	
5.1	The IT Change Management process document was reviewed, however it was in draft and has not yet been approved. In line with our knowledge of similar organisations and IT service providers, the draft document is not at the required level of maturity that would be expected from an experienced IT Service Provider. There was a lack of documented evidence to show effective governance of the IT Change Management process, e.g. the Change Management process lacks a documented owner and there is confusion with who is responsible and accountable for the policy, process and procedure documents.	A lack of an approved IT Change Management process, aligned with good practice, may result in the risk that inappropriate or incorrect changes are made to the IT environment. A lack of effective governance around policies, processes and procedures reduces the level of control and oversight in minimising risk to the operating environment at Barnet Council.	a) Update the IT Change Management procedure document to include the agreed findings from this review. Obtain approvals and circulate the procedure to the required parties. b) Update all policies, procedures and processes to include ownership, responsibility and accountability information. Communicate to the required parties.	**MEDIUM**	**Action:** (a) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016 **Action:** (b) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016
5.2	Change management at the Council is overseen by the Technical Change Advisory Board and the Customer Change Advisory Board (formed in January 2016). The Council view the Customer Change Advisory Board as a forum to communicate forthcoming changes while CSG include the Customer Change Advisory Board as part of the change approval process, using the	Lack of clear roles and responsibilities for the members of Change Advisory Boards increase the risk of changes proceeding without correct approvals. IT Changes may not be	a) The Technical Change Advisory Board meetings and the Customer Change Advisory Board meetings require documented terms of reference to explain their purpose, who should be invited and the roles and responsibilities of the attendees.	**MEDIUM**	**Action:** (a) Recommendation accepted **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 30th April 2016 **Action:** (b) Recommendation accepted &

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	meeting to gain approval of potential business impact to Council services. While it is understood that the Customer Change Advisory Board has only recently been formed, a Terms of Reference document would be expected to be present in order to define purpose, attendees, roles and responsibilities. There is no evidence of a Terms of Reference document, resulting in the Council and CSG having different expectations for the purpose of the Customer Change Advisory Board meetings.	authorised, reviewed and assessed for business impact by the correct business service owners. This could result in an unexpected impact to the Council's services if the IT Change fails or is scheduled at a time that is vital to business operations.	b) Evidence of agreed decisions from the Advisory Board meetings should be attached to the relevant change record.		completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016
6.	**Expectations Management** ***Control design***			**LOW**	
6.1	The Service Level Agreement (SLA) sets out CSG's responsibility in providing IT services to the Council. The three Key Performance Indicators (KPIs) defined in the SLA relate to Capacity Management, Incident Management and Request Fulfilment. CSG produce a monthly Management Information (MI) reporting pack against these KPIs which is submitted to the Council for review on a monthly basis. We found that the SLA for CSG's IT service was not easily visible and accessible to the users of the service. As a result, there are different expectations of the IT service, such as Core Service Hours. As an example, Council staff reported IT incidents during the evening/ night and expected them to be resolved within four hours, however the CSG	A lack of transparency and access to IT Service SLA information for IT services decreases the trust between parties and can create confusion over the nature and quality of service being provided.	a) Publish the SLA and KPI definitions so that they are easily accessible and clear. Clarify Core Service Hours and Key Performance Indicators (KPIs) that are related to service quality. b) Communicate expected resolution timeframes to Council staff when they report incidents and keep them informed if the timeframe is exceeded.	**LOW**	**Action:** (a) Recommendation accepted **Responsible Officer:** Head of Information Management **Target date:** 15th April 2016 **Action:** (b) Recommendation accepted & completed **Responsible Officer:** Head of Service Delivery (CSG) **Target date:** 4th April 2016

Ref	Finding	Risk	Recommendation	Risk category	Management Response and Agreed Action
	IT service for resolving these incidents is only available from 8am to 6pm.				

Appendix 1 – Questions from Councillor Cooke

ID	Question from Councillor Cooke	Information received from Capita during the audit	Audit finding reference and comments
1	Does every system have a lead user and at least one deputy?	Within the CSG delivery, each system would be assigned to a team such as Infrastructure, Desktop or Application. An example of this would be the Infrastructure team leading Emails, the Desktop team leading Office Applications and the Applications team leading Business Objects. For Barnet Council, a list of IT and business lead users are assigned for each system and manually maintained in an 'applications register' which consists of a static spreadsheet. Details of lead users are supplied by the Council for critical systems. CSG are reliant on accurate and complete information being supplied to the CSG Applications Support Team.	**Finding Reference 1.1** Each system should be formally defined as a Configuration Item (CI) and contain various attributes, including information about their owner. The CIs should be implemented into a scalable, relational Configuration Management Database (CMDB) and updated regularly.
2	Do planned changes include systems analysis to identify all dependencies and data flows (rather than relying on application support knowledge and documentation that may not cover dependencies external to the application in question)?	Analysis is the responsibility of the person raising the change and dependencies are discussed with a range of teams and solutions architects within the Technical CAB and Client CAB.	**Finding Reference 1.1** Although dependencies are discussed within the Technical CAB and business impact is discussed within the newly created Customer CAB, the quality of this information is highly dependent on the expertise and knowledge of the representative attending the meeting. Dependency information should be captured as relationships between CIs, updated regularly and stored in a CMDB to allow the impact of changes to be assessed consistently and accurately.

ID	Question from Councillor Cooke	Information received from Capita during the audit	Audit finding reference and comments
3	For every system, are there separate environments for Development, Testing (formal testing by the developer), Acceptance Testing (by the lead business user or their nominee) and Production (live environment)?	No, only a few systems have test environments and for those systems with no testing environment, changes are implemented directly into the live environment without prior testing. This is due to a cost decision and the risk has been accepted by Barnet Council.	**Finding Reference 2.1** Identify which IT systems could have an unacceptable impact to the Council's services in the event of an outage. For these systems, ensure that a separate like-for-like environment exists (with equivalent hardware specification and software versions) for testing and releasing IT changes prior to implementation into the live environment. This reduces the probability of impacting the Council's services due to unforeseen problems during implementation. Where appropriate investment into a test environment is not approved, ensure that the risk of IT change is formally accepted by Barnet Council and is documented and reviewed regularly by CSG and Barnet Council management.
4	What differences exist between non-production (testing) environments and the corresponding production (live) environments (such as database capacity) and what impact do they have on the validity of tests?	Where production and non-production environments are available, the environments may not be the same (in order to reduce costs), e.g. the storage may be on a slower disc for the non-production environment. These differences need to be considered when devising tests, to ensure the results would be valid for the production system.	**Finding Reference 2.1** Identify which IT systems could have an unacceptable impact to the Council's services in the event of an outage. For these systems, ensure that a separate like-for-like environment exists (with equivalent hardware specification and software versions) for testing and releasing IT changes prior to implementation into the live environment. This reduces the probability of impacting the Council's services due to unforeseen problems during implementation.
5	Do programming languages used have formally adopted coding standards?	CSG do not produce any code; this type of work would be carried out by third parties.	**Finding Reference N/A** Not within the audit scope.

ID	Question from Councillor Cooke	Information received from Capita during the audit	Audit finding reference and comments
6	Are code changes labelled with their date, the version into which they are introduced, their purpose and author?	CSG do not produce any code; this type of work would be carried out by third parties.	**Finding Reference N/A** Not within the audit scope.
7	Are code changes subject to peer review before being promoted to the Test environment?	Where a third party is contracted to change code, e.g. the delivery of the Council's website or "My Account", the code would go through peer review, smoke testing and UAT on the non-production environment before release.	**Finding Reference N/A** Not within the audit scope.
8	Are access privileges assigned appropriately by a specialist group, e.g. developers having only 'user' privileges in the Acceptance Testing and Production environments?	Yes, where appropriate.	**Finding Reference N/A** Not within the audit scope.
9	Are software versions kept under configuration control with audit trails of changes?	No, this is not in place.	**Finding Reference 1.1** Each piece of software should be formally defined as a Configuration Item (CI) and contain various attributes, including information about their version control. The CIs should be implemented into a scalable, relational Configuration Management Database (CMDB) and updated regularly.
10	Is approval (preferably using a specialist software tool) by all stakeholders a pre-requisite for consideration of a change proposal by the Change Advisory Board (CAB) (except in cases of urgency)?	Yes, changes are reviewed by the Change Manager and invites are sent out for the requestor and appropriate representatives to attend Technical CAB/ Customer CAB in order to approve the Change Request. This process is managed through the ServiceNow specialist toolset.	**Finding References 3.1 to 3.5** Evidence was found as part of the audit to support this information provided.

ID	Question from Councillor Cooke	Information received from Capita during the audit	Audit finding reference and comments
11	Must a developer attend CAB personally or by telephone in order to answer queries?	Attendance is accepted either in person or by telephone. The representative is expected to answer questions and be challenged on the change and potential risk impact.	**Finding References 3.1 to 3.5** Evidence was found as part of the audit to support this information provided.
12	Does the CAB satisfy itself that the developer has identified all the stakeholders, e.g. users who access the system remotely as well as from Council offices?	Yes, CAB always ensures that all business users and stakeholders are aware. If necessary, the technical or project manager attends customer CAB. IT changes are postponed if there is insufficient representation at the CAB to review a change.	**Finding References 3.1 to 3.5** Evidence was found as part of the audit to support this information provided.
13	Do change plans include a back-out procedure in case something goes wrong? Are they implemented?	The IT Change Management procedure requires steps for a controlled back-out to be included in each change record. It was found that the back-out plan was not always tested prior to changes being implemented and details of the required steps were often broadly documented as 'restore from backup'. Without testing the back-out plan, it is unknown whether changes can be successfully reversed and achieved within the agreed change management window.	**Finding Reference 2.2** Back-out plans should be tested to confirm that the procedure can be executed within the expected change window and under which conditions the back-out plan should be invoked. Restoration times should be accurately known and tested for any data restorations that need to be performed from back-up. Where back-out plans cannot be tested, this risk should be made aware to the Technical and Customer CAB when presenting the change request and formally documented in the change record.

ID	Question from Councillor Cooke	Information received from Capita during the audit	Audit finding reference and comments
14	Does the CAB review all attempted changes after implementation whether deemed successful or not?	No, changes are not reviewed by CSG post implementation, unless specifically requested by Barnet Council (ad-hoc) or unless a major incident arises from a failed change.	**Finding Reference 1.2** All changes should be evaluated post-implementation and a mandatory review should be performed on all failed changes so that the cause of failure can be identified. Change records should be closed once the evaluation has been completed. Change Management service metrics should be produced regularly to monitor and drive improvements.

Appendix 2 – Definition of recommendation priorities

Individual finding ratings

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation or brand of the Council which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation or brand of the Council.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation or brand of the Council.
Low	A finding that could have a: • ***Minor*** impact on the Council's operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the Council.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Appendix 3 – Analysis of findings

Area	Critical		High		Medium		Low		Total
	D	OE	D	OE	D	OE	D	OE	
Change Management Process	-	-	2	-	-	2	-	-	**4**
IT Operational Changes	-	-	-	-	-	1	1	-	**2**
Total	**-**	**-**	**2**	**-**	**-**	**3**	**1**	**-**	**6**

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:**
18/02/2016	23/02/2016	04/03/2016	14/03/2016	05/04/16 to 11/04/16	12/4/16

Appendix 4 – Internal Audit roles and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken the review of *the IT Change Management Process*, 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.

Future periods

Our assessment of controls is for the 2015/16 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 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.