Putting the Community First

BARNET
LONDON BOROUGH

**Appendix 2**

# Internal Audit
# IT Change Management Review
# Follow-up: Phase 2 of 2 (November 2016)

## Executive Summary

An internal audit was conducted in March 2016 to review the appropriateness and effectiveness of the Council’s 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 the Council’s services. The audit highlighted a number of issues and as a result, 6 overarching recommendations were made with 30 agreed actions underpinning them.

The follow up reviews have been undertaken using a two phased approach. Phase 1 was conducted in June 2016 and considered the recommendations that were made regarding control design to address deficiencies identified in the internal audit. Phase 1 was also determined by the actions that were marked as either completed within the internal audit report, or where the action due date was set for April or May 2016.

Phase 2 was conducted in November 2016 and considered all the outstanding actions considering the extent to which controls have been designed, embedded and are operating effectively over a period of time. Of the 30 actions highlighted from the original audit in March 2016, 14 were followed up during Phase 1 from which 8 were implemented. Therefore, it resulted that 22 actions were still open to be reviewed during Phase 2 and final follow up. From those, 5 (23%) have been implemented while 11 (50%) are still in progress and 6 (27%) have not been addressed (no progress has been made with implementing the original agreed action).

During the Phase 2 review, we were informed that the service management toolset in use (ServiceNow) will be enhanced during the first half of 2017 to help better manage some of the IT service management processes, including Change Management. We have been informed that some of the outstanding findings have therefore not yet been addressed, due to this impending project and their due dates have therefore been revised accordingly.

| Status | Description | Phase 1 Results | Phase 2 Results | Current Status |
|---|---|---|---|---|
| Implemented | Evidence provided to demonstrate that the action is complete | 8 / 14 | 5 / 22 | 13 / 30 |
| Partially Implemented | Evidence provided to show that progress has been made but the action is not yet complete | 3 / 14 | 11 / 22 | 11 / 30 |
| Unconfirmed | Exceptional case where evidence was unable to be provided but both the Council and Capita CSG confirm that the action is complete | 1 / 14 | - | - |
| Not Implemented | No evidence seen of the action being progressed or completed | 2 / 14 | 6 / 22 | 6 / 30 |

| Status | Description | High Priority | Medium Priority | Low Priority | Total |
|---|---|---|---|---|---|
| Implemented | Evidence provided to demonstrate that the action is complete | 4 / 14 | 6 / 13 | 3 / 3 | 13 |
| Partially Implemented | Evidence provided to show that progress has been made but the action is not yet complete | 6 / 14 | 5 / 13 | - | 11 |
| Not Implemented | No evidence seen of the action being progressed or completed | 4 / 14 | 2 / 13 | - | 6 |

Since the audit fieldwork in November, management have taken further action and a summary of progress at January 2017 as per management is below. **This has not been verified by audit** but is included here for reference.

| Status | Description | High Priority | Medium Priority | Low Priority | Total |
|---|---|---|---|---|---|
| Implemented | Evidence provided to demonstrate that the action is complete | 10 / 14 | 9 / 13 | 3 / 3 | 22 |
| Partially Implemented | Evidence provided to show that progress has been made but the action is not yet complete | 3 / 14 | 3 / 13 | - | 5 |
| Not Implemented | No evidence seen of the action being progressed or completed | 1 / 14 | 1 / 13 | - | 2 |

## 2) Detailed Status Updates

| Audit finding, date and recommendation (March 2016) | Audit follow-up status (November 2016) |
|---|---|
| **1) Process Lifecycle: Control design – High Risk** | |
| 1.1 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.<br>**Action:** Recommendation accepted<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 31st August 2016<br>**New target date:** 30th June 2017 | **Not Implemented**<br>We examined *P0073 Operational Procedure for CMDB updates* (issued 12th October 2016).<br>We noted that this document is in a draft stage and outlines the process to update the *Current Fixed Asset v7* spreadsheet (in lieu of a relational CMDB). Since the last review, we noted that the spreadsheets have been updated to include the latest CMDB information and that the Change Management process is designed to keep this data current. However, the spreadsheet still does not record dependencies between CIs (Configuration Items) and therefore it is not possible to identify the dependent IT services that may be impacted by a change. Migration to a scalable relational configuration management database is planned but yet to be implemented.<br>Capita has advised that this recommendation is planned to be addressed with the new implementation of ServiceNow in 2017. |
| b) Ensure that CIs are routinely updated into the CMDB through the IT Change Management process.<br>**Action:** Recommendation accepted<br>**Responsible Officer:**<br>Head of Service Delivery (CSG) | **Implemented**<br>We examined *P0073 Operational Procedure for CMDB updates* (issued 12th October 2016) and the *Current Fixed Asset v7* spreadsheet.<br>We noted that there is a process to update the spreadsheet (see finding 1.1a). When analysing it, we observed that:<br>• CIs are not deleted but are struck through when updates are made, preserving an auditable trail; |

| | |
|---|---|
| **Original target date:** 31st August 2016 | • There is a version control page outlining the latest CIs for each asset; and<br>• It is updated by the owner of each area (e.g. network, server estate, applications) and reviewed by the IT Change Manager prior to closing the change record.<br><br>We examined a sample of 25 change records between 7th June 2016 and 2nd November 2016 that were recorded within the ServiceNow service management toolset and noted that:<br>• The workflow has been updated with instructions to update the CMDB and Post Implementation review steps, prior to the IT Change Manager closing the ticket; and<br>• Within the notes field of all 25 change records, we were able to confirm a note from the change implementer stating whether the CMDB needed to be updated or not.<br><br>Therefore, although a formal relational CMDB is yet to be implemented, a process to routinely update changes to configuration records through the IT Change Management process is in place. |
| 1.2 Changes are not reviewed to determine whether they were 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. | |
| c) Perform post-change evaluations and ensure change records are closed<br><br>**Action:** Recommendation accepted<br><br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br><br>**Original target date:** 31st August 2016<br>**New target date:** 2nd January 2017<br><br>**Note: As per management this was fully implemented on 2nd January 2017. This has not been verified by audit.** | **Partially Implemented**<br><br>**Note: As per management this was fully implemented on 2nd January 2017. This has not been verified by audit.**<br><br>As noted in 1.1b, as part of updating the change logs in the CMDB, post-change evaluations are conducted.<br><br>We noted that the IT Change Manager reviews all the change records before closing them. However there is currently a backlog that the IT Change Manager is yet to complete.<br><br>We have also examined a sample of 25 change records between 7th June 2016 and 2nd November 2016 recorded within ServiceNow and noted that 13 are not marked as closed (52%). From those, 10 were marked as implemented as follows:<br>• 3 were marked as implemented more than 2 months ago:<br>○ 1 Minor change; |

| | |
|---|---|
| | ○ 1 Significant change; and<br>○ 1 Major change.<br>• 4 were marked as implemented in September:<br>○ 3 Significant changes;<br>○ 1 Major change.<br>• 3 were marked as implemented in October:<br>○ 1 Minor change;<br>○ 2 Significant changes.<br>10 change records remain open due to the IT Change Manager needing to work through a backlog of change requests. |
| 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 additional change training and support.<br>**Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 2nd September 2016<br>**New target date:** 30th June 2017 | **<u>Partially Implemented</u>**<br>We examined the *ICT Monthly Report July*, *ICT CSG Monthly Report August v2* and *ICT CSG Monthly Report September.*<br>From the documents reviewed, metrics are provided on:<br>• The number of major, significant and minor changes<br>• The number of changes progressed and approved via Technical and Customer CABs<br>• The number of failed changes raised.<br>The report currently lacks commentary to analyse the data. It should be noted that the process to extract the number of failed changes is manual as ServiceNow has not been configured to provide such information. Therefore, to mitigate the residual risk of the accuracy of data a new change request status (e.g. Cancelled, Failed, etc.) should be included in ServiceNow to reflect the real status of each change. We have been advised that this will be addressed as part of the new implementation of ServiceNow in 2017. |
| 1.3. 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. | |
| b) Incorporate project-related changes to the existing reports. | **<u>Partially Implemented</u>** |

| | |
|---|---|
| **Action:** Recommendation accepted<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 12th April 2016<br>**New target date:** 28th February 2017 | We examined the *ICT Monthly Report July*, *ICT CSG Monthly Report August v2* and *ICT CSG Monthly Report September.*<br>From the documents reviewed, we noted that only the September report included the number of project-related changes. However, it wasn't possible to understand how many major, minor, emergency or standard changes were raised regarding projects, or how many project related changes failed. We were also able to examine the final November report where details about project-related changes were provided, however the report lacked commentary to analyse the data.<br>Given that this finding was due to be implemented in April and that evidence of the implementation was only seen at the end of this review (in November), we can conclude that the monthly report is still evolving and therefore not yet embedded or at the required level of maturity. Once the report format has been finalised, a template or documented procedure would be helpful, to ensure consistency with the information reported upon each month. |
| **2) Change Testing & Validation: Control design - High Risk** | |
| 2.1 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) Identify which IT services could have an unacceptable impact to the Council's services should there be a prolonged outage.<br>**Action:** Recommendation accepted<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>IT Contract Manager (LLB)<br>**Original target date:** 28th October 2016<br>**New target date:** 31st March 2017 | **Partially Implemented**<br>We examined *P0066 Systems and Applications register v1* as well as a sample of emails exchanged with the business to address the criticality of each system.<br>We noted that a re-classification of all IT service criticalities was performed as a one-off exercise for ascertaining IT DR requirements. A tiered (Tier 1, Tier 2 and no DR) approach was taken to re-classify the IT Services with the business involvement and approval.<br>Capita stated that a formal annual review of the criticality list is planned, however no evidence of this formal process has been seen. In addition, the process to update system criticality from a change management perspective is not clearly documented or defined.<br>We were also informed that changes required in the mid-year can be addressed in the monthly Service |

| | |
|---|---|
| | Review Meeting, Project Operating Board and Delivery Board, however, evidence of these reviews were not provided.<br>It is also worth noting that technical work has yet to be undertaken to implement the DR arrangements in line with the reclassification of tiers. It is therefore not yet possible to differentiate the level of change control required by the criticality of each IT service. |
| 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.<br>**Action:** Recommendation accepted<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>Operations Manager (CSG)<br>**Original target date**: 8th July 2016<br>**New target date:** 2nd January 2017<br>**Note: As per management this was fully implemented on 2nd January 2017. This has not been verified by audit.** | **Partially Implemented**<br>**Note: As per management this was fully implemented on 2nd January 2017. This has not been verified by audit.**<br>We examined *P0066 Systems and Applications Register v1.*<br>We noted from the documentation reviewed that there is a record of which applications have a User Acceptance Testing (UAT) environment.<br>Additionally, there is a record of whether test and production environments are like-for-like. Out of 129 applications, 100 (78%) do not have test environments. For the remaining 29, 11 (38%) do not have a like-for-like environment. During our interviews we were informed that whenever a change is requested to a system without a test environment, options are presented to Council for their consideration.<br>Although an example has been provided where the implementation of a new Social Care system included a test environment, no documentation was provided to evidence that a solution was presented to Council regarding changes to an implemented system without a test environment. Therefore we were unable to confirm the extent to which this process is operationally embedded. Documentation that demonstrates alternative proposed options which were presented to Council, along with Council's response should be collated and attached to the change record in order to mitigate the risk. |
| c) Where proposed options are declined by the Council, ensure that the risk of IT change is formally accepted by the Council and is reviewed regularly by CSG and Barnet Council management. | **Partially Implemented**<br>**Note: As per management this was fully implemented on 9th January 2017. This has not been verified by audit.**<br>Based on the previous finding 2.1b and the sample reviewed, there was no evidence regarding a formal |

| | |
|---|---|
| **Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>Head of Projects and Programs (CSG)<br>Head of Service Delivery (CSG)<br>Operations Manager (CSG)<br>**Original Target date:** 8th July 2016<br>**New target date:** 9th January 2017<br>**<u>Note: As per management this was fully implemented on 9th January 2017. This has not been verified by audit.</u>** | acceptance of risk by Council.<br>However, Council has informed us that these discussions do take place and that the business is aware of the risks and accept them. As this risk acceptance is not formally recorded, we were unable to evidence that this is occurring. Documentation that demonstrates alternative proposed options which were presented to Council, along with Council's response should be collated and attached to the change record in order to mitigate the risk. |
| 2.2 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 risk should be made aware to the Technical and Customer CAB when presenting the RFC and formally documented in the change record.<br>**Action:** Recommendation accepted & completed | **<u>Not Implemented</u>**<br>**<u>Note: As per management this was fully implemented on 2nd January 2017. This has not been verified by audit.</u>**<br>We reviewed 25 records between 7th June 2016 and 2nd November 2016.<br>During a walkthrough of ServiceNow, we noted that:<br>• 8 out of 25 records (32%) were Cancelled (6 records) or Informational only (2 records);<br>• There was no evidence showing testing of back-out plans for any of the remaining 17 change records. |

| | |
|---|---|
| **Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 12th April 2016<br>**New target date:** 2nd January 2017<br>**Note: As per management this was fully implemented on 2nd January 2017. This has not been verified by audit.** | Additionally, where back-out plans could not be tested, the associated risks were not escalated to the Technical and Customer CAB. |
| b) Specify under which conditions the back-out plan should be invoked.<br>**Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 12th April 2016<br>**New target date:** 2nd January 2017<br>**Note: As per management this was fully implemented on 2nd January 2017. This has not been verified by audit.** | **Not Implemented**<br>**Note: As per management this was fully implemented on 2nd January 2017. This has not been verified by audit.**<br>We reviewed 25 change records between 7th June 2016 and 2nd November 2016 and noted that there is no defined criteria to invoke the back-out plan for any of the reviewed change records.<br>Consequently, change requesters will not know when a back-out plan should be executed, increasing the likelihood and impact of a prolonged outage. |
| 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.<br>**Action:** Recommendation accepted & completed | **Not Implemented**<br>**Note: As per management this was fully implemented on 9th January 2017. This has not been verified by audit.**<br>During the walkthrough of change records in ServiceNow, we noted that there is no evidence of testing of a back-out plan. Therefore, when the procedure is dependent upon data restoration from backup, no |

| | |
|---|---|
| **Responsible Officer:**<br>Operations Manager (CSG)<br>**Original target date:** 4th April 2016<br>**New target date:** 9th January 2017<br>**Note: As per management this was fully implemented on 9th January 2017. This has not been verified by audit.** | test is performed to ensure:<br>a) The restoration time is known.<br>b) The back-out plan will work.<br>We have been advised that the time needed for a complete data restoration of the IT estate is 12 hours, however this 12-hour window is not built into the change time window. The current practice is to base the change time window on experience of previous data restorations. While experience may indicate that a shorter restoration time is possible, this is not guaranteed and as such, the data restoration time should be communicated as 12 hours (worst case scenario) for approval by the CAB. |
| **3) Result of Sample Records Testing: Operating effectiveness – Medium Risk** | |
| 3.1 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.<br>**Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>Head of Service Delivery (CSG) | **Partially Implemented**<br>**Note: As per management this was fully implemented on 5th December 2016. This has not been verified by audit.**<br>We reviewed 25 change records between 7th June 2016 and 2nd November 2016.<br>Of the 25 change records sampled, 8 change records (32%) were marked as being major changes which, in line with Change Management procedures, require a full work plan. From the 8 major changes we noted:<br>• 7 records (87.5%) included a full work plan;<br>• 1 record (12.5%) did not include a full work plan however, the IT Change Manager did not classify |

| | |
|---|---|
| **Original target date:** 4th April 2016<br>**New target date:** 5th December 2016<br>**Note: As per management this was fully implemented on 5th December 2016. This has not been verified by audit.** | that record as a major change.<br>After further analysis, the record that did not include a full work plan referred to a firewall change which is templated and classified as a standard minor change. After reviewing the impact assessment, we noted that not all fields are correctly populated (they are blank) and cannot be changed (fields are blocked for amendments). We noted the change was reviewed at Technical CAB as a minor change. We were also informed by Capita that this was due to a manual error while reviewing the change.<br>It is worth mentioning that the risk assessment was not fully populated in ServiceNow which, by default, should have flagged this change as a major change. This situation highlights the risk of human error leading to incorrect change classification which may lead to lack of governance on major changes (accidentally classified as minor changes) which can then lead to unexpected IT outages. |
| 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 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.<br>**Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>IT Contract Manager (LBB)<br>Head of Service Delivery (CSG)<br>**Original target date:** 4th April 2016<br>**New target date:** 31st March 2017 | **Not Implemented**<br>We examined *P0035 Server Estate Patching by Capita Central Services v2* (issued 14th November 2015) and *P0020 v5 Desktop Patch Management Policy* (issued 5th November 2016).<br>Changes are not reviewed to determine how they could be built, tested and deployed together. As a result, more releases may be raised than is necessary, resulting in an increased risk to the number of change-related outages. |

| | |
|---|---|
| 3.2 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 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.<br>**Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original Target date:** 4th April 2016 | **Implemented**<br>We reviewed 25 change records between 7th June 2016 and 2nd November 2016 of which 8 were considered to be standard or emergency changes.<br>6 of the 8 records (75%) included a back-out plan and although 2 of the 8 records (25%) did not have back-out plans defined, they were "Informational only" changes and as such, did not require a back-out plan to be provided. |
| 3.3 A lack of test plan increases the likelihood of unforeseen IT incidents during release/implementation which may cause an impact to Council services. | |
| a) The IT Change Manager must ensure that essential documentation including test plans are in place for all standard and emergency change requests. Where not applicable, clear justification should be provided and documented.<br>**Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>Head of Service Delivery (CSG) | **Partially Implemented**<br>**Note: As per management this was fully implemented on 5th December 2016. This has not been verified by audit.**<br>We reviewed 25 records between 7th June 2016 and 2nd November 2016 of which 8 were considered to be standard or emergency changes.<br>For 1 record (12.5%) from the 8, a test plan was not provided and no clear justification was documented.<br>Additionally, for the remaining change records, results of testing were not documented. |

| | |
|---|---|
| **Original target date:** 4th April 2016<br>**New target date:** 5th December 2016<br>**Note: As per management this was fully implemented on 5th December 2016. This has not been verified by audit.** | |
| 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.<br>**Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 8th July 2016<br>**New target date:** 2nd December 2016<br>**Note: As per management this was fully implemented on 2nd December 2016. This has not been verified by audit.** | **Not Implemented**<br>**Note: As per management this was fully implemented on 2nd December 2016. This has not been verified by audit.**<br>As mentioned in 2.1b, we examined *P0066 Systems and Applications Register v1* and noted that out of 129 applications, 100 (78%) do not have test environments. For the remaining 29, 11 (38%) do not have a like-for-like environment.<br>We did not see evidence of stakeholders being aware of the risks of not having like-for-like configured test environments and their corresponding response in accepting the risks. |
| 3.4 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. | **Partially Implemented**<br>As mentioned in 1.1b, we examined *P0073 Operational Procedure for CMDB updates* (issued 12th |

| | |
|---|---|
| **Action:** Recommendation accepted<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 31st August 2016<br>**New target date:** 28th February 2017 | October 2016) that outlines the process to update the *Current Fixed Asset v7* spreadsheet (considered to be the CMDB). As part of that process, the IT Change Manager is responsible for the review and closure of all the change records.<br>For further information, please refer to finding 1.2 c. We have been advised that an additional resource is being recruited in January to assist with the Change and Configuration Management process and that this should help clear the backlog. |
| b) The Configuration Management process requires maturity, to ensure all configuration information is captured and updated in a timely manner.<br>**Action:** Recommendation accepted<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 31st August 2016<br>**New target date:** 30th June 2017 | **<u>Partially Implemented</u>**<br>We examined *P0073 Operational Procedure for CMDB updates* which is still in draft (dated 12th October 2016). This document outlines the process to update the *Current Fixed Asset v7* Spreadsheet and noted that:<br>• Within that process, CIs are not deleted but are struck through.<br>• A version control front page is created in the spreadsheet, outlining the latest CIs for each asset.<br>From the walkthrough within ServiceNow, we were also able to note that:<br>• The ServiceNow workflow was updated to include a step to confirm whether the CMDB needs to be updated or not, which is reviewed by the IT Change Manager.<br>• Within the notes field of each change record we were able to confirm a note from the implementer stating if the CMDB needed to be updated or not.<br>Although a process to update the CMDB is in place, we concluded that:<br>• A scalable relational configuration management database is yet to be implemented leading to a lack of dependency linkage between CIs.<br>• The CMDB was initially updated based on discovery tools. However, since that period it now relies on manual updates from the change implementer and post-implementation review done by the IT Change Manager.<br>We noted that with an average of 80 change requests made each month, the process in place is not able to handle the volume of updates required, and this has resulted in a backlog of configuration updates. Consequently, there is still a risk of change records not being closed in a timely manner, resulting in |

<table>
<tr><td></td><td>inaccurate status reporting and potential inaccuracies to IT configuration information available for future IT change impact assessments.<br>We have been advised that an additional resource is being recruited in January to assist with the Change and Configuration Management process and that this should help clear the backlog. Furthermore, we have been advised that the implementation of the ServiceNow upgrade is intended to address these process deficiencies.</td></tr>
<tr><td colspan="2"><b>4) Continuous Service Improvement – Operating Effectiveness - Medium Risk</b></td></tr>
<tr><td colspan="2">4.1 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. Design and operating deficiencies within the change management process cannot be effectively identified unless the cause of failed change is known. Lack of understanding behind failed changes prohibits service improvement and can result in a repeat of incidents.</td></tr>
<tr><td>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.<br><b>Action:</b> Recommendation accepted &amp; completed<br><b>Responsible Officer:</b><br>Head of Service Delivery (CSG)<br><b>Original target date:</b> 4th April 2016</td><td><b><u>Implemented</u></b><br>We examined June 2016 Failed Change Review minutes (dated 27/07/2016) as well as Failed Change Reports CHG0054614, CHG0055977, CHG0054472, CHG0055824 and CHG0056343.<br>We noted that, in each failed change report, information was provided documenting:<br>• The situation around the failed change;<br>• Possible root cause; and<br>• What steps should be taken to ensure that changes of a similar nature do not fail in the future.</td></tr>
<tr><td colspan="2">4.2 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.</td></tr>
<tr><td>Review all failed changes for root cause analysis and lessons learned. Routinely review and consolidate the lessons learned into the</td><td><b><u>Partially Implemented</u></b></td></tr>
</table>

<table>
<tr><td>Service Improvement Plan, to prevent similar incidents repeating in the future.<br><br>**Action:** Recommendation accepted &amp; completed<br><br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br><br>**Original target date:** 4th April 2016<br>**New target date:** 28th February 2017</td><td>We examined *July 2016 Failed Change Review minutes* (dated 27/07/2016) as well as the *P0030 Change Management Procedure*.<br><br>• We noted that failed changes are reviewed quarterly and that these are also reported in the monthly service report.<br>• Failed change reports are reviewed in the monthly meetings in order to validate trends and common issues.<br><br>However, a Service Improvement Plan in which to formally consolidate lessons learned and enable Continuous Service Improvement is not in place.<br><br>It should also be noted that at the time of this review, a major incident and failed changes tracker has been recently designed. This is intended to centralise information relating to the root cause of incidents and failed changes as well as to enable analysis for lessons learned.<br><br>We have been advised that since November, failed changes have started to be reviewed with the Council fortnightly. To consider this risk fully mitigated, we would need to evidence a fully embedded process where failed changes were reviewed and actions captured in the service improvement plan on a regular basis.</td></tr>
<tr><td colspan="2">**5) Governance of IT Change Management: Control design - Medium Risk**</td></tr>
<tr><td colspan="2">5.2 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 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 Changes fails or is scheduled at a time that is vital to business operations.</td></tr>
<tr><td>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.<br><br>**Action:** Recommendation accepted &amp;</td><td>**Implemented**<br><br>We examined *P0060 Terms of Reference for Technical CAB for the London Borough of Barnet v1.1* dated 22nd June 2016.<br><br>We were able to see evidence that further revisions have been made since the Phase 1 review. The document was approved by the CSG Service Delivery Manager on 22nd June 2016. Evidence to show</td></tr>
</table>

| | |
|---|---|
| completed<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Original target date:** 8th July 2016 | review by the Council was no longer required as this is an internal Capita document.<br>We also examined *P0069 Terms of Reference for Customer CAB for the London Borough of Barnet v1.1* dated 25th October 2016.<br>This document was reviewed with Council management and acceptance was confirmed via an email dated 25th October 2016. Implementation of this document is considered complete. |
| **6) Expectations Management – Control Design – Low Risk** | |
| 6.1. 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.<br>**Action:** Recommendation accepted & completed<br>**Responsible Officer:**<br>Head of Service Delivery (CSG)<br>**Target date:** 28th October 2016 | **Implemented**<br>We examined the intranet page where the SLAs and KPIs are made available to the Council Staff.<br>We noted that definitions for KPIs such as Critical Availability, User Satisfaction, Incident Resolution and Year 1 targets are provided as well as measurement periods for KPIs.<br>We also examined *ICT Monthly Report July, ICT CSG Monthly Report August v2* and *ICT CSG Monthly Report September* where we were able to confirm that the Service Quality is reported to the Council's Senior Management Team. |