Internal Audit Report
Corporate and Democratic Services
IT Change Management
Assignment No. 17- 23
March 2018

Final Report (Report No. 18/169)

Finance Division
Corporate and Democratic Services
Perth & Kinross Council
Council Offices
2 High Street
Perth
PH1 5PH

Internal Audit

“Internal Audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes”. Public Sector Internal Auditing Standards (PSIAS)

On 27th March 2013, the Council’s Audit Committee approved the PSIAS as the relevant standard for its Internal Audit activity.

Background and Introduction

This audit was carried out as part of the audit plan for 2017/18, which was approved by the Audit Committee on 18 April 2017.

The Council’s ICT Strategy is the Digital Strategy for 2016 – 2020 and IT Change Management follows the IT Service Management model and Policy agreed in 2011. This policy has been reviewed and continues as the current policy and is available on ERIC for Council users to read.

The Council follows the principles of Change Management defined by IT Service Management and the industry standard framework of ITIL (Information Technology Infrastructure Library) Service Management. ITIL, sets out the primary mission of the IT change management process as being to implement changes efficiently whilst minimising any negative impact on customers.

IT Change requests can be either pre-authorised standard change or planned change. A standard change is a change to a service or infrastructure when the approach is pre-authorised by change management and has an accepted and established procedure to provide a specific change requirement. Risk of standard change is usually low, and activities/tasks are well known, documented and proven.

Planned changes are different in that they must follow the complete change management process; they are often categorised according to risk and impact to the organisation/business. Those that are categorised as medium or high risk will be reviewed by the Change Advisory Board (CAB). A formal request for change is made on a form based on the ITIL template style.

Emergency change is a ‘drop everything to restore services’ type. They are designed to repair any error in an IT Service which is negatively impacting the business to a high degree. They may not all require Manager involvement and may in some cases be delegated to support teams to action, document and report on. Some documentation may be done retrospectively in an emergency situation.

The change management process is controlled with a process map based on documentation and decision stages, quality assurance checks and approvals. The process map defines these to ensure certain actions are completed before a change can move from one stage to the next.

Responsibilities for management of change sits with the Change Advisory Board and Team Leader in IT Services. The CAB review requests for change in context of associated risk impact assessment by the IT Change Technical Owner, then recommend on the change future – approve, reject or defer, pending further details or rescheduling.

Since the IT Change Management Assignment no 14-15 reported to Audit Committee in 2015, there have been changes to the IT Change Management processes. From September 2017, requests for change have moved onto the IT Service's Service Management Tool, Service Desk. Prior to this, user requests were emailed to the IT Customer and Business Services team who input and completed change management documentation using paper, spreadsheets and email. Benefits and change resulting from the new Service Desk environment are currently being assessed by the Team to confirm that the process map and change forms are sufficient and provide necessary detail.

Scope and Limitations

The audit work consisted of interviews with key officers, sample testing of Requests For Change (RFC) raised in the financial year 2017-2018 and a review of emergency change to ensure the adequacy of service. Field work was carried out in March 2018. This audit did not include Release Management and Project Management changes.

Control Objectives and Opinions

This section describes the purpose of the audit and summarises the results. A 'control objective' is a management objective that requires the maintenance of adequate and effective internal controls to ensure that it is achieved. Each control objective has been given a rating describing, on the basis of the audit work done, the actual strength of the internal controls found to be in place. Areas of good or poor practice are described where appropriate.

Control Objective 1: Governance - ensure that Framework Policy and Procedures for IT Change management are in place and comply with IT management best practice and Council corporate strategy and business plans to ensure consistent and timely processing of changes.
Audit Comments: Policy and procedures are available to provide consistency and governance for IT Change Management. The Council's ICT Change Management Policy dated 2011 remains as the current policy. There is no document management section giving details of contributors and version control to confirm this. The Council follows the ITIL best practice standard for managing change. Templates based on ITIL have been designed to meet the needs of the Council process and are regularly reviewed to confirm their usefulness. Procedures for IT Change and responsibilities are found in the following documents produced in 2015 - • CM ICT Business Owner Guidance • CM IT Tech Owner Guidance and • Approach to Change Advisory Board including Team Leaders • CAB Operating Guidelines There is also a Change Matrix document for considerations and categorisations of

risk and complexity scoring. ICT Services plan to revise procedures documentation once the ICT Change Management Team have reached a version for the new Service Desk process that satisfies both ICT customers and ICT Service needs, whilst adhering to a quality management standard. Changes may require approval by the CAB. Change Advisory Boards (CABs) are the IT industry-standard vehicle for involving IT users, with appropriate skill and authority, to influence and contribute materially to decisions about changes to the IT services they receive. The CAB Operating Guidelines defines the CAB structure and roles, communications, meetings and emergency CAB meetings plus indicative CAB timelines for responding to planned change.

Strength of Internal Controls:	Strong

Control Objective 2: Ensure that Change control is recorded for confirmation that change is controlled and authorised at each stage.
The request for change process map and ICT change management flow diagram define process stages, decision points and options and provide a useful reference when reviewing progress of change. RFCs progress through each stage towards final approval or rejection. Within the process quality assurance checks are carried out by the team. For example, within free-form fields, there is a check to ensure sufficient detail is provided before the RFC can move to the next stage. Authorisation of change is in line with the risk / impact level. For example, Standard change has minimal / no impact and risk; these are repetitive tasks agreed and listed by the Team and have a lower level of approval. Planned minor change can require some authorisation through the Change Advisory Board which is comprised of IT Team Leaders. For highest risk, there has to be a majority of the CAB in favour of change – that is a minimum of 3 out of 5 CAB members agreeable. Minor change requires less. Authorisation is recorded within the RFC and change will not continue through processing until required authorisation is achieved. Change Management processes are recorded at each stage of the change process, with username and date-stamp maintained in audit logs for reference. User requests are logged by IT staff through Service Desk (with the user as the requestor of the RFC). Users can view their RFC via the Self Service portal and will receive Service Desk updates once the RFC has been approved by the CAB. After CAB approval at stage 3, the RFC can be accepted; change implementation scheduled and the IT Technical Owner builds and tests change. When this is successful and a rollback plan is created, the change can then be implemented in the live environment. A sample check of RFC’s found all complied with controls in the process stages.

Strength of Internal Controls:	Strong

Control Objective 3: Ensure that Monitoring of change control is carried out and checks made to confirm changes made have produced the required outcomes including compliance with the Council change management policy framework.	
Performance of the Change Management process is reported within the operational monthly IT Performance Reports for internal use. These are reviewed by the IT Service Managers. There is also regular reporting on general user satisfaction IT performance in general carried out by an external independent assessor, the Society for IT practitioners in the public sector, SOCITM. This is reported on the staff intranet, ERIC for IT users. Within the SOCITM survey there is some detail of satisfaction regarding impact of changes. Customers can view the progress of the change requests as in objective 2.	
Strength of Internal Controls:	Strong

Control Objective 4: Ensure that any emergency change is controlled and documented in true emergencies	
Audit Comments: The separate listing of emergency changes from 2014 showed a small and reducing number of these requests. There were two in 2015 and one in 2016, whereas previously in 2014 there were eighteen. This could suggest that preventative processes are reducing the numbers of these arising. Emergency changes can be implemented prior to the creation and submission of the formal change request with verbal approval and data input retrospectively. However the incident is required to be logged for assessment of change, authorisation, testing and agreed change, description of a back-out plan. Post implementation documentation is updated to reflect any changes. Operating guidelines for the CAB include procedures for emergency CAB meetings and the IT Change Co-ordinator is responsible for ensuring retrospective completion of all documentation for emergency change. The latest emergency change recorded in 2016 confirmed a unique change reference logged with a change requestor and assigned technical owner, risk assessment, resource estimate and executive CAB approver, which was satisfactory.	
Strength of Internal Controls:	Strong

Management Action and Follow-Up

Responsibility for the maintenance of adequate and effective internal controls rests with management.

Where the audit has identified areas where a response by management is required, these are listed in Appendix 1, along with an indication of the importance of each

'action point'. Appendix 2 describes these action points in more detail, and records the action plan that has been developed by management in response to each point.

It is management's responsibility to ensure that the action plan presented in this report is achievable and appropriate to the circumstances. Where a decision is taken not to act in response to this report, it is the responsibility of management to assess and accept the risks arising from non-implementation.

Achievement of the action plan is monitored through Internal Audit's 'follow up' arrangements.

Management should ensure that the relevant risk profiles are reviewed and updated where necessary to take account of the contents of Internal Audit reports. The completeness of risk profiles will be examined as part of Internal Audit's normal planned work.

Acknowledgements

Internal Audit acknowledges with thanks the co-operation of IT Service Managers, IT Team Lead and IT Co-ordinator during this audit.

Feedback

Internal Audit welcomes feedback from management, in connection with this audit or with the Internal Audit service in general.

Distribution

This report has been distributed to:

L Harris and D Adams IT Service Managers

Main contacts during the audit as above

If necessary, dependent upon the findings, other Services may be involved in the reporting process. This will be agreed with the Chief Internal Auditor prior to issue.

The final report will be issued, as a minimum, to:

B Malone, Chief Executive

J Valentine, Depute Chief Executive

A Taylor, Head of Corporate IT & Revenues

IT Service Managers as above

K McNamara, Head of Strategic Commissioning and Organisational Development

L Simpson, Head of Legal and Governance Services

G. Taylor, Head of Democratic Services

D Henderson, Information Compliance Manager

C Wright, IT Change Management Team Lead

External Audit

Authorisation

The auditor for this assignment was N Duncan. The supervising auditor was J Clark.

This report is authorised for issue:

_____

Jacqueline Clark
Chief Internal Auditor
Date: 29 March 2018

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1	Change Management Policy	Low
2	Change Procedures and the Service Desk	Medium
3	Monitoring performance of Change	Low

Appendix 2: Action Plan

Action Point 1 - Change Management Policy

The Change Management Policy has been reviewed since 2011 and remains the current policy. However there is no document management section giving details of contributors and version control. Risks from not having version control details include potential for misunderstanding of which is the current policy to apply.

Management Action Plan

The Change Management Policy will include a document management control section with dates, including when it was approved by the Council and when reviews have taken place

Importance:	Low
Responsible Officer:	D Adams, IT Service Manager
Lead Service:	Corporate and Democratic Services
Date for Completion (Month / Year):	May 2018
Required Evidence of Completion:	Updated document management section from the Change Management Policy

Auditor's Comments

Satisfactory

Action Point 2 - Change Procedures and Service Desk environment

There are documented procedures in the CM ICT Business Owner Guidance, CM IT Tech Owner Guidance, and Team Leader CAB Approach. These were written in 2015 to be used in conjunction with the process at the time. In 2017, the Change Management environment moved forward with the IT Service's Service Management Tool.

Positive benefits from this include detailed audit logs and automated alerts to CAB for authorisation of changes.

It is understood the CM Team are reviewing outcomes from the new environment to confirm CM process mapping and documentation are adequate.

Management Action Plan

As the introduction of the IT Service's Service Management Tool is new, processes are under continuous review; therefore procedures have not yet been updated. However, the Service are aware that the procedures will require to be documented.

Importance:	Medium
Responsible Officer:	D Adams, IT Service Manager
Lead Service:	Corporate and Democratic Services
Date for Completion (Month / Year):	September 2018
Required Evidence of Completion:	Copy of updated Change Management procedures

Auditor's Comments

Satisfactory

Action Point 3 - Monitoring Performance of Change in Service Desk

The move of Change Management onto the IT Service's Service Management Tool is being continuously monitored by the Team to confirm the new processes are meeting ICT Services objectives. There are almost 6 months of data available for review.

Management Action Plan

A summary review document of Change Management on the Service Desk will be prepared to confirm outcomes.

Importance:	Low
Responsible Officer:	D Adams, IT Service Manager
Lead Service:	Corporate and Democratic Services
Date for Completion (Month / Year):	September 2018
Required Evidence of Completion:	Copy of report to IT Management Team

Auditor's Comments

Satisfactory