INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	IT Incident & Problem Management
TO:	Head of Corporate & Community Services	**DATE:**	30 September 2012
C.C.	Chief Executive Head of Finance ICT Services Manager Technical Support Manager		

1. Introduction

1.1 In accordance with the Audit Plan for 2012/13, an examination of the above subject area has been undertaken and this report presents the findings and conclusions drawn from the audit for information and action where appropriate. This is the first time that this topic has been audited.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

2. Background

2.1 The council uses the SupportWorks system to record all incidents and problems that have been reported to ICT Services. Service requests are also recorded on the system, but they were not included within the scope for this audit.

2.2 Calls are generally received via the ICT Services Helpdesk, with incidents being reported either via telephone, email or in person.

3. Scope and Objectives of the Audit

3.1 The audit was undertaken to test the controls in place to ensure that incidents and problems that occur on the council's computer systems are dealt with and managed effectively.

3.2 In terms of scope, the audit covered the following areas:

- Service level agreement
- Case management
- Analysis and monitoring
- Problem management.

3.3 The audit programme identified the expected controls. The control objectives examined were:

- Management at the council have agreed the level of service that they expect from ICT Services
- If issues are picked up by other staff members, they can easily identify how the problem was initially recorded and how it has been dealt with up until the point of their involvement
- Customers receive a seamless service
- Issues can be dealt with in a timely manner as the correct staff are assigned to deal with them
- Jobs are dealt with in priority order in line with the expectations of management
- Service users are kept informed of IT issues that may affect them
- Repeat calls to resolve the same issue are not required
- The reoccurrence of issues is prevented as far as possible
- Root causes of multiple or significant incidents are resolved
- Issues can be resolved in a timely manner as IT staff do not have to 'reinvent the wheel' if solutions are already recorded on the system.

4. Findings

4.1 Service Level Agreement

4.1.1 A Service Level Agreement (SLA) is in place between ICT Services and the council as a whole and this was agreed with management in February 2010. The document sets out the different service resolution times for incidents, based on the priority assigned to an incident and the process for escalation if a customer feels that the call has not been dealt with appropriately.

4.1.2 The ICT Services Manager advised that the resolution timescales had not been specifically discussed with management, although they had been agreed as part of the overall SLA. He advised that they had been set based on what he thought would be reasonable for the business and not necessarily what was achievable by ICT Services at the time. He further advised that no adverse comments have been received on the timescales set.

4.2 Case Management

4.2.1 The Service Level Agreement includes rough definitions of what is classed as an 'Incident' and types of things that come under the 'Request for Service' heading. There is no definition of what a 'Problem' is, as the distinction between an incident and a problem (as made within ITIL documentation) is not made at the council.

4.2.2 The incidents are assigned a priority level within the system, based on impact and urgency and definitions for the scores within the matrix set-up are included within the SLA.

4.2.3 Specific definitions are not recorded for the different statuses that are used within the SupportWorks system, although they are generally self explanatory and the system will automatically assign some of them, based on actions performed.

4.2.4 Staff are of the understanding that if they can undertake the job (i.e. they have the expertise and the relevant system rights), they will but, if not, they will be aware of who to pass the job onto (e.g. ICT Technical Support Analyst, Application Support Analyst etc.).

4.2.5 There is nothing within the system that automatically reviews who has the relevant capabilities to undertake jobs received or to manage the allocation of jobs based on the number of current jobs per staff member. However, when the call is to be assigned to a staff member, the system brings up a list of all staff and this list shows how many jobs each staff member has, although this does include the jobs that are on-hold and those that are resolved (prior to being closed) so it can only be used as a rough guide.

4.2.6 The individual who has been assigned the job has the responsibility for seeing the job through to conclusion. This is highlighted each year during appraisals.

4.2.7 The Technical Support Manager (TSM) advised that emails are sent to customers to advise them that the job had been logged and this was thought to include details of the target resolution time. However, upon receipt of a

test email it transpired that this information was not provided, despite it appearing on the system when the test was conducted.

Risk
Customers are not aware of the priority (resolution target time) that has been assigned to their issue.

Recommendation
The format of the emails, that are sent to users to advise them that the call has been logged, should be reviewed to ensure that the target resolution time is included.

4.2.8 The TSM advised that the priority assigned to a job can be amended by entering an update and amending the SLA. These amendments are automatically recorded on the call diary for each job.

4.2.9 Sample testing was performed on a sample of incidents to check whether appropriate levels of detail were being recorded which were consistent with supporting documents and emails where appropriate, whether appropriate job profiles, statuses and SLA priorities were being used, whether jobs were being escalated as appropriate and that customers were being contacted to confirm that fixes applied had worked before the job was formally closed.

4.2.10 Testing revealed that, in a number of incidents, the level of details recorded against the job was not sufficient. The TSM had highlighted this a potential issue prior to testing taking place.

Risk
Staff picking up jobs are not aware of the work already performed.

Recommendation
Staff should be reminded of the need to record sufficient details of the call received, the work performed to try and resolve the issue and any communication with the customer.

4.2.11 Testing also highlighted that, whilst the profile recorded was always consistent with the original description of the job, the actual cause of the issue was sometimes different. However, the closing profile was not always updated to reflect this.

Risk
Results of trend analysis performed are inaccurate.

Recommendation
Profiles should be updated as appropriate to reflect the actual issue identified if this varies from the initial description received.

4.2.12 It was also identified that the SLA prioritisation was often left in the default state, rather than a formal completion of the matrix on the system being undertaken. Whilst the prioritisation may have been correct, it is not clear whether staff have actually reviewed this.

Risk
Jobs are not dealt with in line with the timescales agreed with management.

Recommendation
The SLA prioritisation should be used appropriately.

4.2.13 The TSM advised that duplicate calls are sometimes logged if the customer does not quote a log number or advise the Helpdesk staff member that they have already logged a call. She advised that when SupportWorks was being purchased, they had required that it be able to bring up a list of jobs for each customer when a new job was being logged to ensure that there wasn't already a job of that description open, but that was not provided.

4.2.14 Searches can be performed to check open jobs for each customer, but this can be quite laborious and the user would have to come out of the screen which they were using to log the job to perform the search, so this was not really practical.

4.2.15 Testing was performed to ascertain whether duplicate or repeat calls were being recorded on the system by reviewing all calls received within a certain timescale for a sample of users. This testing proved satisfactory, although one potential duplicate job was identified during the main testing detailed above.

4.2.16 On-screen reviews of the status of each job are performed, although there is no formal process that would allow for jobs to be reviewed at a certain stage to try and work on a temporary fix to enable the customer to carry on working whilst a full solution is worked on.

4.2.17 The TSM suggested that this is the type of incident where the use of the 'problem' classification may be useful. This would allow for the incident to be closed once a temporary fix is arrived at, allowing for the statistics produced to show an accurate picture. She also suggested that the level of detail recorded may be an issue as, if a member of staff provided a temporary fix but didn't document it as such, the job may be escalated and other staff may follow it up and spend time working on a different fix. However, if the temporary fix closed the incident, and a 'problem' was generated, this may solve such potential issues.

4.2.18 During the sample testing of calls, one such incident was highlighted where a temporary workaround was found. The incident was closed in this case, but there was still a need for a full solution to the problem.

Risk
Incidents remain open after fixes have been applied which may result in inaccurate performance monitoring.

Recommendation
Review the use of problem classification for relevant incidents where temporary fixes are provided.

4.3 Analysis & Monitoring

4.3.1 The TSM advised that she produces management information from the SupportWorks system, extracting details regarding the number of calls received (both service requests and incidents) and then summarising this by

the most frequent types of requests and which departments are making the most calls.

4.3.2 This information is then used for trend analysis by the TSM in order to identify if specific training needs can be highlighted or if greater 'problems' are apparent. Upon review of sample information, it is clear that the vast majority of calls are service requests and it is hard to pick up specific trends relating to incidents recorded.

4.3.3 Other information is also produced which shows performance information for individual staff members. Certain information is stripped from this raw data (such as specific work for the IT team and unblocking emails) and statistics reports are produced for the monthly management team meetings.

4.3.4 As highlighted above, the TSM also advised that the status of jobs is monitored on screen so, if jobs are nearing the stage where they will be escalated, she can prompt staff and enquire about the progress. Other staff will also note the status of jobs and will pick up if possible.

4.4 Problem Management

4.4.1 As previously highlighted, there is no formal classification of a 'problem'. On the whole, incidents will be left open until they are fully resolved, even if temporary work-arounds have been put in place, although some incidents may be classed as major incidents if it will affect a number of users. However, there is no threshold regarding the number of calls received that would necessitate this.

4.4.2 The Application Support Manager (ASM) advised that the two areas (i.e. incident and problem management) were fairly blurred, with no straight split along the ITIL lines. This is largely due to the size of the organisation and the fact that each business application has a named Application Support Analyst.

4.4.3 If suppliers are required to have input to solve the problem, the incident can be placed on hold. Managers can then keep an eye on the open incidents and chase suppliers as necessary.

4.4.4 Application Support staff may document work-arounds if they feel that more calls are expected. These documents will be held on the MOSS site for Business Applications under the Support Documentation section and will be periodically reviewed by the relevant staff members to ascertain if they are still relevant or if they can be deleted.

4.4.5 When calls are received that lead to an incident being created, the first port of call will be the relevant Application Support Analyst. However, if they are not around, other staff will check the MOSS documents to see if a work-around has been documented.

4.4.6 The ASM indicated that the use of the 'known error' function on SupportWorks had been started at one stage but it was felt that it wasn't being used at the other end (i.e. by Helpdesk staff), so its use had generally been discontinued.

Risk

Staff dealing with incidents undertake unnecessary work as they are not aware that similar incidents have previously been resolved.

Recommendation
The 'known error' function on SupportWorks should be populated with relevant information, with Helpdesk staff being made aware of the existence of the content.

5. Summary & Conclusion

5.1 Following our review, we are able to give a SUBSTANTIAL degree of assurance that the systems and controls in place for the management of incidents and problems that occur on the council's computer systems are working effectively.

5.2 Minor issues were identified relating to the detail included in emails to customers, the level of detail recorded on the system, the updating of profile information, the correct use of SLA prioritisation, the use of problem classification and the use of the known error function on the system.

6. Management Action

6.1 The recommendations arising above is reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of IT Incident & Problem Management – October 2012

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer	Management Response	Target Date
4.2.7	The format of the emails, that are sent to users to advise them that the call has been logged, should be reviewed to ensure that the target resolution time is included.	Customers are not aware of the priority (resolution target time) that has been assigned to their issue.	Low	Technical Support & Application Support Managers	Agreed. The format of the emails has been amended to include the classified SLA target date / time for resolution.	Completed
4.2.10	Staff should be reminded of the need to record sufficient details of the call received, the work performed to try and resolve the issue and any communication with the customer.	Staff picking up jobs are not aware of the work already performed.	Low	Technical Support Manager	Agreed. Staff have been sent an email to remind them of this requirement.	Completed
4.2.11	Profiles should be updated as appropriate to reflect the actual issue identified if this varies from the initial description received.	Results of trend analysis performed are inaccurate.	Low	Technical Support Manager	Agreed. Staff have been sent an email to remind them of this requirement.	Completed

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer	Management Response	Target Date
4.2.12	The SLA prioritisation should be used appropriately.	Jobs are not dealt with in line with the timescales agreed with management.	Low	Technical Support Manager	Agreed. Staff have been sent an email to remind them of this requirement.	Completed
4.2.18	Review the use of problem classification for relevant incidents where temporary fixes are provided.	Incidents remain open after fixes have been applied which may result in inaccurate performance monitoring.	Low	Technical Support, Application Support and Network & Communications Managers	Agreed. The use of the problem classification has been reviewed and will be used as appropriate for future cases.	Completed
4.4.6	The 'known error' function on SupportWorks should be populated with relevant information, with Helpdesk staff being made aware of the existence of the content.	Staff dealing with incidents undertake unnecessary work as they are not aware that similar incidents have previously been resolved.	Low	Technical Support, Application Support and Network & Communications Managers	Upon further inspection, it transpired that more use of this function was being made than was thought at the time of the review, although the content could not easily be viewed by different users due to the set-up of the SupportWorks system. However, it will be used where relevant for future cases.	Completed

* Risk Ratings are defined as follows:

Low - Minimal adverse impact on achievement of the Authority's objectives if not adequately addressed.
Medium - Moderate adverse impact on achievement of the Authority's objectives if not adequately addressed.
High - Requires urgent attention with major adverse impact on achievement of Authority's objectives if not adequately addressed.