9

Shropshire and Wrekin Fire and Rescue Authority
Audit and Performance Management Committee
1 March 2012

ICT Systems Failure and Internal Audit

Report of the Chief Fire Officer

For further information about this report please contact Paul Raymond,
Chief Fire Officer, on 01743 260205.

1 Purpose of Report

This report summarises the issues identified following the internal audit of the failure of information and communications technology (ICT) systems and identifies actions to rectify the situation.

2 Recommendations

The Committee is asked to note the contents of the report.

3 Background

A failure of the Shropshire Fire and Rescue Service storage area network occurred on 7 June 2011 at 10.16 pm. NViron, who originally installed the virtual server environment, initiated the recovery process on 8 June 2011; on 10 June 2011 it was determined that the failure was irrecoverable. Work did not begin in earnest on rebuilding the network until the Network Manager returned from leave on 22 June 2011. During this pause the Service set up a Disaster Recovery Team (DART) and a Business Continuity Group (BCG), chaired by the Deputy Chief Fire Officer and Chief Fire Officer respectively.

During this time there was no impact directly on the mobilising system and critical functions of service delivery were maintained.

At the request of the Chief Fire Officer Shropshire Council Audit Services undertook a review of the circumstances surrounding the failure of the network.

The loss of the virtual server environment caused loss of connectivity to all virtual servers, which host network file storage and some programs, including bespoke in-house developed web-based applications and data. The full recovery process was delayed awaiting the return of the Network Manager from leave, although staff, working through the BCG and DART, pulled together and created some innovative solutions to keep the Service operating. Since moving to the new HQ building the ICT team, working with external agencies, has rebuilt the local area network and re-launched the disaster recovery / data replication servers and systems at Telford.

4 Scope of the Audit

The Chief Fire Officer discussed with in-house ICT staff, the Assistant Chief Fire Officer – Human Resources and Internal Audit what questions were required to be answered by the audit.

These were agreed as:

1. What was the nature of the failures?

2. What, if any, processes failed or were absent that contributed to the failure of the system?

3. What, if any, acts or omissions led to the failure of the back-up systems?

4. Were all appropriate resilience measures in place to minimise the risk of such a failure? If not what was missing?

5. Why did the Service’s backup systems, including the business continuity back-up arrangements in Telford, fail to operate correctly?

6. Why did two hard drives fail simultaneously?

7. Why were we unable to immediately or quickly return to back-up files on the failure of the main server?

8. Was there anything that reasonably could or should have been done to minimise the impact of the failures identified in the early stages?

9. Was any aspect of the actual failure reasonably foreseeable and, if so, what?

10. Are there any skills gaps that may have led to or contributed to any systems failures identified?

11. Are there any areas of ICT business recovery that are currently not being addressed?

12. Are there any recommendations as to the structure / contents of the new ICT strategy that will prevent a future reoccurrence of this failure?

5 The Internal Audit Report

The confidential report was presented to the Chief Fire Officer in final draft form on 3 November 2011. It contained fifteen recommendations, eleven of which were classified as significant. The Chief Fire Officer has kept the Chair of the Authority informed of progress in dealing with this issue.

Now that the immediate and crucial functions have been replaced and repaired, the Audit and Performance Management Committee will wish to ensure that the recommendations made by Internal Audit are dealt with.

A summary of the recommendations is set out in the appendix to this report along with the actions taken to date by officers.

6 Financial Implications

The Fire Authority has identified an ICT reserve, which will be sufficient to deal with issues arising from the failure and the move to the new headquarters.

7 Legal Comment

There are no direct legal implications arising from this report.

8 Equality Impact Assessment

Officers have considered the Service's Brigade Order on Equality Impact Assessments (Personnel 5 Part 2) and have determined that there are no discriminatory practices or differential impacts upon specific groups arising from this report. An Initial Equality Impact Assessment has not, therefore, been completed.

9 Appendix

ICT Action Plan

10 Background Papers

There are no background papers associated with this report.

Appendix to Report 9 on
ICT Systems Failure and Internal Audit
Shropshire and Wrekin Fire and Rescue Authority
Audit and Performance Management Committee
1 March 2012

Information and Communications Technology Action Plan

Fundamental	Significant	Requires Attention	Best Practice
Immediate action required to address major control weakness that, if not addressed, could lead to material loss.	A recommendation to address a significant control weakness where the system may be working but errors may go undetected.	A recommendation aimed at improving the existing control environment.	Suggested action which aims to improve best value, quality or efficiency.

Rec No.	Recommendation	Rec Rating	Accepted Yes/No/ Partially	Management Response	Lead Officer	Date to be Actioned	Progress Review Date:
1	The replication process needs to be re-implemented as a matter of urgency. A gap analysis should be undertaken with a clear plan to replicate SFRS data to an appropriate off-site location.	Significant	Y	Test scripts from Telford DRS showing that all data on SFRS servers in Shrewsbury is replicated. Letter from Intrinsic (the DRS Builders) that data replication is working.	ACFO Worrall	18 November 30 November	Replication of AD, Exchange and DFS data has been demonstrated to be free from issues during normal working hours. Improved network communications between Telford and Shrewsbury have made the link faster and more reliable
2	Adequate controls should be operating to ensure that appropriate resilience measures are in place, tested regularly to ensure they are working effectively and management informed accordingly.	Significant	Y	A monthly data audit, reported to ACFO and to CFO during monthly 1 to 1s, that DR is operating.	ICT Manager	First Report January 2012	System Center Manager to be deployed date tbc for reporting and monitoring. Adhoc test have proved successful. Weekly checks and monthly failover to take effect from 1 April 2012. Duties have been included in refreshed Job Descriptions.

Rec No.	Recommendation	Rec Rating	Accepted Yes/No/ Partially	Management Response	Lead Officer	Date to be Actioned	Progress Review Date:
3	Adequate escalation procedures should be in place for early system failure identification and initiation of remedial action.	Significant	Y	Correct managerial controls in place for each critical system to include: Monthly ‘ system health’ reports to ACFO 1 to 1s with ICT Manager ‘ICT health’ verbal report included Service Management Team agenda.	ACFO Worrall	End January 2012 Immediate	SLA with Intrinsic and Shropshire Council 1 to 1s carried out.
4	Adequate processes should be put in place to identify all software and hardware maintenance contracts, their costs and termination dates. Monitoring or renewal should be undertaken to ensure appropriate continuity arrangements are maintained from both hardware and software vendors and third party management arrangements.	Significant	Y	Records of all system components, upgrades; licence agreement end dates and patches with dates, signed off by ICT Manager.	ACFO Worrall	Immediate and developing. Third party management agreements by end December.	This is recorded in a spreadsheet

Rec No.	Recommendation	Rec Rating	Accepted Yes/No/ Partially	Management Response	Lead Officer	Date to be Actioned	Progress Review Date:
5	All backup and recovery processes should be documented, shared and made available across ICT with a hard copy readily available in the event of a system failure.	Significant	Y	A backup and recovery process file containing all necessary information to be presented to the Corporate Planning and Risk Manager with the original kept in ICT department. System for updating the file produced. This must have system of audit.	ICT Manager	End January 2012 End January 2012	Workshop to the ICT Team to disseminate this information has taken place. Awaiting full documentation from Intrinsic.
6	Each server and or network component configuration should be documented, shared and made available across ICT. Where applicable local hard copies should be retained.	Significant	Y	To be included within the above file lodged with the Corporate Planning and Risk Manager with original in ICT.	ICT Manager	End January 2012.	Documentation stored on shared drive. Awaiting further documentation from Intrinsic.
7	Formal Change control procedures should be introduced and adhered to	Significant	Y	Copy of control procedures signed off by ACFO and included with the evidence at Feb meeting with CFO and IA.	ICT Manager	End November 2011.	Change control has been implemented but requires some guidelines to be distributed to avoid it becoming overly bureaucratic. Duties have been included in refreshed Job Descriptions.

Rec No.	Recommendation	Rec Rating	Accepted Yes/No/ Partially	Management Response	Lead Officer	Date to be Actioned	Progress Review Date:
8	A clear and formalised patch management procedure should be introduced to ensure that all critical hardware and software is patched up to date. This should be subject to the ICT change management processes.	Significant	Y	This is to be included in the file at recommendation 5 above.	ICT Manager	End April 2012	Plans to fully implement System Center Manager to support the procedure
9	Further investigation work is required to establish why the actions for improvement identified in the ICT Manager's report of May 2010 were not delivered, monitored or formally reported on.	Significant	Y	Implement managerial control to remedy any issues raised. Further interviews to be undertaken.	CFO	January 2012	Interviews carried out by CFO and appropriate action taken.

Rec No.	Recommendation	Rec Rating	Accepted Yes/No/ Partially	Management Response	Lead Officer	Date to be Actioned	Progress Review Date:
10	Clarification of the roles of both the ICT Manager and Network manager need to be clearly laid out and responsibilities assigned in respect of preventative and reactive tasks relating to network failure and the maintenance of hardware and software support agreements. This should include the role of third party organisations who manage aspects of the network to ensure clarity of roles.	Significant	Y	New structure of ICT Team with draft job and role descriptions produced and presented to CFO. Responsibilities of third party agents to be presented in plain English to CFO with management gap analysis.	ACFO Worrall	January 2012 January 2012	Awaiting Service Management support arrangements from Shropshire Council regarding the WAN. Discussions actively taking place with Intrinsic about Service Support arrangements. The above has contributed toward the team review and the proposed roles and responsibilities. Refreshed Job Descriptions to reflect clarification of roles.

Rec No.	Recommendation	Rec Rating	Accepted Yes/No/ Partially	Management Response	Lead Officer	Date to be Actioned	Progress Review Date:
11	The ICT team members should be trained up and capable of covering each other's technical duties. An exercise to deliver skill transfer within the ICT team is critical to service continuity, skills gap analysis and appropriate training plans should be drawn up and delivered within a realistic timescale and monitored through the IPDR and CPD process. This recommendation relies on the structure of the ICT team being agreed and staff employed appropriately. This in turn is dependent on organisational acceptance of the new ICT strategy.	Significant	Y	New ICT Strategy (to include team structure) accepted by Service Management Team. Recruitment / retention recommendations presented to CFO ICT Team skills gap analysis carried out to gauge ability to deliver strategy. Each member of ICT Team to receive IDR with new JD.	ACFO Worrall ACFO Worrall ICT Manager ICT Manager	December 2011 December 2011 January 2012 January 2012	Recruitment for new team members is now in the process following the team review. Staff to be in post by end of March and IPDRs scheduled for April 2012.

Rec No.	Recommendation	Rec Rating	Accepted Yes/No/ Partially	Management Response	Lead Officer	Date to be Actioned	Progress Review Date:
12	Management and Monitoring of critical event logs should be undertaken as a routine daily exercise. Responsibility for these tasks should be formally assigned and an appropriate mechanism put in place to report completion of log reviews and action taken where problems are identified to mitigate any risk to the running of the corporate network.	Requires attention	Y	Critical event logs presented to ACFO Worrall Above logs included with ICT audit plan with Internal Audit.	ICT Manager ICT Manager	March 2012 March 2012	Reactively, Event logs should be the first place to look if there are any issues but reviewing them proactively every couple of days can help prevent problems. Event Logs to check • Domain Controllers (one in each site) - System, Application, DFS replication, File Replication Service, DNS Server, Directory Service • Exchange Server in each site - System, Application Other servers - System, Application
13	Consideration be given to scoping further detailed investigations into any specific concerns highlighted in the report or subsequent findings from implementation of the recommendations	Requires attention	Y	End of improvement report to contain any further recommendations for improvement.	CFO	June 2012	Considered and not required at present.

Rec No.	Recommendation	Rec Rating	Accepted Yes/No/ Partially	Management Response	Lead Officer	Date to be Actioned	Progress Review Date:
14	The management of ICT function needs to be clearly documented and staff made aware of and understands their responsibilities.	Requires attention	Y	Updated department structure and job descriptions signed by employees and placed on EPR. One to one system for all staff in LCT in place. (CFO to see notes for each initial meeting)	ACFO (CPO) and ICT Manager	ICT Manager CFO	See 10 ICT Strategy to be formally published in March
15	Management meetings between the ICT Manager and the Head of Operations and Risk should document key issues and actions to be taken which should be monitored on an on-going basis. Serious issues, such as the failure of the replication process, should be appropriately prioritised, and senior management informed as required.	Requires attention	Y	New section in corporate risk register created 'ICT Risks Log'. This must include all ICT risks including mobilising system. The responsibility for ICT has now moved to the direct management of ACFO Worrall, thus separating management and audit of this function. The ACFO Will be required to record key issues and action in normal 1 to 1s	Head of Corporate Risk. ACFO Worrall	Immediate Immediate	121 meeting with ACO every Monday