BEDFORDSHIRE FIRE AND RESCUE AUTHORITY

IT Shared Service

FINAL

Internal Audit Report: 6.15/16

5 May 2016

CONTENTS

Debrief held	12 April 2016	**Internal Audit team**	Dan Harris, Partner Suzanne Lane, Senior Client Manager Steven Snaith, Technology Risk Assurance (TRA) Partner Kevin Hickman, TRA Principal Consultant
Draft report issued	18 April 2016		
Responses received	4 May 2016		
Final report issued	5 May 2016	**Client sponsor**	Gavin Chambers, Head of Finance and Asset Management
		Distribution	Gavin Chambers, Head of Finance and Asset Management Alison Ashwood, Head of Strategic Support Mark Dix, Service Delivery Manager, ICT Shared Service Suzanne Hodgkiss, ICT Support Manager, ICT Shared Service

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at http://www.icaew.com/en/members/regulations-standards-and-guidance.

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Therefore, the most that the internal audit service can provide is reasonable assurance that there are no major weaknesses in the risk management, governance and control processes reviewed within this assignment. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is supplied on the understanding that it is solely for the use of the persons to whom it is addressed and for the purposes set out herein. Our work has been undertaken solely to prepare this report and state those matters that we have agreed to state to them. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any party other than the Board which obtains access to this report or a copy and chooses to rely on this report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to our Client on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

1 EXECUTIVE SUMMARY

1.1 Background

An audit of Bedfordshire Fire and Rescue Service's ("BRFS's") IT Shared Service was conducted as part of the annual audit plan for 2015-16.

In April 2010, the ICT Service Manager for Bedfordshire Fire and Rescue Service presented to the senior management teams of the Service and Cambridgeshire Fire and Rescue Service, an outline business case which considered a number of options for delivering IT services, ranging from maintaining the existing arrangements, through a number of collaboration options, to full outsourcing of the ICT functions.

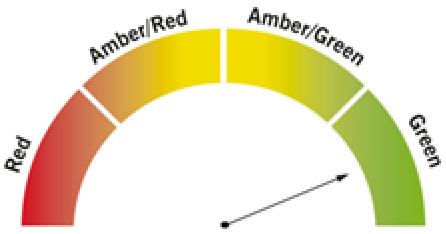
Consideration of these options identified a clear case for moving forward with a shared IT service arrangement. As a result, a project was formally established encompassing a number of key objectives, including the modernisation and integration of the IT network infrastructures, the formation of a shared IT Team structure, supplying IT services to BFRS and Cambridgeshire Fire and Rescue Service (CRFS) and the creation of the IT Shared Service Agreement which sets out the IT Shared Service Governance arrangements.

On 22 October 2013 Bedfordshire Fire and Rescue Authority authorised the completion of an ICT Shared Service Agreement for a term of five years. The IT Shared Service then entered a 'transition' phase which completed on 31 March 2014, with the new arrangements becoming fully established as from April 2014.

1.2 Conclusion

Overall, we found that the IT Shared Service arrangements for Bedfordshire Fire and Rescue Service were well - controlled and we have identified only two areas for control improvement in this review. These relate to obtaining senior management and Authority approval of a specific IT strategy for BFRS and the documentation of 'end to end' Incident Management procedures.

Internal Audit Opinion:
Taking account of the issues identified, the Authority can take substantial assurance that the controls in place to manage the IT Shared Service are suitably designed, consistently applied and operating effectively.



1.3 Key findings

The following controls were found to have been designed adequately:

- The IT Shared Service team structure and allocation of duties have been documented and made available to managers and staff within the Shared Service teams, reducing the risk of lack of awareness by team leadership and team members of their roles and responsibilities, which could have a negative impact on the delivery of BFRS's IT service and business requirements.

- Formal governance arrangements are in place concerning the delivery of the IT Shared Service, including the establishment of an IT Shared Service Governance Board, reducing the risk of lack of sufficient senior management oversight, monitoring and review of IT operations conducted by the Shared Service teams. This in turn reduces the risk of failure to identify and remedy any shortfalls in service delivery and performance which could have a negative impact on BFRS's business operations.

- A number of processes have been designed and implemented regarding the measurement of the performance of IT Shared Service, including the production of monthly Key Performance Indicator (KPI) reports and the regular and frequent service delivery review meetings between BFRS and IT Shared service management. This reduces the risk of a lack of awareness by BFRS management of any significant shortfalls in the performance of the IT shared service which, if not remedied in a timely manner could negatively affect the business operations supported by the Shared Service.

- Procedures are in place for the management of IT assets, including the use of an asset register and indicators within the register identifying asset owners, reducing the risks of:

  - The inability to accurately account for all IT assets for financial valuation purposes.

  - Difficulties in tracing the movement and location of IT assets.

  - Failure to identify lost or stolen assets in a timely manner which could negatively impact business operations prior to replacements being obtained.

- An activity-based time recording system is in place for IT services undertaken for BFRS and CFRS which is designed to facilitate the management, monitoring and control of service costs, reducing the risk that:

  - The relative costs of the provision of IT services to each partner in the Shared Service will be allocated and calculated incompletely, incorrectly or inappropriately.

  - Excessive deviations from budgeted costs for providing IT services for each Fire Service are not identified in a timely manner and adjustments not made to expenditure where appropriate.

  - Incorrect residual payments (for sums owed by each of the Partners for Shared services provided are made or received at the end of the year.

- A number of control procedures are in place within BFRS for handling Freedom of Information (FoI) requests, including the allocation of responsibility and procedures in place for logging, co-ordinating, and monitoring FoI requests, and guidance provided on the BFRS website for members of the public regarding the request process These arrangements reduce the risks of:

  - The lack of appropriate guidance for members of the public on making FoI requests for information held by BFRS.

  - The inability to track and monitor FoI requests and to confirm compliance with statutory FoI target dates.

No significant instances of inadequate control design were found during our review of the IT Shared Service, though we have identified two minor areas for control improvement for which we have agreed Low priority actions for management. These have been included in the Actions for Management and Detailed Findings sections below. One minor observation on control design has also been included, for management’s information only, in the Additional Feedback section below.

Application of and Compliance with the Control Framework

Our testing identified that the recurring controls identified and evaluated during this audit were generally operating and being complied with; in particular:

- We reviewed a sample of the minutes of IT Shared Service Governance Board meetings, covering the period April 2015 to January 2016. We verified that the meetings were held regularly (every 1-2 months) as planned and that the Shared Service action plans were updated as a result of the meetings.

- We obtained copies of the IT Shared Service KPI management reports produced during 2015-16 and verified that monthly, rolling 6 monthly and combined rolling 6 monthly reports were produced as planned.

- We obtained a copy of the IT Asset Management Plan and appropriate minutes of the Corporate Services Policy and Challenge Group (the committee which includes Fire Authority Members responsible for ICT services) and verified that the IT Asset Management Plan for 2015-16 was produced in a timely manner (in June 2015) and had been approved by the above Group, in line with policy requirements.

- We obtained a copy of the FoI request log covering the period October 2015 to January 2016 and verified that information on all requests has been completed as per the FoI risk request template and that responses were sent out in respect of all requests which had reached their statutory expiry date within (or in one case, within a day of) the 20 day target time.

There were no particular issues identified during our testing which we wish to draw to management's attention.

1.4 Additional information to support our conclusion

Risk	Control design*	Compliance with controls*	Agreed actions		
			Low	Medium	High
The IT Shared Services control arrangements in place are inadequately designed and poorly managed, leading to IT services which fail to meet organisational requirements in terms of availability, performance, data security and confidentiality and cost sharing.	2 (10)	0 (4)	2	0	0
Total			**2**	**0**	**0**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

1.5 Additional feedback

Observation:

In discussion with the Shared Service Infrastructure Manager that at the time of our audit, a number of legacy shared email accounts were in use across the BFRS computer estate, particularly in fire stations.

In subsequent discussions with the Head of Strategic Support and the joint Service Delivery Manager for the Shared Service we were assured that as part of the Virtual Desktop Infrastructure rollout, which was due to start on 4th April 2016 and finish in July 2016, the usage of separate email logins would cease, as the use of particular email accounts will be linked to users' single sign-on credentials, each of which is unique to the user.

The use of generic email accounts weakens the audit trail and increases the risk of the inability to trace activity back to particular users in the event of investigations into error or system misuse.

However, as noted above, we were informed by management that the above risk will be mitigated when the VDI infrastructure has been implemented across the whole of BFRS. We therefore make no formal recommendation on this matter but have just included it in our report as an observation for management's attention.

2 ACTION PLAN

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may, with a high degree of certainty, lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The table below sets out the actions agreed by management to address the findings:

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
Risk: The IT Shared Services control arrangements in place are inadequately designed and poorly managed, leading to IT services which fail to meet organisational requirements in terms of availability, performance, data security and confidentiality and cost sharing.					
1.7	A draft IT Strategy has been created for BFRS which was found to be designed adequately and in line with best practice. However, at the time of our review, the new Strategy had not been submitted to the appropriate level of senior management for approval and issued to staff across the Service.	Low	The full new IT strategy for BFRS, incorporating the Shared Service arrangements, will be submitted to the appropriate senior management group at BFRS for comments, approved and made available to management and staff across the Service.	30/06/2016	Head of Strategic Support
1.8	Although there is a standard form for recording the result of IT incident investigations, the end to end IT incident management and reporting procedure has not been documented.	Low	Management will design, document and make available to staff an IT incident management and reporting procedure.	30/06/2016	Service Delivery Manager, IT Shared Service

3 DETAILED FINDINGS

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
Risk: The IT Shared Services control arrangements in place are inadequately designed and poorly managed, leading to IT services which fail to meet organisational requirements in terms of availability, performance, data security and confidentiality and cost sharing.						
1.7	**IT strategy development and review processes** An Action Plan was produced for the development of the IT Shared Service in response to 23 recommendations made in a SOCITM (Society of Information Technology Management) review conducted for BFRS in April 2015. For BFRS, a record of progress against the recommended development plans is monitored, maintained and regularly updated by the Head of Strategic Support and includes the planned target date, ownership, progress and overall status of each agreed action. Recommendation 5 of the above SOCITM review stated that a separate Strategic Context document be produced by each of the parties to the Shared Service (BFRS and CFRS). In response to this, a draft Service Strategy for ICT had been produced by the Head of Strategic Support. This takes account of the action plans incorporated within the Service's Action Management Plan and identifies further opportunities for development.	No	N/A	The draft IT Strategy and associated IT Asset Management Plans and Action Plan were found to be designed adequately and in line with best practice, as well as comprehensively addressing the key IT issues faced by the organisation. The current/proposed processes for the continual review of these documents were also assessed as being robust. However, the lack of formal approval by the appropriate senior management group of the final version of the full IT Strategy for the next four years increases the risk of lack of corporate support and oversight of the strategy. This in turn potentially negatively impacts the achievement of the strategy's key objectives, the development of the IT service as a whole and the level of support provided in relation to the achievement of the organisation's planned overall business objectives.	Low	Management will finalise the new IT strategy for BFRS and will ensure that it is submitted to the appropriate senior management group at BFRS, approved and made available to management and staff across the Service.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
	The Strategy states that the opportunities highlighted will be developed into a roadmap and will be incorporated into the ICT Asset Management Plan and ICT Shared Service action plan as appropriate. It also adds that the newly formed ICT Strategy Group will ensure that the Strategy remains organisation-led and implementation provides value for money. The original target date for the production of the new IT Strategy was February 2016. Although the document was drafted during that month, at the time of our review (mid-March 2016), it had not been submitted to the appropriate level of senior management for comments/approval and issued to BFRS staff.					
1.8	**Shared IT policies and procedures (including those addressing data security matters).** We noted that majority of BFRS's IT policies and procedures, including those addressing data security matters, are the responsibility of BFRS corporate management, rather than the IT Shared Service teams and were therefore not reviewed in detail. However, we noted that the IT Shared Service has responsibility for investigating IT- related incidents and has carried out a number of such investigations since its inception in April 2014.	No	N/A	In the absence of a documented 'end to end' IT incident management and reporting procedure communicated across BFRS, there is an increased risk that staff will be unaware of best practice and the organisation's approach to incident management and that: ▪ IT incidents will not be investigated fully, root causes determined and remediation action taken regarding security weaknesses. ▪ IT incidents will not be reported to the appropriate internal governance Groups (such as the Corporate Policy and Challenge Group and the Shared Service Governance Group) for senior management oversight and scrutiny.	Low	IT Shared Services management will design, document and make available to BFRS staff an end to end IT incident management and reporting procedure.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
	These included, for example, confirming whether a contractor had accessed BFRS premises using an electronic key fob which had not been returned when he ceased working for the organisation; searches for email correspondence between BFRS staff and certain contractors; and reports on door access data for comparison with an employee's annual leave and flexileave requests and timesheet submissions. Notwithstanding this, although there is a standard form for recording the result of IT incident investigations, the end to end incident management and reporting procedure has not been documented.			▪ Incidents will similarly not be reported to the appropriate external bodies, for example the Information Commissioner's Office, in the case of breaches of the Data Security Act. This in turn could have negative legal and financial consequences for BFRS.		

APPENDIX A: SCOPE

Scope of the review

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. The scope was planned to provide assurance on the controls and mitigations in place relating to the following risks:

Objective of the risk under review	Risks relevant to the scope of the review	Risk source
To ensure that the control framework for the organisation's IT Shared Services arrangements is adequately designed and complied with.	The IT Shared Services control arrangements in place are inadequately designed and poorly managed, leading to IT services which fail to meet organisational requirements in terms of availability, performance, data security and confidentiality and cost sharing.	Discussion with management.

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

The following areas were considered as part of the review:

- Roles and responsibilities within the shared service;
- Governance of the shared service arrangement;
- Shared IT policies and procedures;
- Performance management and reporting;
- The management of ICT assets (jointly owned and separately identifiable);
- Activity based time recording that leads to the allocation of ICT Shared Services resource expenses;
- IT strategy development and review processes;
- Alignment of IT strategic objectives and plans with corporate strategy ;
- Monitoring of achievement of strategic objectives;
- Data security governance;
- Data security policies and procedures;
- Technical controls regarding data security, including network security, access controls, internet and email controls, remote access and removable media controls; and
- Procedures for handling Freedom of Information requests.

Limitations to the scope of the audit assignment:

- The scope of our work was limited only to those areas examined and reported on, and is not to be considered as a totally comprehensive review.

- The review was limited to identifying the existence of controls in the areas for review, and obtaining supporting documentation.

- All audit testing was carried out on a sample basis.

- We noted at the time of the audit, the BFRS Information/data governance structure was undergoing development. We therefore agreed with management that it was not appropriate for us to review the organisation's information data security governance arrangements at that time.

- At the request of the BFRS Head of Strategic Support, the organisation’s technical controls regarding data security were not assessed and tested as part of this audit, as they have been or will be covered within the scope of a number of other IT reviews.

- In addition, our work does not provide an absolute assurance that material error; loss or fraud does not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Alison Ashwood, Head of Strategic Support, BRFS
- Mark Dix, Service Delivery Manager, ICT Shared Service
- Suzanne Hodgkiss, ICT Support Manager, ICT Shared Service
- Paul Brown, Infrastructure Manager, BFRS
- Karen Daniels, Service Assurance Manager, BFRS
- Frank Renouf, Business Information Manager, BFRS

FOR FURTHER INFORMATION CONTACT

Suzanne Lane, Senior Manager

suzanne.lane@rsmuk.com

07720 508148

rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 11 Old Jewry, London EC2R 8DU. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Consulting LLP, RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM Employer Services Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.