DORSET & WILTSHIRE FIRE AND RESCUE AUTHORITY

Item 17/35

MEETING	Finance, Governance and Audit Committee
DATE OF MEETING	29 September 2017
SUBJECT OF THE REPORT	Internal Audit Quarterly Report (July-September)
STATUS OF REPORT	For open publication
PURPOSE OF REPORT	For approval
EXECUTIVE SUMMARY	During this quarter, two internal audits have been undertaken covering the areas of Information Systems Migration and IT Health Check. Both audits received substantial level assurances with no fundamental risks arising from these audits. Management responses have been proposed to address the issues raised in the report.
RISK ASSESSMENT	The issues raised by these audits do not represent a significant risk to the Authority. Both audits received a substantial level of assurance. Management responses have been agreed and are detailed in the audits.
COMMUNITY IMPACT ASSESSMENT	None for the purposes of this report
BUDGET IMPLICATIONS	None for the purposes of this report
RECOMMENDATIONS	Members are asked to: 1. Consider and approve the management responses
BACKGROUND PAPERS	None for the purposes of this report
APPENDICES	Gateway Assure Block 2 Audit Report (attached)
REPORT ORIGINATOR AND CONTACT	Robin Pritchard (Gateway Assure), Engagement Director Email: robin.pitchard@gatewayassure.com Tel: 07792 296830

Dorset & Wiltshire Fire and Rescue Services

Internal Audit Report

Block 2 2017/18 (Draft)

CONTENTS

CONTACT DETAILS – MANAGEMENT TEAM

Team Member	Role	Mobile	Email
Robin Pritchard	Engagement Director	07792 296830	robin.pritchard@gatewayassure.com

INTRODUCTION

OPERATIONAL AUDIT PLAN

1.1 This report summarises the outcome of work completed to date against the operational audit plan approved by the Authority, Finance, Governance and Audit Committee and the Chief Fire Officer and incorporates cumulative data in support of internal audit performance and how our work during the year feeds in to our annual opinion.

1.2 The sequence and timing of individual reviews has been discussed and agreed with management to ensure the completion of all audits within the agreed Internal Audit Strategy 2017/18; the current planned schedule is shown in Appendix C.

1.3 In brief the areas subject to audit on this occasion and the result of those audits are as follows:

		Recommendations				
Audit Area	Opinion	F	S	MA	Total	Agreed
Information Systems Migration	Substantial	0	1	2	3	
IT Health Check	Substantial	0	1	1	2	

KEY

Fundamental (F)	-	The organisation is subject to levels of fundamental risk where immediate action should be taken to implement an agreed action plan.
Significant (S)	-	Attention to be given to resolving the position as the organisation may be subject to significant risks.
Merits Attention (MA)	-	Desirable improvements to be made to improve the control, risk management or governance framework or strengthen its effectiveness.

1.4 We would like to take this opportunity to thank all members of staff for their co-operation and assistance during the course of our visit.

1.5 The results of each audit are reported through the Executive Summary and agreed Action Plan.

STANDARDS

1.6 We have performed our work in accordance with the principles of the Institute of Internal Auditors (IIA) International Professional Practice Framework (IPPF) 2013 and the Public Sector Internal Audit Standards (PSIAS) 2013 in so far as they are applicable to you our client. Our working papers are available for inspection.

QUERIES

1.7 Should any recipient of this report have any queries over its interpretation or content they should contact the client engagement director either directly or through the client contact as appropriate and we shall be happy to discuss the assignments and provide any detail or explanations necessary.

SCOPE & BACKGROUND

1.8 We have reviewed each area in accordance with the scope and objectives agreed with management prior to our visit. Appendix A provides detail of the scope of our work; our conclusions regarding the level of assurance that can be provided and where appropriate the agreed Action Plan to be implemented by management to remedy potential control weaknesses.

1.9 Our approach was to document and evaluate the adequacy of controls operating within each system. For each system the key controls operated by management were assessed against the controls we

would expect to find in place if best practice in relation to the effective management of risk, the delivery of good governance and the attainment of management objectives is to be achieved. Where applicable, selected and targeted testing has been used to support the findings and conclusions reached.

1.10 We report by exception and only highlight those matters that we believe merit acknowledgement in terms of good practice or undermine a system's control environment and which require attention by management.

AUDIT OBJECTIVE & OPINION

1.11 The objective of our audit was to evaluate the auditable areas with a view to delivering reasonable assurance as to the adequacy of the design of the internal control system and its application in practice. The control system is put in place to ensure that risks to the achievement of the organisation's objectives are managed effectively.

1.12 Our opinion is based upon the control framework (as currently laid down and operated) and its ability to adequately manage and control those risks material to the achievement of the organisation's objectives for this area. We provide our opinion taking account of the issues identified in the Executive Summary and Action Plan.

Overall Opinion

1.13 Each Executive Summary provides an overall assessment of our findings for each system reviewed and provides an opinion on the extent to which management may rely on the adequacy and application of the internal control system to manage and mitigate against risks material to the achievement of the organisation's objectives for each area.

Conclusion on the Adequacy of Control Framework

1.14 Based on the evidence obtained, we conclude for each area upon the design of the system of control, and whether if complied with, it is sufficiently robust to provide assurance that the activities and procedures in place will achieve the objectives for the system.

Conclusion on the Application of Controls

1.15 Based on the evidence obtained from our testing, we conclude for each area upon the application of established controls.

VALUE FOR MONEY

1.16 Where value for money issues are identified as a result of our work the corresponding recommendation will be annotated with **VFM** in the bottom right hand corner. This is used to identify recommendations which have potential value for money implications for the organisation or which indicated instances of over control.

PREVIOUS AUDIT RECOMMENDATIONS (FOLLOW UP)

1.17 Where a previously accepted audit recommendation remains outstanding at the time of our review and the original implementation date has passed the corresponding recommendation within Appendix A will be annotated with **PAR** in the bottom right hand corner.

EXECUTIVE SUMMARY

FINDINGS & CONCLUSIONS

2.1 The results of our visit to Dorset & Wiltshire Fire and Rescue Services ('the Service'), are summarised in this section of the report and are considered in relation to each area reviewed.

2.2 The extent of comment in relation to each audit area is restricted deliberately so as to highlight the key issues that we believe need to be drawn to the attention of the Finance, Governance and Audit Committee and senior management. They are supported by a more detailed analysis of each review that is contained in this report.

Information Systems Migration

2.3 The Information Systems Migration Programme was approved by the Strategic Leadership Team (SLT) in July 2016. The document sets out an overall governance and process for all migrations of information systems to support the new Service. This also contained supporting documentation regarding the priority of the projects, and was organised by scheduling the projects which offered the greatest benefits to the Service in the first year of its operation (2016/17).

2.4 Once a project is confirmed and agreed by the Project Manager and Project Sponsor, then a unique project is set up in the performance, risk and project management systems known as Sycle, which provides an automated recording and reporting process for project management, control and reporting. This system uses the 12 stage process which was agreed when the original programme was approved. The 12 stages then have individual activities within them, these have scheduled start and completion dates. The activities are assigned to individuals within the project team who are responsible for ensuring that they are completed in accordance with the schedule and that Sycle is frequently updated regarding the progress of migration.

2.5 Where the Service is migrating to an existing information management system in current operation, no detailed business case is required and needs to be approved by SLT. For other projects which include the potential to use another system that is not currently used, a business case is be prepared and considered by the SLT. According to the original approved programme in July 2016, project initiation documents should also be used, however the Head of Strategic Planning & Knowledge Management stated that the need for these is likely to be removed due to the lack of value they are considered to add given the detailed business case that is prepared and considered. We also agree that providing a comprehensive business case should result in a project initiation document not being necessary.

2.6 The project plan is created and approved by the Project Team working with the Information Systems Manager; this is approved by the sponsoring Director. Individual project managers meet on at least a monthly basis to confirm that the project is on track. The Information Systems Manager then provides reports to the sponsoring programme director and SLT on a monthly basis. The progress of the programme is reported to the Finance, Governance and Audit Committee as a control measure within the strategic risk register.

2.7 The Service has a target to complete post implementation reviews within three months of the project 'go live' date. From our testing of projects, one of which was completed in April 2017, the post implementation review is due to be completed in the immediate future; this is slightly behind the desired target date. Post implementation review dates have not yet occurred within the 3-month target. Whilst reviews should not be unnecessarily delayed it would be advisable to set the date following agreement of practical completion, although this may necessitate a compromise in relation to when the system has effectively achieved a go-live position for reporting purposes. We noted that

one project had a 'go live' date that did not appear to match that within Sycle on the project plan.

2.8 Whilst the Service has a clear methodology and system, currently there is no official procedure in place for managing projects. We acknowledge that this is something that the Head of Strategic Planning & Knowledge Management plans to complete during the summer/autumn 2017 and for which a draft exists. We recommend that this activity should be given a formalised target date and ensure that it contains criteria regarding the frequency of reporting and appropriate review meetings, as well as defining the guidelines on the use of the manually prepared coloured RAG progress reports sent to SLT. Appropriate commentary should be provided to explain or accompany any interpretation within the assessment being made by the Programme Manager of the information being generated by Sycle.

2.9 With respect to the training that the Service provides regarding the Sycle system, the project managers are predominately responsible for ensuring that the project team are fully competent in delivering the expectations required in a timely manner. All project staff members have access to advice manuals via 'Dwdle' site and also within Sycle, as there is a comprehensive user manual available which was demonstrated within the audit.

Taking account of the issues identified above and the recommendations contained within Appendix A, in our opinion the control framework for the area under review, as currently laid down and operated, provides **substantial assurance** that risks material to the achievement of the organisation's objectives for this area are adequately managed and controlled.

IT Health Check

2.10 The objective of the review was to ensure that IT suitably meet organisational need and are adequately protected from operational risk, security threats and environmental hazards.

2.11 To achieve a successful merger the Service needed to manage a significant level of transformation within its IT provision ensuring that systems can be accessed from all areas of the combined Authority through either increased compatibility or new infrastructure, whilst still maintaining a viable continuous service to both operational and support areas.

2.12 A costed roadmap of how the IT provision needed to transform was agreed as a basis for providing a seamless service. In this respect, work continues against the roadmap with a view to achieving this aim in accordance with the agreed strategy. This is monitored by senior management on a monthly basis. System users are engaged in the development function as appropriate, and this is viewed as generating a greater level of system ownership

2.13 To supplement the transformation appropriate policies and procedures have been developed and approved with access to systems controlled at an individual level; password management is in place and has been established in accordance with new industry standards. Penetration testing has been undertaken and where threats to security have been identified these are being managed through an action plan which is reviewed by the Head of department with an overview provided to the Director on a monthly basis. Most actions are due to be completed by end of September 2017.

2.14 The hardware asset inventory identifies details of those devices held, a history of ownership, and also provides details of those that attach to the network on a regular basis. This allows receipt of updates and patches as they are rolled out and management of those items that do not regularly attach to the network, allowing follow up and investigation of need.

2.15 The inventory record dating back to the early 2000s identifies a small number of items as 'lost'. These are of a low value, maybe obsolete or have been misplaced. If a device that contained Service data

were to be reported to the ICT Department as lost, then this would be raised as a security breach, and would be dealt with through the security breach procedure. We have recommended that these should be investigated further to establish and record the circumstances, if there is any latent potential threat prior to formal write off.

2.16 Reports on the Firewall performance are not produced as a matter of course and it is therefore recommended that the level of intrusion attempts should be reported on to senior management on a routine basis to highlight the inherent risk and residual risks being faced in what is clearly a potential threat to maintaining service provision.

Taking account of the issues identified above and the recommendations contained within Appendix A, in our opinion the control framework for the area under review, as currently laid down and operated, provides **substantial assurance** that risks material to the achievement of the organisation's objectives for this area are adequately managed and controlled.

APPENDIX A1 – 02/18 INFORMATION SYSTEMS MIGRATION

Management Objective:	Information systems suitably meet organisational need and are adequately protected from operational risk, security threats and environmental hazards.		
Responsible Officer:	Bob Ford – Head of Strategic Planning and Knowledge Management		
Risk areas for consideration: 1. The migration plan is incomplete and no management reporting, governance and follow-up in place to ensure successful transition 2. Project design and changes do not provide suitable resilience for front line and back office operations and successful migration. 3. Support activities and revised / new policies and procedures not embedded.			
Limitations to scope: Information Systems Migration audit to follow up work commenced in 2016/17.			
Overall opinion:	Substantial	Adequacy of control framework:	Good
		Application of control:	Good

Main Recommendations	Priority	Management Response	Implementation Plan
1. Information Migration Procedure We acknowledge that the documentation of the procedure for managing projects is a work programme target for the Head of Strategic Planning and Knowledge Management, but believe that a formal target date should be established for completion as this represents a key aspect of control within the process.	MA	The draft project management procedure will be finalised and issued.	**Responsibility:** Robert Ford, Head of Strategic Planning and Knowledge Management **Target date:** December 2017
2. RAG Indicator Guidance The progress monthly reports for SLT use RAG indicators as a mechanism for visually reporting on progress of projects across the programme. Guidelines should be introduced regarding definitions of progress, as the reports are not system generated within Sycle.	S	Guidelines to support an objective RAG status will be produced	**Responsibility:** Robert Ford, Head of Strategic Planning and Knowledge Management **Target date:** October 2017

3. Monthly Reporting We recommend that all 'Go Live' dates are checked on the monthly report and in Sycle to ensure that they all match correctly so as to enable an effective post-implementation review timetable.	**MA**	Go live dates will be further checked against the project plans and a post implementation timetable agreed.	**Responsibility:** Robert Ford, Head of Strategic Planning and Knowledge Management **Target date:** December 2017

APPENDIX A2 – 03/18 IT HEALTH CHECK

Management Objective:	To ensure the combined Service continues to migrate (transition) systems to a secure, reliable and resilient data centre and communications configuration capable of supporting its front line and back office operations. For clarity the scope includes: • Network integration • Active directory (AD) migration • Telephony • Service resilience		
Responsible Officer:	Chris Donaldson - Head of ICT		
Risk areas for consideration: 1. Responsibility for IT systems, IT needs and developments are poorly defined leading to lack of co-ordination, inconsistent developments, poor use of resources and failure to meet needs of core Authority functions. 2. The Authority's IT infrastructure and operating environment is insufficiently protected from internal and external threats increasing exposure to loss, theft and corruption. 3. Third party access to the Authority's systems is not appropriately controlled.			
Limitations to scope: The review is intended to deliver reasonable assurance as to the adequacy of the design of the internal control system and its application in practice at an organisational level by management responsible for the Authority's IT environment; the review does not extend to security testing such as penetration tests.			
Overall opinion:	Substantial	Adequacy of control framework:	Good
		Application of control:	Good

Main Recommendations	Priority	Management Response	Implementation Plan
1. IT Asset Inventory Reconciliation of the assets inventory has identified that there are a small number of devices logged as 'lost'. These devices should be investigated further to identify the reason for the loss and any potential security threat. Once verified as 'lost', the devices should be written off by the IT Manager and reported to the SLT as an information item on an annual basis.	S	On reviewing the lost items within the inventory we (ICT) have identified that we do need to change our process in the following ways: 1. Ensure that the inventory record for the lost equipment is suitably documented with comments to indicate what we suspect has happened, what we have done to attempt to locate it, and when we last tried to locate it. 2. Review lost records on a regular basis, and where relevant, follow up any comments, so that lost items are actively pursued - this is something that the ICT Service Desk could follow up on. 3. Review lost records to identify, if they are low risk, whether it would be appropriate to mark as disposed - an example would be a SIMM card where the comments indicate that the number has been ported to a new SIMM and the missing SIMM deactivated.	**Responsibility:** Chris Donaldson Head of ICT **Target date:** March 2018
2. **Intrusion attempts** There is currently no reporting conducted on intrusion attempts blocked by the Firewall. To provide a greater level of understanding for the senior management and to support continual investment needs, it is felt that an appropriate report detailing intrusion attempts blocked	MA	ICT is currently purchasing and installing a product (Alien Vault) which, amongst other things, will monitor and report on logs from multiple devices. This will allow us to produce reports from the firewalls as well as the system which protects against spam e-mails and mail virus attacks.	**Responsibility:** Chris Donaldson, Head of ICT **Target date: March 2018**

should be produced as an information item identifying the inherent risks being managed.			

APPENDIX B – SUMMARY OF OPINIONS & RECOMMENDATIONS

Reports being considered at this Finance and Audit Committee meeting are shown in italics. The definitions with regard to the levels of assurance given and the classification of recommendations can be found in the Notes section at the end of this report.

Audit	Progress	Opinion	Recommendations Made				
			F	S	MA	Total	Agreed
1. Communications	Final Report	Substantial	**0**	**1**	**3**	**4**	
2. IT Systems Migration Projects	Draft Report	Substantial	**0**	**1**	**2**	**3**	
3. IT Health Check	Draft Report	Substantial	**0**	**1**	**1**	**2**	
4. Business Case Management							
5. Strategic Workforce Planning							
6. Strategic Planning							
7. Key Financial Controls							
		Total	***0***	***3***	***6***	***9***	

At the moment there is nothing that impacts negatively upon our annual opinion.

APPENDIX C – OPERATIONAL PLAN 2017/18

Block 1 Audits - Finance and Audit Committee – 7 July 2017	Plan Days	Actual Days	Progress
1. Communications	10	10.0	
Follow Up	3	2.0	
Management	3	3.0	
Total	**16**	**15.0**	

Block 2 Audits - 29 September 2017	Plan Days	Actual Days	Progress
2. Information Systems Migration	10	9.5	
3. IT Health Check	8	9.5	
Management	2	1.5	
Total	**20**	**20.5**	

Block 3 Audits - 15 December 2017	Plan Days	Actual Days	Progress
4. Business Case Management	8	1.5	Considered complete as covered within review of ICT/ Systems Migration
5. Strategic Planning	8		
Management	2		
Total	**18**		

Block 4 Audits – 28 March 2018	Plan Days	Actual Days	Progress
6. Strategic Workforce Planning	6		
7. Key Financial Controls	15		
Follow Up	2		
Management	3		
Total	**26**		

TOTAL AUDIT DAYS 2017/18	80	37.0

APPENDIX D – PERFORMANCE INDICATORS YTD

Report Turnaround

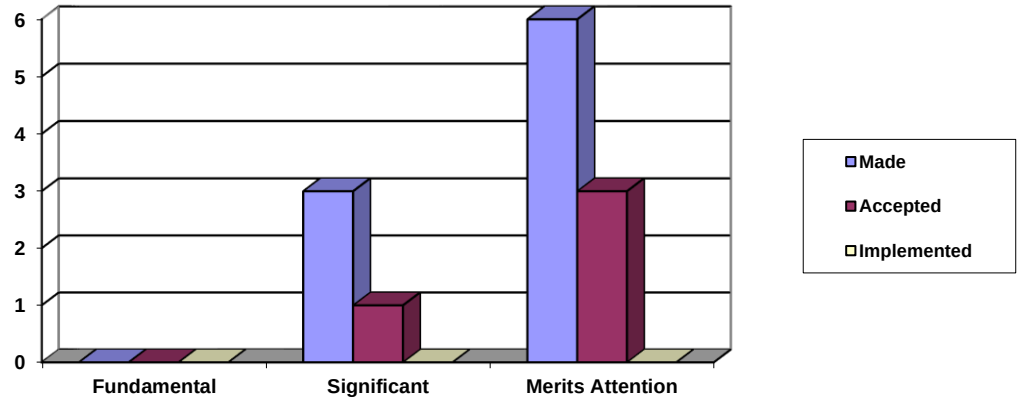
Performance Indicator	Target	Actual	Comments
Draft report turnaround (average working days)	10 days	1 day	
Final report turnaround (average working days)	5 days		

Resources

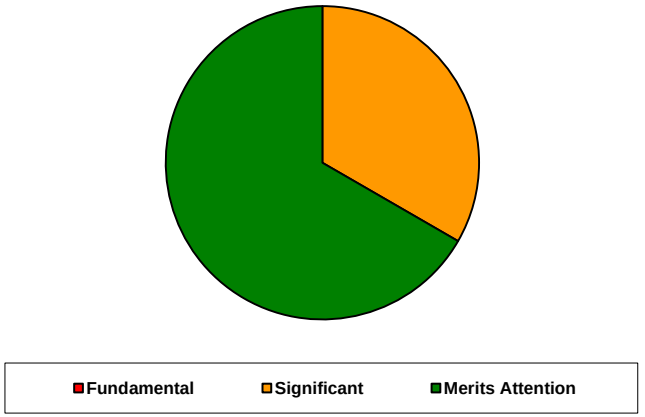
Performance Indicator	Annual	Actual	Comments
Number of Audit Days	80	37	On target
Audit Fee	Budget	Within budget	
Director Input	10%	26%	
Manager Input	15%		
IT Auditor Input	10%	13%	
Senior Auditor Input	35%	31%	
Auditor Input	30%	30%	

Recommendations

Made, Accepted & Implemented



Analysis of Priority



APPENDIX E – NOTES

KEY FOR RECOMMENDATIONS (IN RELATION TO THE SYSTEM REVIEWED)

Fundamental (F)	-	The organisation is subject to levels of fundamental risk where immediate action should be taken to implement an agreed action plan.
Significant (S)	-	Attention to be given to resolving the position as the organisation may be subject to significant risks.
Merits Attention (MA)	-	Desirable improvements to be made to improve the control, risk management or governance framework or strengthen its effectiveness.

ADEQUACY & APPLICATION OF CONTROL

OVERALL OPINION (ASSURANCE)	FRAMEWORK OF CONTROL	APPLICATION OF CONTROL	EXPLANATION	TYPICAL INDICATORS
Substantial (Positive opinion)	Good	Good	The control framework is robust, well documented and consistently applied therefore managing the business critical risks to which the system is subject.	There are no fundamental or significant recommendations attributable to either the Framework or Application of Control.
Appropriate (Positive opinion)	Good	Appropriate	As above however the audit identified areas of non-compliance which detract from the overall assurance which can be provided and expose areas of risk.	There are no fundamental recommendations surrounding the Framework of Control; coupled with no fundamental and no more than two significant recommendations attributable to the Application of those controls.
	Appropriate	Good	The control framework was generally considered sound but with areas of improvement identified to further manage the significant risk exposure; controls were consistently applied.	There are no fundamental recommendations attributable to the Framework of Control.
	Appropriate	Appropriate	As above however the audit identified areas of non-compliance which expose the organisation to increased levels of risk.	There are no fundamental recommendations attributable to the Framework and Application of Control.
Limited (Negative opinion)	Good / Appropriate	Weak	As above however the extent of non-compliance identified prevents the Framework of Control from achieving its objectives and suitably managing the risks to which the organisation is exposed.	There are more than two significant recommendations attributable to the Application of Controls.
	Weak	Good / Appropriate	The control framework despite being suitably applied is insufficient to manage the risks identified.	There are more than two significant recommendations attributable to the Framework of Controls.
	Weak	Weak	Both the Framework of Control and its Application are poorly implemented and therefore fail to mitigate the business critical risks to which the organisation is exposed.	There are fundamental recommendation(s) attributable to either or both the Framework and Application of Controls which if not resolved are likely to have an impact on the organisations sustainability.
The above is for guidance only; professional judgement is exercised in all instances.				