Joanne Brown
Director
T: 0141 223 0848
E: joanne.e.brown@uk.gt.com

Peter Clark
Manager
T: 0131 659 8505
E: peter.c.clark@uk.gt.com

Argyll and Bute Council

IT internal audit indicative three year needs assessment (2016/17 – 2018/19) – DRAFT report

Distribution		Timetable	
For action	Gerry Wilson (ICT and Digital Manager)	Fieldwork completed	
	Kevin Anderson (Internal audit)	Draft report issued	
For information		Management comments	
		Final report issued	

Contents

Sections

It is the responsibility solely of Argyll and Bute Council's management to ensure that there are adequate arrangements in place in relation to risk management, governance and control.

1 Executive Summary

1.1 Background

IT skills and experience are essential to the service delivery and operation of Argyll and Bute council. Under the Internal Audit Framework Contract with the Council, the Council's Head of Internal Audit has asked Grant Thornton to undertake an IT needs assessment to inform future IT audit plans. The primary purpose of the IT needs assessment was to help identify and prioritise the key areas for inclusion in the Internal Audit Plan over the next three years.

The IT needs assessment involved a review of previous audit activity (which is summarised in Appendix A), meetings with key staff and review of relevant documentation. The information obtained during this initial exercise was documented and risk assessed to identify those areas of greatest concern to Argyll and Bute Council.

1.2 Scope

The IT needs assessment looked at the following areas:

- Asset Management
- IT Service Management
- Change Management
- Database Security
- Data Warehousing
- Application Security
- Implementation Audit
- ICT Maturity
- Disaster Recovery
- Service Level agreements
- Capacity and Performance
- System Development
- Application Effectiveness
- Data Protection Act

1.3 Overall conclusion

From the 14 areas looked at we identified three areas of high risk and two areas of medium risk. In order to meet with Argyll and Bute's budgetary requirements we propose that reviews for 2016/17 cover the following areas:

- Contracts and agreements in place with third party providers of IT, including: tendering, service provision, KPIs, change management, roles and responsibilities

- Application Security, including passwords and use of privileged accounts

Given the range and scope of IT systems in use at the Council consideration should also be given to undertaking a General IT Controls audit which could cover access security, licenses, back-ups, patch management, batch jobs and change management. This could be conducted in the first, and third years, of the audit plan.

The table on the following page details the key findings from our review, while Appendix B outlines a suggested IT audit plan over the next three years.

1.4 Acknowledgement

We would like to take this opportunity to thank the staff involved for their co-operation during this IT needs assessment.

2 Detailed Findings

1.	Low risk	Asset Management

Finding	To be included in 2016/ 17 audit plan?
An asset tagging system is in place. Assets are tagged when they come in to / arrive at the council. Annual reconciliations are undertaken between the asset tag listing and the physical assets.	No Reason: Well established process.

2.	Medium risk	IT Service Management

Finding and Implication	To be included in 2016/ 17 audit plan?
A new Service Desk system, TopDesk, is in the process of being rolled out. This is expected to be fully functional by March 2017. The service desk can be contacted 24 hours a day by email, or between 8am and 6pm during the week. Monthly KPIs and target resolution times are reported upon.	No Reason: While the new system introduces risks it is not planned to be fully implemented until 2017. As such it could be included in the 2017/18 audit plan.

3.	High risk	Change Management

Finding and Implication	To be included in 2016/ 17 audit plan?
Third party involvement with the provision of IT services, particularly around HR and payroll, was considered to require improvement. In particular the change management process, separation of roles and responsibilities, provision of training on the use of the systems as well as monitoring of internal training undertaken, and provision of upgrades was considered inadequate.	Yes Reason: With third party involvement over a number of key IT systems a review covering the change management and systems development processes, along with the split of responsibilities and any SLAs in place, is proposed for 2016 / 17. Additionally a review, specifically focusing on the Change Management process at the Council is proposed for 2017/18

4.	Low Risk	Database Security

Finding and Implication	To be included in 2016/ 17 audit plan?
Annual external health checks are in place to scan databases for vulnerabilities, as well as internal quarterly database scans.	No Reason: Regular scanning and well understood process.

5.	Low Risk	Database Warehouse

Finding and Implication	To be included in 2016/ 17 audit plan?
N/A – no data warehousing	No Reason: N/A

6.	Medium Risk	Application Security

Finding and Implication	To be included in 2016/ 17 audit plan?
Password controls are in place for applications, servers and desktops. There is no single sign on in place at the moment - Desktop and Server password settings are controlled by the IT team, while application passwords are the responsibility of the system owner. User accounts are not provided with enhanced privileges, instead shared privileged accounts are used to access these privileges.	Yes Reason: Possibility for increased risk due to shared privileged accounts depending on how these are logged and monitored.

7.	Low Risk	Implementation Audit

Finding and Implication	To be included in 2016/ 17 audit plan?
Processes are in place for both replacement of applications and servers This includes testing outside of the live environment and backups.	No Reason: Well understood and defined process

8.	Low Risk	ICT Maturity

Finding and Implication	To be included in 2016/ 17 audit plan?
IT is considered to be heavily embedded at the Council. Systems and applications are purchased on the open market, with suppliers responsible for maintaining them and the council responsible for hosting them	No Reason: Well understood and defined systems in place

9.	Low Risk	Disaster Recover

Finding and Implication	To be included in 2016/ 17 audit plan?
IT operations can be operated from two physically separate sites. Additionally there are two physically separate data centres. Data is copied between these sites and tape backups are stored off site. Annual disaster recovery exercises are undertaken.	No Reason: Well understood and defined process

10.	High Risk	Service Level Agreements

Finding and Implication	To be included in 2016/ 17 audit plan?
Service Level Agreements (SLAs) are in place with third party providers, but there have been issues with some services provided. Additionally there are not SLAs in place internally between departments.	Yes Reason: With third party involvement over a number of key IT systems a review covering the change management and systems development processes, along with the split of responsibilities and any SLAs in place, is proposed for 2016 / 17.

11.	Low Risk	Capacity and Performance

Finding and Implication	To be included in 2016/ 17 audit plan?
Network capacity is provided by Vodafone with bandwidth analysis having been conducted in 2015. Capacity allows for at least 5 new servers to be added each year. A new network contract is in the process of being agreed with Swan.	No Reason: Well understood internally; Internally tested in last year

12.	High Risk	Systems Development

Finding and Implication	To be included in 2016/ 17 audit plan?
Limited risk identification is undertaken by the council for new system development as reliance is placed on the third party providers for this. Nevertheless there have been issues in the last year in regards to HR/payroll and VAT.	Yes Reason: With third party involvement over a number of key IT systems a review covering the change management and systems development processes, along with the split of responsibilities and any SLAs in place, is proposed for 2016 / 17.

13.	Low Risk	Application Effectiveness

Finding and Implication	To be included in 2016/ 17 audit plan?
Key applications are assessed and included within an annual Group Asset Management Plan (GAMP). An annau IT health check also identifies out of date systems, or systems which have not been utilised recently. There is an internal process in place for raising concerns relating to applications which would allow the ICT Steering Board to consider if applications are in line with legislative requirements and up to date.	No Reason: Well understood process; Annually checked

14.	Low Risk	Data Protection Act

Finding and Implication	To be included in 2016/ 17 audit plan?
While the IT team enforce controls around access (such as limits to the use of USB devices, encrypted hard drives and mobile phones) day to day responsibility for compliance with the Data Protection Act does not lie with the IT team	No Reason: Well understood process; Controls are in place

3 Appendix A

3.1 The below table shows all internal audits undertaken in the last three years by Argyll and Bute Council which related to IT

Audit Title	Scope	Date
Review of CareFirst	Assessment of the CareFirst system, which is a web based case management system utilised in the Social Work Department	March 2014
Review of Electronic Signatures and authorisation methods	Review of the use, processes and policies in place	September 2015
Information Communications Technology Review	Assessment of compliance with the public service network code of connection (PSN CoCo)	May 2015
Performance Management Review	Review of the integrity of data used for performance information	Nov 2015
Review of records management plan and information security	Assessment of the councils compliance with the public records (Scotland) Act, and the council's management of public records against the data protection act	Jan 2015
Review of Roads Costing System	To ascertain whether the Roads Costing system application incorporates adequate internal controls, ensure that they are effective and are not invalidated when changes are made	Jan 2013
Review of Uniform System	To ascertain whether the Uniform system application incorporates adequate internal controls, ensure that they are effective and are not invalidated when changes are made	March 2014

4 Appendix B

4.1 Suggested IT audit plan over three year period

	Year 1	Year 2	Year 3
IT Audit Name	16/17	17/18	18/19
General IT Controls (GITC) , including application security	Yes	-	-
Third party providers	Yes	-	-
IT Service Management	-	Yes	-
Change Management	-	Yes	-
General IT Controls	-	-	Yes
Follow up review of actions and recommendations raised	-	-	Yes

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

grant-thornton.co.uk