INTERNAL AUDIT OUTSTANDING AUDIT RECOMMENDATIONS
PERIOD: 01 APRIL 2015 TO 31 JANUARY 2017

Summary	Total	R	A
1. Completed Audits	2	0	2
2. Follow Up Audits Completed	3	0	3
3. Advice And Guidance / Consultancy	0	0	0

INTERNAL AUDIT OUTSTANDING AUDIT RECOMMENDATIONS

PERIOD: 01 APRIL 2015 TO 31 JANUARY 2017

1. Completed Audits - RED, AMBER or GREEN flag

Audit	Date	Area [Section]	Organisational Risk	Areas for Development / Improvement and comments	Total Recs (H)	Timescale / Responsible Officer	Outcome	BRAG Status
Information Governance and Security - Intranet Policies and Guidance	12/07/2016	Authority Wide	Minor	Ten recommendations were made which do not present a significant risk to the organisation.	10 (0)	November 2016 Authority-Wide	The Head of Digital reported at the January ARMC meeting that all audit recommendations will be completed by May 2017.	A
Cyber Security	26/09/2016	Business Services [Digital]	Moderate	Ten recommendations were made covering: - information security policies - firewalls - vulnerability monitoring - rogue wireless access points - information risk register - information security training - cyber insurance	10 (0)	June 2017 Director of Business Services	The Head of Digital reported at the January ARMC meeting that all audit recommendations will be completed by May 2017.	A

INTERNAL AUDIT OUTSTANDING AUDIT RECOMMENDATIONS

PERIOD: 01 APRIL 2015 TO 31 JANUARY 2017

2. Follow Up Audits Completed - RED, AMBER or GREEN flag

Audit	Follow up date	Original Report date	Area [Section]	Organisational Risk Position as at the date of the original audit	Areas for Development / Improvement and comments	Original Total Recs (H)	Implementation timescale for all actions Director	Outcome	BRAG Status Current position	Organisational Risk Current Position
ICT Business Continuity	04/09/2015	Dec 14	Authority-Wide	Moderate	Ensure that all Directorates include ICT business continuity requirements in their risk registers and CESG to approve the critical services list so that business continuity plans can be put in place using the new template.	4 (4)	December 2015 Authority-Wide	The Head of Digital reported at the January ARMC meeting that the project will be complete by September 2017. This area is included in the draft Internal Audit plan for 2017/18.	A	Moderate
Payment Card Industry - Data Security Standard	04/09/2015	Jul 14	Authority-Wide	No opinion required at the time the audit was carried out.	Original review highlighted that the Council is currently not compliant with the standard, but appropriate measures, decisions and actions have or will be taken to ensure compliance in due course. 1 High priority recommendation. is outstanding: 1) Determine and implement the most appropriate installation in the Customer Services Centre, ie running Paye.net in a virtualised environment, running two machines on each desk with a KVM (keyboard, video and mouse) switch, running machines in separate secure environment via RDP (remote desktop protocol).	3 (1)	December 2015 Director for Business Services	The Head of Digital reported at the January ARMC meeting that the project will be complete by May 2017. This area is included in the draft Internal Audit plan for 2017/18.	A	Minor
Data Loss Prevention	07/11/2016	Oct 14	Authority-Wide	Major	A DLP policy for the management of information assets should be produced, agreed by the Information Governance Board, and made available to all staff. This will ensure the correct management of information via the delivery of a technical solution by IT Services and the development and enforcement of appropriate working practices by Information Asset Owners.	3 (3)	January 2017 Information Governance Board	The Head of Digital reported at the January ARMC meeting that the project will be complete by May 2017. This area is included in the draft Internal Audit plan for 2017/18.	A	Major

KEY:

Organisational Risk	
MAJOR	The likelihood/impact of the risks identified during the review, should these materialise, would leave the Council open to major risk.
MODERATE	The likelihood/impact of the risks identified during the review, should these materialise, would leave the Council open to moderate risk.
MINOR	The likelihood/impact of the risks identified during the review, should these materialise, would leave the Council open to minor risk.
NEGLIGIBLE	There were no weaknesses identified during the review.

RAG status		
B	**Audits**	All actions agreed and implemented, with no further Internal Audit action necessary.
	Follow Ups	All actions implemented, with no further Internal Audit action necessary.
G	**Audits**	Most actions agreed and implemented, e.g. low priority recommendations are outstanding, with no further Internal Audit action planned.
	Follow Ups	Most actions implemented, e.g. low priority recommendations are outstanding, with no further Internal Audit action planned.
A	**Audits**	Actions agreed and officers committed to implement within agreed timescale.
	Follow Ups	Actions in process of being implemented within agreed timescale with some implemented.
R	**Audits**	Actions agreed
	Follow Ups	Little or no progress made to implement actions within agreed timescale.

Recommendation Priority Rating	
HIGH	A matter that is fundamental to the control environment for the specific area under review. The matter may cause a system objective not to be met. This needs to be addressed as a matter of urgency (suggested timescale: within one month).
MEDIUM	A matter that is significant to the control environment for the specific area under review. The matter may threaten the achievement of a system objective.
LOW	A matter that requires attention and would improve the control environment for the specific area under review. The matter may impact on the achievement of a system objective.