INTERNAL AUDIT OUTSTANDING AUDIT RECOMMENDATIONS
PERIOD: 01 APRIL 2016 TO 31 OCTOBER 2017

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

INTERNAL AUDIT OUTSTANDING AUDIT RECOMMENDATIONS

PERIOD: 01 APRIL 2016 TO 31 OCTOBER 2017

1. Completed Audits - RED or AMBER flag

Audit	Date	Audit Area as per plan	Organisational Risk	Summary of Findings and Conclusions	Total Recs (H,M)	Implementation timescale for all actions Responsible Officer	Status	RAGB Status
Cyber Security	26/09/2016	Business Services	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 Head of Digital	The Head of Digital reported at the January ARMC meeting that all audit recommendations will be completed by May 2017. 11/09/17 - The Head of Digital reported at the June ARMC that of the five medium recommendations (five were low), two are included in the Data Centre Project and the remaining three relating to Information Governance will be covered as part of the ICO audit. 03/11/17 - The Head of Digital is providing an update report at the November ARMC meeting.	A

INTERNAL AUDIT OUTSTANDING AUDIT RECOMMENDATIONS

PERIOD: 01 APRIL 2016 TO 31 OCTOBER 2017

2. Follow Up Audits Completed - RED or AMBER flag

Audit	Follow up date	Original Report date	Audit Area as per plan	Organisational Risk Position as at the date of the original audit	Summary of Findings and Conclusions	Original Total Recs (H,M)	Implementation timescale for all actions Responsible Officer	Status	RAGB 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. The Head of Digital will include an update on this in his report to ARMC in November.	A	Moderate
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. 03/11/17 - The Head of Digital will include an update on this in his report to ARMC in Nov	A	Major
Patch Management	23/05/2017	Feb 16	Business Services [Digital]	Minor	Four high risk recommendations relating to implementing an approved patching policy, including the patching methodology and management information, and ensuring patches applied as appropriate in the DMZ.	8 (4)	July 2017 Head of Digital	Four of the eight recommendations have been implemented. A new implementation date of July 2017 has been proposed for the remaining outstanding recommendations. The SIRO presented a report to ARMC in June 2017 identifying progress currently being made to address all required actions.	A	Minor

KEY:

Organisational Risk	
MAJOR	A major organisational risk opinion indicates that the likelihood/impact of the risks identified during the review, should they materialise, would leave the Council open to major risk of a fundamental or material nature. This opinion suggests that there are some potentially serious weaknesses in the design and/or operation of the control environment that may have a significant impact on the achievement of systems and or corporate objectives if not addressed.
MODERATE	A moderate organisational risk opinion indicates that the likelihood/impact of the risks identified during the review, should they materialise would leave the Council open to moderate risk of a fundamental or material nature. This opinion suggests that there are some weaknesses in the design and/or operation of the control environment that may have varying degrees of impact on the achievement of the systems and/or corporate objectives.
MINOR	A minor organisational risk opinion indicates that the likelihood/impact of the risks identified during the review, should they materialise, would leave the Council open to minor risk.
NEGLIGIBLE	A negligible organisational risk opinion indicates that there were no weaknesses identified during the review and that the Council is not exposed to any risks directly associated with the findings.

RAGB 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.