Warwick District Council

ICT Audit Strategic Plan

2017/18 to 2019/20

May 2017

ICT Audit – Strategic Plan 2017/18 to 2019/20

Introduction

1.1 The development of an appropriate Information, Communication and Technology (ICT) Internal Audit Strategy and annual operational plan by conducting an audit needs assessment (ANA) represents a critical ingredient in the provision of an adequate, relevant and timely internal audit service. It not only identifies those activities and risks which management consider to be of most significance to the organisation, but it also allows wider consideration of potential risks based on the internal auditor's experience so that those systems which manage business critical and significant risks are identified in order to attach appropriate risk factors to each auditable area. This ensures that internal audit's efforts are effectively prioritised and focused upon the organisation's key objectives and current issues, so that the benefits from investment in audit are maximised through the development of an informed and effective internal audit strategy.

1.2 This assessment is specifically intended to consider the internal audit priorities going forward and has been undertaken largely by:-

(1) meeting with members of the management team

(2) meeting with the ICT Manager and his team;

(3) consideration of the results of, or proposals to undertake other internal audit work and factoring this into the process;

(4) Review of the corporate and ICT risk register, which has been a valuable source of information in constructing the strategic plan; and

(5) Internal audit experiences from elsewhere.

This enables internal audit to draw together what we feel represents a comprehensive review of the (ICT) internal audit needs of the Council for the period 2017/18 to 2019/20.

1.3 The outputs from the meetings and discussions have then been considered and assessed by the internal auditor in conjunction with known current and future risks in order to develop a strategy for the future scope of the (ICT) internal audit services.

1.4 We are grateful to those staff involved in the discussions for their co-operation during the needs assessment, the risk analysis and for the time that they took to consider the issues being addressed.

1.5 The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

ICT Audit Strategy

2.1 An internal audit strategy which addresses issues of risk and priority is contained within the report as Appendix A. This is annotated with any relevant information obtained during the assessment.

2.2 We have a medium-term vision with regard to the internal audit strategy that we believe will satisfy both the needs of the Council's business going forward and also good governance through control assurance year on year. We appreciate the benefit of information provided by the in-house internal audit service to inform the process which has also been very useful. We are also happy with the balance of the work over the forthcoming three years so that no one area, department, system or function is over or under audited in any one period.

2.3 With the above in mind we have structured the audit plans on the basis of known risks or significance of project at the time of preparation. However, there is a clear need to re-visit the plans to ensure that they stay focused on those risks and reflect any emerging changes.

ICT Audit Risks

3.1 In undertaking the ANA we assess systems against various categories of risk, which are described below some of which are more or less relevant to the auditable area. We have also used such documents that were made available so as to further inform the audit needs assessment, and the resultant strategic plan.

1 - Fraud & misappropriation
2 - Safeguarding of assets
3 - Efficiency and effectiveness
4 - Safety and security of people
5 - Financial control
6 - Achievement of objectives
7 - Business management
8 - Adequacy of management information
9 - Safety and security of data and information
10 – Compliance (legislation & regulation)

3.2 During the ANA we try to remain focused on identifying auditable systems and controls which manage these risks and attempt to place them into the above risk categories.

3.3 We have made a high level assessment of each system made known to us from the discussions with ICT management in terms of its relative importance and its likely risk impact and have allocated a number of days to the audit of each system so that:

- all aspects of perceived risk are comprehensively audited during the three year period of the strategy;
- internal audit days are optimally used over the life of the plan according to perceived greatest risk.

3.4 Whilst the plan provides no contingency for ad-hoc advice to the council, the plan is flexible and will also be refreshed annually to ensure that emerging risks, not clear at the time of preparation, can be included. By this means we will ensure that the forward plans will provide the right level of assurance to the ICT risks faced by the Council.

APPENDIX A

2017/18 Plan

Audit	Indicative Scope	Indicative Days	Indicative Timing
Cyber Security	An assurance review of the level of control to offset the ongoing risk of cyber-attack, including an assessment against the guidelines in the Cyber Essentials Scheme (CES) as follows:- • Firewalls and Internet gateways; • Secure configuration; • Access control; • Malware protection; and • Patch management.	8	Q2
Information Governance	An assurance review of the information governance arrangement in light of the legislation changes in 2018 and to include information asset policies, ownership, categorisation, and sharing along with the ICT evidencing arrangements and technical controls which the new Act imposes.	6	Q2
Remote Access	An assurance review to evaluate the security controls and data integrity arrangements for staff using remote technology, including access protocols to network infrastructure and data, data storage arrangements, transmission protocols, and mobile device management.	6	Q3
Business System	An assurance review of the Paris Income Management application incorporating access rights and privileges, audit trails, system administration functions, application support, data and system backup.	7	Q2
Total		**27**	**-**

2018/19 Plan

Audit	Indicative Scope	Indicative Days	Indicative Timing
Database security	An assurance review to ensure that database system administration processes are sound and that adequate logical security settings have been implemented on the live server database environment. The database security build standards, access rights for database administrators and super-user privileges, password controls, security patching, vulnerability scanning, database auditing, and capacity / performance management will also be included.	7	Q1 TBC
System Ownership and Management	An assurance review of system administration and user account management for (key) business systems to ensure robust access controls, information (security) management, upgrade and licensing methodologies.	7	Q2 TBC
Financial Systems Interfaces	An evaluation of the efficiency and effectiveness of the interface files provided by various applications into the finance system.	6	Q3 TBC
Total		**20**	**-**

Note: the scopes are specifically pitched at high level in the above plan, and will be re-visited at the start of the year to ensure the work is still required and then detailed scopes will be provided.

2019/20 Plan

Audit	Indicative Scope	Indicative Days	Indicative Timing
Infrastructure	An assurance review of the continued security and resilience of the ICT network infrastructure during / after the relocation planned for 2019. Added to this review may be an element of ensuring the best use is being made of the available technologies.	7	Q1 TBC
Cloud applications	An assurance review to assess the risks known to exist as a result of the increased use of cloud technologies within the Council. This involved the assessment of the Council's risk profile against the risks identified from sources including the Cloud Security Alliance, and controls in place to mitigate the following risks: • Systems and data are lost, or becomes unavailable; • Council's reputation is damaged or financial losses are incurred due to inappropriate activity or lack of understanding; • Service standards and/or efficiencies are not realised.	7	Q2 TBC
Information Systems Policies	An assurance review of the continued relevance of the key information systems and security policies and the understanding of them and adherence to them in the operational areas of the Council.	6	Q3 TBC
Total		**20**	**-**

Note: the scopes are specifically pitched at high level in the above plan, and will be re-visited at the start of the year to ensure the work is still required and then detailed scopes will be provided.