Agenda No

AGENDA MANAGEMENT SHEET

Name of Committee	**Audit And Standards Committee**
Date of Committee	**22 November 2006**
Report Title	**IT Audit Plan 2006 - 2009**
Summary	This report seeks approval for the IT Audit plan for 2006 – 2009.
For further information please contact:	Greta Needham Head of Law and Governance Tel: 01926 412319 greatneedham@warwickshire.gov.uk Garry Rollason Audit and Risk Manager Tel: 01926 412679 garryrollason@warwickshire.gov.uk
Would the recommended decision be contrary to the Budget and Policy Framework?	No.
Background papers	None

CONSULTATION ALREADY UNDERTAKEN:- Details to be specified

Other Committees	☐	.....
Local Member(s)	☒	Not applicable
Other Elected Members	☐	.....
Cabinet Member	☒	Cllr Fowler
Chief Executive	☐	.....
Legal	☒	Reporting officer
Finance	☒	Dave Clarke
Other Chief Officers	☐	.....
District Councils	☐	.....
Health Authority	☐	.....
Police	☐	.....
Other Bodies/Individuals	☐	.....

FINAL DECISION YES

SUGGESTED NEXT STEPS: Details to be specified

Further consideration by this Committee	☐	.....
To Council	☐	.....
To Cabinet	☐	.....
To an O & S Committee	☐	.....
To an Area Committee	☐	.....
Further Consultation	☐	.....

Agenda No

Audit And Standards Committee – 22 November 2006.

IT Audit Plan 2006 - 2009

Report of the Strategic Director of Performance and Development

Recommendation

That the Committee approves the proposed IT Audit plan.

1 Members will be aware of the rapid pace of change in computer and communications technology and the significant investment that the Council is making in this technology. To make an effective contribution to these developments and to ensure that new computer systems are secure requires specialist audit skills. These skills are in short supply nationally and are expensive. Consequently, the County Council in common with many other organisations buys in specialist help, as it is uneconomic to maintain an adequately skilled in-house capability.

2 In 2002 the Council's then external auditors were asked to provide specialist IT audit services. As PriceWaterhouseCoopers are no longer the Council's external auditors a review of our approach to IT audit was undertaken in 2005. As a number of districts in Warwickshire also needed to review their arrangements for IT audit it was agreed that the County Council and district councils would jointly tender for these services. The result of this exercise was that a new provider (Haines Watts) was appointed to provide IT audit services at a daily rate which is much lower than that charged by PWC.

3 The service to be provided is an independent and impartial IT audit service to the County Council and the districts in accordance with best professional practice as outlined by CIPFA in its computer audit guidelines. The Internal Audit Strategy for 2006 approved by the Standards Committee on 3 May indicated that the first task of Haines Watts would be to prepare a detailed risk assessment and audit plan. This work has now been completed and a copy of their report is attached.

4 The draft plan provides for 80 days of IT audit each year (on average). The plan focuses on key areas and allows only a high level review of the more technical areas. Members will appreciate that this is not an unreasonable number of days given the complexity of the Council's IT infrastructure, scale of IT developments and pace of change required to support the new ways of

working agenda. Even so, funding within the existing internal audit budget is only available for some 40 days of work.

5 A bid for extra funding in 2007/8 onwards, to allow the full plan to be commissioned, has been submitted. However, for 2006/7 IT audit work will be limited to that which can be funded from existing budgets.

6 The Committee is asked to consider the draft plan.

DAVID CARTER
Strategic Director of Performance and Development

Shire Hall
Warwick

3 October 2006

PRIVATE AND CONFIDENTIAL

WARWICKSHIRE COUNTY COUNCIL

INTERNAL AUDIT

IT Audit Planning Review

2006/2007

DRAFT REPORT V2

AUDITOR:	**Yusuf Denath, HW Consulting**
TELEPHONE NUMBER:	**01827 61835**
AUDIT VISITS:	**June & July 2006**
DISTRIBUTION LIST:	▪ **Garry Rollason, Audit & Risk Manager**
	▪ **Tonino Ciuffini, Head of ICT**

CONTENTS **Page**

1.0 Introduction

1.1 A strategic audit planning review encompassing a risk assessment based on eighteen generic categories has been conducted to assist in the production of the ICT Strategic Audit Plan for the financial years 2006/2007, 2007/2008 and 2008/2009.

1.2 In carrying out this review we have taken into account the findings of the recent Audit Commission ICT Healthcheck Document to supplement our discussion with Warwickshire County Council staff

1.3 Our preferred approach to IT strategic audit planning comprises two elements, namely:

- Fundamental financial computer applications. (These should be subject to periodic review); and
- All other areas of IT provision should be audited on the basis of risk.

1.4 To reflect the above, we have adhered to the following indicators to prioritise fundamental financial applications for the purpose of audit planning, as follows;

- Internal Audit's order of priority, as indicated by Garry Rollason, Audit & Risk Manager;
- The anticipated life expectancy of the application if due for replacement within the next three years;
- Whether the application has been subject to significant downtime or disruption in the last three years; and
- The year that each application was last subject to significant IT audit work.

1.5 The order of priority is taken from a detailed risk assessment which utilises the total risk weighting calculated for each category. Where the same risk weighting applies to more than one category, the priority order has been based upon information gained from the narrative questionnaire and upon the Auditor's experience and understanding of IT in local authorities.

1.6 Allocation of time to audit is provided on an estimate that is dependent upon the actual scope of the audit concerned. In view of the limited number of days available for IT audit, the number of days shown for each audit is the minimum required to conduct a "key controls" review of each area.

2.0 Objectives and Scope

Objectives

2.1 The objectives of the audit planning review were as follows:

- To reflect corporate risks that have been identified by the Authority and which originate from or impact upon the provision of ICT services;
- To reflect the IT audit requirements placed upon Internal Audit by the Authority's external auditors;
- To incorporate any regulatory and other external obligations that affect the Authority's ICT provision but have not been highlighted by the corporate risk register;
- To risk assess key areas of ICT provision. The areas covered reflect the coverage of the ISO17799 Information Security Management standard; and
- To produce a structured IT audit plan that provides a weighted, prioritised audit programme that reflects external requirements, corporate priorities, current facilities and planned changes.

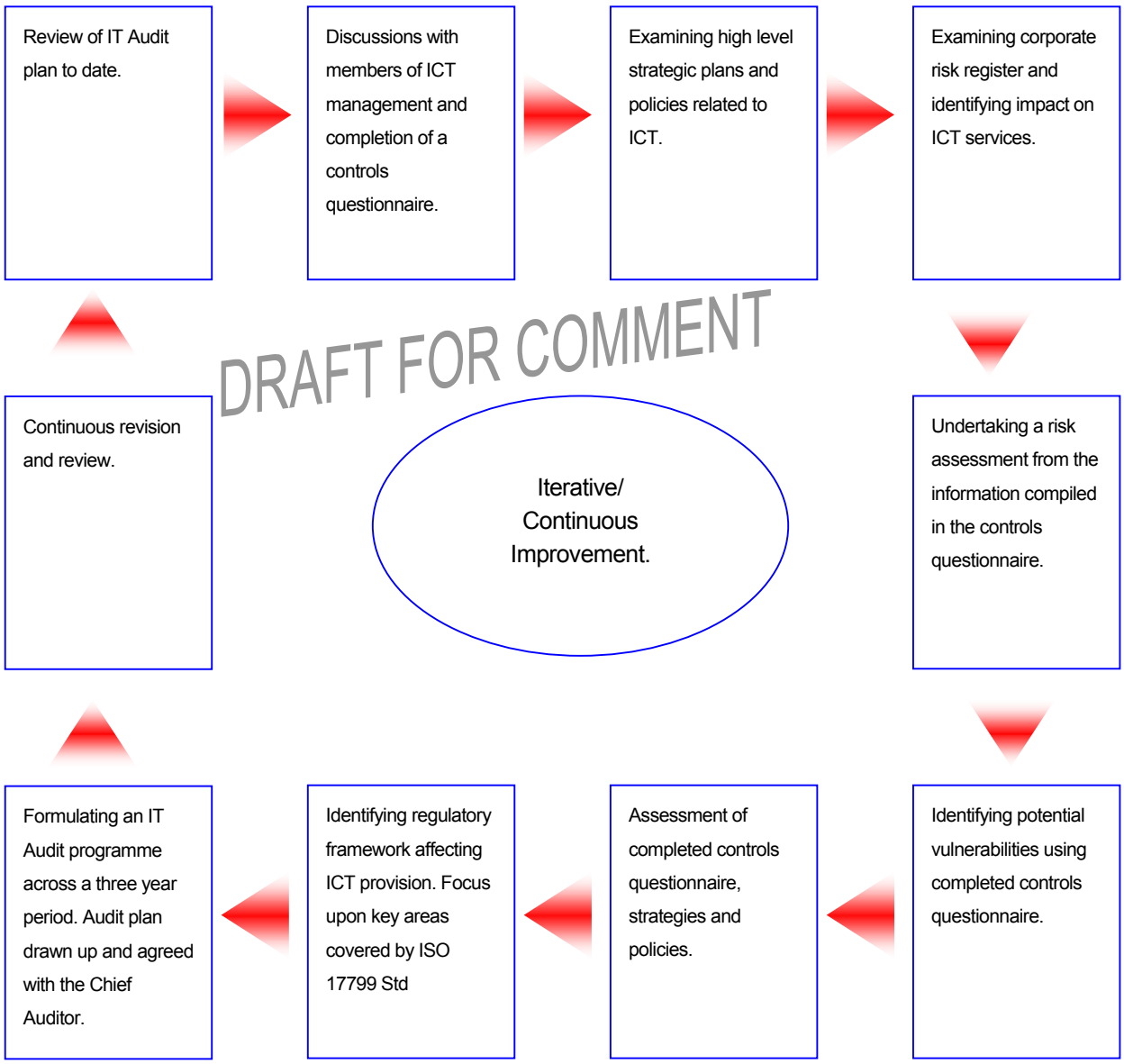
Scope

2.2 This audit planning review was restricted to a review of documented strategies and policies, including the recent Audit Commission ICT Healthcheck Report and discussions with key members of IT staff. Only limited testing has been carried out.

3.0 Audit Approach

3.1 The audit planning work was completed during June and July 2006, utilising the process illustrated below.

Audit planning methodology



3.2 The Auditor, Yusuf Denath, would like to acknowledge and thank all members of staff who contributed to the plan for their co-operation.

4.0 Executive Summary

4.1 Based on our audit assessment, an IT audit provision of approximately 75 days per year is required, this compares with the 40 days per year that is available for allocation to IT audit work. Consequently, the limited resources available are insufficient to permit audit work to be undertaken for each fundamental application and for each of the categories covered by the risk assessment. Whilst a recommended plan for each year has been provided here, it must be noted that this is subjective. The decision as to the content of the three-year plan must ultimately be made by the Audit and Standards Committee in conjunction with advice given by the Audit and Risk Manager and Haines Watts.

4.2 In compiling the plan, priority has been given to the audit of the fundamental financial applications. Each of the financial applications that were confirmed during the review have therefore been featured within the recommended plan. Consequently, several areas of IT activity that have been highlighted to require IT audit work do not feature. These are as follows:

- Software Licensing;
- Provision of IT Services (eg: performance management)
- Highways Management; and
- Operating Systems.

It is recommended that the areas listed above be monitored to assess the ongoing risk profiles. A decision should then be made as to whether to undertake an audit or to substitute with a planned audit whose risk profile changes. In the event of any additional budget becoming available during the course of the plan, consideration should also be given to the above risk-based areas.

It should also be noted that in addition to the specific audits included in the plan it is wise to include a contingency for each year. Current practice dictates that a contingency of in the order of 10% of the planned days is advisable.

4.3 For an in-depth analysis of our proposed plan, please refer to the main body of this report.

5.0 Recommended Audit Plans

5.1 First Year (2006/2007)

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
IT Strategic Audit Planning Review	N/A	▪ Formation of the IT audit plan	8	8
ICT Strategy (Input at the start & finish of current review to check process & output. also monitoring the implementation plan over next 2-3 years.}	Risk-based	▪ The strategy approval process.	2	10
Network (As above)	Risk based.	▪ See ICT Strategy	2	12

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Network Security & Administration (To link to review of Network Security & Firewall Configuration design)	Risk Based	▪ Compliance with strategy ▪ Network responsibilities ▪ Network administration ▪ Control over remote access ▪ Control over ISP connections ▪ Control over connections to shared partnership buildings ▪ Documentation, policies and training. ▪ Network management and monitoring. ▪ Installation of network connections and equipment ▪ User authentication.	12	24
Virus Controls/Firewalls As this follows the Network Security review need to ensure scope links to the previous review particularly the	Risk based	▪ The selection, installation and configuration of anti-virus software ▪ Update of signature file for	8	32

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
relationship to firewalls which is anticipated will form a major part of the Network Security review.		desktop and server software ▪ Coverage provided by anti-virus software ▪ Procedures for dealing with infections ▪ ICT and user responsibilities ▪ User training and guidance ▪ Monitoring procedures		
Social Care (OLM – Carefirst)	Key Business Application	See scope for Payroll	15	47
Customer Relationship Management (Northgate Frontoffice) (Possibility of coordinating with Districts)	Key Business Application	▪ System administration and user access ▪ Incoming interfaces ▪ Control over system parameters ▪ Configuration documentation ▪ Audit trail ▪ Application recovery	12	59

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Change Control (ICT plan to develop improved procedures in the network & infrastructure arena)	Risk based	▪ Adequacy of the procedural documentation in place ▪ System administration and user access. ▪ The processes that ensure that the documentation is kept up to date The processes that ensure compliance with key requirements through development, test and promotion to live.	8	67
Contingency			7	74

5.2 Second Year (2007/2008)

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Internet and Email	Risk based	▪ Provision of access Internet services. ▪ Email & Internet policy. ▪ Policy compliance and monitoring. ▪ Virus prevention strategy and policy ▪ Controls over access to corporate email. ▪ Provision of access to e-mail ▪ E-mail policy ▪ Automated and manual controls over user access, including email and web filtering.	10	10

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Back up Strategy & Procedures (In view of positive comments in ICT Healthcheck. moved back to Year 2).	Key Business Function	▪ See scope for Payroll	6	16
ICT Continuity (emphasis will be ICT not wider Business Continuity)	Risk based	▪ Business continuity strategy at the corporate level. ▪ Links between business continuity and ICT continuity. ▪ Priorities for IT recovery. ▪ IT disaster recovery procedures. ▪ IT disaster recovery testing. ▪ Compliance with the Civil Contingencies Act 2004.	8	24

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Acquisitions and Disposals	Key Business Function	▪ Procurement and disposal Policy. ▪ Links to other strategies and policies. ▪ Compliance with EU and Council regulations. ▪ Selection of aged equipment for replacement. ▪ Ordering and receipt of goods. ▪ Removal of data and software from equipment due for disposal.	6	30

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Payroll/Human Resources (Oracle HRMS)	Fundamental Financial Application	▪ System administration and user access ▪ Incoming interfaces ▪ Control over system parameters ▪ Maintaining data integrity ▪ Configuration documentation ▪ Audit trail ▪ Application recovery	10	40

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Creditors / E-Procurement (OAPS) Need to consider the relationship to the Financial Systems Strategy Review.	Fundamental Financial Application	▪ System administration and user access ▪ Incoming interfaces ▪ Control over system parameters ▪ Maintaining data integrity ▪ Configuration documentation ▪ Audit trail ▪ Application recovery	10	50
Debtors/Debt Recovery (Ash/Solicitec)	Fundamental Financial Application	See scope for Creditors / E-Procurement.	12	62
General Ledger (Flexi)	Fundamental Financial Application	See scope for Creditors / E-Procurement.	10	72
ICT and Network Strategies	Risk-based	• Monitoring • Formation and Coverage	4	76
Contingency			7	83

5.3 Third Year (2008/2009)

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Information Security	Risk based	▪ Formal assessment in relation to the ISO17799 Information Security Management Standard. ▪ Security responsibilities and controls.	8	8
Remote Access	Risk based	▪ Physical and logical security ▪ Configuration ▪ Inventory Control ▪ Security of Laptop Protocol ▪ Data Protection	6	14
E-Payments (In-house system)	Fundamental Financial Application	▪ System administration and user access ▪ Incoming interfaces ▪ Control over system	10	24

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
		parameters ▪ Configuration documentation ▪ Audit trail ▪ Application recovery		
Corporate Web Site, Intranet and Document Management System (Vignette ECM)	Key Business Application	▪ Data Protection responsibilities ▪ Content Management of website and document management system ▪ Data Standards ▪ System administration and user access ▪ Control over system parameters. ▪ Configuration documentation ▪ Audit train ▪ Application recovery ▪	12	36

Name of Audit	Category of Audit (Fundamental Financial Application or Risk-based)	Scope	Days required	Total days to date
Education Management by then should be replaced by a more ≠ Service related system. (EMS)	Key Business Application	See scope for E-Payments	8	44
Database Security	Key Business Application	• There is adequate set up and use of system privileges. • Mechanisms to prevent and detect unauthorised access or internal abuse of data. • Amendment of data to critical tables is adequately monitored. • Configuration of Oracle follows industry standards (including relevant audit logs and system alerts).	12	56
GIS Mapping System	Key Business Application	See scope for E-Payments	10	66

Name of Audit	**Category of Audit (Fundamental Financial Application or Risk-based)**	**Scope**	**Days required**	**Total days to date**
(ArcInfo/MapInfo)				
Property Management (In house system)	Key Business Application	See scope for E-Payments	8	74
ICT and Network Strategies	Risk-based	• Strategic Responsibilities • Links to other Strategies • Monitoring • Formation and Coverage	4	78
Contingency			7	85

Notes.

1. Some financial applications form part of an overall modular package that features shared functionality. Similarly, some applications are directly related to other applications in terms of how data is processed. Where any such relationship applies, the same number for each related application as the order of priority.

2. An Implementation review of the Oracle HRMS was conducted by Price Waterhouse Coopers (PwC) The impact to the council is deemed high priority. The audit order priority has therefore been adjusted to reflect this.

3. Warwickshire County Council hosts and provides a bureau arrangement service to six local Warwickshire local authorities for Payroll as part of a shared Payroll services scheme amongst six Warwickshire councils.

4. Creditors is covered under e-Procurement.

5. Waste Management, Registration Service, Trading Standards Regulatory Service are not included in the IT Audit Plan as they are considered lower priority applications. A decision should be made as to whether these systems warrant auditing along with lower priority risk based audits in the event of additional funding becoming available during the course of the plan.