COPELAND BOROUGH COUNCIL **APPENDIX A**

INFORMATION TECHNOLOGY (IT) AUDIT STRATEGY

1.0 INTRODUCTION

1.1 The Council is highly dependent upon information technology (IT) to deliver services effectively. Internal Audit, therefore, needs to reflect this within its audit plan and have a defined strategy to give assurance that there is a secure IT environment. This was identified as a requirement for full compliance with the CIPFA Code of Practice for Internal Audit in Local Government.

2.0 DEFINING IT AUDIT

2.1 CIPFA guidelines define IT audit as the application of auditing skills to the technological aspects of an organisation's business processes. It embraces the independent reviewing and testing of the organisation's practices and procedures relating to:

- The secure provision of business processing
- The processes for developing and acquiring new systems and facilities
- The economy, efficiency and effectiveness of the use and exploitation of IT facilities.

2.2 It includes the reviewing of:

- The risks of accidental and deliberate threats; the parts of the organisation most vulnerable to such threats; and the impact upon the delivery of services if such threats occurred

- The effectiveness of controls and safeguards and recommending improvements where necessary

- Procedures to determine the extent to which they ensure compliance with relevant standards and legislative requirements for security, health and safety aspects relating to IT facilities used within the organisation

- Procedures for safeguarding access to and use of all computerised data

- the effectiveness, integrity and completeness of controls within computerised applications

- the effectiveness of the procedures for managing and controlling the development of bespoke systems and the adaptation of packaged software

- the arrangements for procuring IT facilities by:

  - verifying the conformance with relevant standards and EC directives

- assessing whether value for money has been sought in the procurement process
- ensuring that high standards of contracting and tendering are adhered to

- the arrangements for the provision of the IT service and the procedures for defining and measuring the IT service delivered.

2.3 It also includes using software and specific computerised audit techniques to provide an effective and efficient audit service.

3.0 IT AUDIT STRATEGY

3.1 The IT Audit Strategy focuses on identifying the audit coverage needed, the skills required to carry out the audits and the timing of the audits, based on a risk assessment.

3.2 The systems-based approach is used to identify, and test compliance with, the key control objectives of the particular computer environment – whether this is a corporately networked system, a stand-alone PC based system or if it involves internet access.

IT Audit Coverage

3.3 IT coverage has been identified in line with the CIPFA Computer Audit Guidelines. There are 3 broad areas to consider:

- the management of IT
- the security of the IT facilities
- the controls relating to each application / software programme which makes use of those facilities.

3.4 In reviewing the overall controls over IT throughout the organisation, internal audit need to consider:

- The standards, controls and procedures which ensure the safe and efficient day-to-day operation of the facilities
- The procedures which the organisation adopts when determining the need for and procurement of IT facilities
- The arrangements made by management to ensure that the facilities are used effectively and efficiently.

All these aspects relate to the administrative and organisational controls that provide the framework for controls governing specific applications e.g. the Council Tax system.

3.5 As far as the specific applications are concerned, internal audit will review:

- The standards and procedures for managing the development / implementation of computerised systems
- The controls which govern the day-to-day processing of each system
- The procedures for changing the application after its initial development or implementation

- The effectiveness of the procedures and of the application itself after it has been implemented.

Staffing Resources Needed

3.6 In order to carry out the above work, internal audit depend upon the co-operation of the IT department for technical information and support. Approximately 10 days internal IT support is needed each year, depending upon audits undertaken. Where the audit requires in depth technical expertise, this will need to be bought in. This has been identified in the detailed IT Audit coverage shown at Appendix A. Based on a review of the technical tests, it is estimated that we would have to buy in around 16 days of specialised computer audit, spread over 3 years, in order to achieve full computer audit coverage. A specification detailing these tests could be used to obtain quotes. Depending upon the results of these computer audits, additional time may be needed for follow ups. After the 3 year cycle, the position would need to be reviewed. Any increase in the level of computer audit, will also increase the demand on the internal IT team, in terms of supplying information and in accompanying the computer auditor on physical inspections of the IT systems.

Risk Assessment

3.7 The risk assessment gives a score for the impact of each IT area –

High	= 3	[Significant financial loss, inability to meet legislative Requirements or serious embarrassment to the Council]
Medium	= 2	[Failure will seriously affect the Service but have limited impact on the overall performance of the Council]
Low	= 1	[Localised or minor impact on the Council's services And performance]

and for the level of existing Control -

Not previously audited	= 5
Poor	= 4
Adequate	= 3
Good	= 2
Excellent	= 1

Impact multiplied by Control = Risk score

Risk Score:	1 to 6 = low risk
	8 to 10 = medium risk
	12 to15 = high risk

3.8 Appendix A shows the detailed audit coverage needed, the risk assessment scores and when the particular IT areas were last audited.

INFORMATION TECHNOLOGY (IT) AUDIT STRATEGY

INFORMATION TECHNOLOGY (IT) AUDIT STRATEGY

APPENDIX A

Risk Area	Audit Area	Impact Score	Control Score	Total Risk Score	Last audited	2006/07 Audit Days	2007/08 Audit Days	2008/09 Audit Days	In-house audit days	Bought-in audit days [estimate]
Security and Control										
	Organisational & Admin Controls / File Controls / Physical & Environmental Controls	3	2	6	2003/04 Follow up - 2005/06			15	12	**3**
	PC controls	2	3	6	2003/04				6	**-**
	Network controls	**3**	**5**	**15**	-	15			9	**5**
	Internet controls	3	2	6	2002/03 Follow ups – 2004/05 & quarterly 2005/06				18	**-**
	E-commerce controls	**3**	**5**	**15**	-		5		5	**3**
	Business Continuity Planning	**3**	**5**	**15**	10 days included in 2005/06 plan	10	10	10	10	**5**

COPELAND BOROUGH COUNCIL **APPENDIX A**

INFORMATION TECHNOLOGY (IT) AUDIT STRATEGY

Risk Area	Audit Area	Impact Score	Control Score	Total Risk Score	Last audited	2006/07 Audit Days	2007/08 Audit Days	2008/09 Audit Days	In-house audit days	Bought-in audit days [estimate]
	Data Protection	3	3	6	2005/06	Covered as part of main systems audits annually				-
Project Management Controls										
	New Financial Management System [2006/07]	**3**	**5**	**15**	-	16			16	-
	Implementation Controls :									-
	- Revenues & Benefits system	**3**	**3**	**9**	2004/05				-	-
	- **Civica E. Payments & Cash Receipting system**	**3**	**5**	**15**	2005/06				10	-
	- MVM – Env. Health, Building Control & Planning	**2**	**5**	**10**	-	15			15	-
	Change Control	**3**	**5**	**15**	-	4	4	4	4	-
	Post implementation review	1	5	5	-	Project team to carry out specific post implementation reviews				-
Applications systems audits										
	Main financial systems audited on an annual basis									-
	Other systems audited on a cyclical basis – See Strategic Audit Plan and Risk Assessment									-
Management Issues										
	IS / IT Strategy	**3**	**5**	**15**	-		6		6	-
	Implementing Electronic Government	**3**	**5**	**15**	2005/06	8	8	8	8	-
	Financial management of IT / Performance monitoring of IT service / recharging for IT	**3**	**5**	**15**	-		8		8	-
	Acquisition of Hardware / software	3	2	6	2004/05 Follow up 2005/06				8	-
Using IT for Audit										
	Data extraction – used on all the main financial feeder systems. Data extracted by in-house IT staff / system									-

COPELAND BOROUGH COUNCIL **APPENDIX A**

INFORMATION TECHNOLOGY (IT) AUDIT STRATEGY

Risk Area	Audit Area	Impact Score	Control Score	Total Risk Score	Last audited	2006/07 Audit Days	2007/08 Audit Days	2008/09 Audit Days	In-house audit days	Bought-in audit days [estimate]
	administrators . Estimated 10 days work each year.									
	Use of audit software to manipulate / test data extracted. Incorporated in main financial systems audits – see Audit Plan.									-