

## REPORT OF THE CHIEF FIRE OFFICER

# INTERNAL AND EXTERNAL AUDITS: DATA, INFORMATION TECHNOLOGY AND COMMUNICATIONS

### 1 Background

Members are requested to note the developments that have taken place in reinforcing the Service's policies and procedures to secure further improvements in the management of data, information technology and communications.

### 2 Recommendations

Members are requested to note the contents of this report.

### 3 Background

The Authority has, in recent years, been subjected to a variety of audits, some of which have reviewed the Service's policies and procedures for management of data, information, technology and communications. At the Committee's previous meeting officers informed Members of the findings of the 2005/06 Internal Audit that had identified eleven recommendations relating to information technology and eight relating to data protection (see Appendix A).

More recently, the Audit Commission has requested that the Authority complete a Data Quality Review exercise (see Appendix B).

This report sets out progress in meeting the recommendations and requirements of the aforesaid appraisals.

### 4 Actions to Date

Since receipt of the Internal Audit report, and the more recent Data Quality Review, significant progress has been made in evaluating, adjusting and, where necessary, developing new procedures and practices to enhance the Service's management of data, information technology and communications. The timing of the audit and review has been opportune and has created the impetus to review a broad range of disparate policy documents that had over the years been developed in isolation.



Documented policy (initially created in 2001) has lagged behind the rapid expansion of information technology and communications systems. It is a widely recognised fact that the Fire Authority's commitment to furnishing the Service with modern and cutting-edge technology has placed Shropshire at the forefront of resilient operational communications and command technology. However, in addressing priorities to secure improvements in core service delivery areas, it is acknowledged that insufficient emphasis has been placed upon the development and maintenance of management policy.

With the increasing proliferation of electronic data, information technology and communications systems across the entire organisation, both manual and technical, the need has arisen to produce a revised policy and strategy in one single point of reference. This has resulted in the development of what will undoubtedly be one of the organisation's key strategic policies recorded within a revised Brigade Order. The Order will be accompanied by the production and distribution of a pragmatic user handbook, issued to all Members and staff alike.

## **5 Brigade Order 16 on Data, Information Technology and Communications Strategy**

The central point of reference for policy, strategy and the management of data, information technology and communications will be Brigade Order 16. The Order comprises of six parts and sets out a clear and coherent strategy, pulling together previously unrelated policies. Appendix C of this paper presents the table of contents of Brigade Order 16. A full copy of the draft Order, which has been circulated for consultation to internal stakeholder groups, is available on request.

## **6 Information, Technology, Communications and Data User Handbook**

Whilst Brigade Order 16 will act as the central point of reference for policy, strategy and the management of data, information technology and communications, a pragmatic summary user handbook has been prepared to promote greater awareness and understanding of Authority policy. The Handbook (see Appendix D for table of contents) will provide a useful, yet simplified, guidance document that will be issued on a personal basis to Members and staff. The draft Handbook has also been circulated for consultation to internal stakeholder groups.

## **7 Internal Audit – 2005/06**

Internal Audit identified eleven recommendations relating to information technology and eight relating to data protection. All of the recommendations raised have now been addressed, albeit some actions undertaken now form part of a larger improvement programme. Appendix E to this report provides summary evidence of the actions undertaken.

## **8 Audit Commission Data Quality Review**

The Audit Commission Data Quality Review exercise has required the submission of a Data Quality Self-Assessment (submitted on 18 August 2006). A copy of the submitted assessment is attached (see Appendix F). The Commission's Review document identifies a comprehensive range of data quality criteria, which, if met in full, would create an environment of excellence in terms of governance, process and procedure.



Actions, primarily documented within Brigade Order 16, have been instigated to begin a controlled step-change approach towards the organisation's management of data, together with that of information technology and communications. This process will require both cultural and corporate change to achieve a position of excellence. Officers will present periodic reports to the Committee on progress achieved.

Details of the Commission's review of the Authority's data quality arrangements will be brought before the Committee, when available.

## 9 Financial Implications

Apart from the consequences of dealing with automatic fire extinguishing systems for the Information Technology server room, there are no direct financial implications arising from this report.

## 10 Legal Comment

There are no legal implications arising directly from this report.

## 11 Appendices

- Appendix A** Internal Audit Report 2005-2006
- Appendix B** Audit Commission Data Quality Review (May 2006)
- Appendix C** Brigade Order 16: Table of Contents
- Appendix D** Information Technology, Communications and Data User Handbook: Table of Contents
- Appendix E** Actions in respect of Internal Audit Report (August 2006)
- Appendix F** Audit Commission Data Quality Self-Assessment (August 2006)

## 12 Background Papers

Shropshire and Wrekin Fire Authority Audit and Performance Management Committee 15 June 2006 report 9 - Internal Audit 2005/06 Summary Audit Report

Implications of all of the following have been considered and, where they are significant (i.e. marked with an asterisk), the implications are detailed within the report itself.

Balance Score Card		Integrated Risk Management Planning	
Business Continuity Planning		Legal	
Capacity	*	Member Involvement	*
Civil Contingencies Act		National Framework	*
Comprehensive Performance Assessment	*	Operational Assurance	*
Equality and Diversity		Retained	
Efficiency Savings		Risk and Insurance	*
Environmental		Staff	
Financial	*	Strategic Planning	*
Fire Control/Fire Link		West Midlands Regional Management Board	

For further information about this report please contact Alan Taylor, Chief Fire Officer, on 01743 260201 or Steve Worrall, Assistant Chief Fire Officer, on 01743 260204.



## **INTERNAL AUDIT RECOMMENDATIONS**

### **1. IT Installation**

- i. The IT strategy should be finalised and approved as soon as possible. (Requires attention)
- ii. Management should ensure that all staff are aware of the security incident procedure and implement a formal process to record and escalate incidents as appropriate. (Requires attention)
- iii. The draft network access request form should be finalised (Requires attention)
- iv. A formal process of notifying IT of staff leavers should be implemented to ensure that access for staff leaving the authority is removed promptly (Requires attention)
- v. A process should be defined to ensure that leavers have deleted all personal information from their mailbox, computer and network drive prior to leaving the authority. (Requires attention)
- vi. Formal guidance should be written to ensure that staff are aware of their responsibilities for securing the equipment and information contained on it. (Requires attention)
- vii. IT should be involved in the full procurement cycle and not just the specification stage. (Requires attention)
- viii. The authority should consider the advantages of installing an automatic fire extinguishing system in the server room. (Significant)
- ix. The back up tapes should be stored in a secure off-site location. (Significant)
- x. The Authority should produce a business continuity plan (BCP) as a matter of urgency as this is a significant area of risk. The plan should identify the criticality of key systems and the timeframes by which these should be available in the event of an incident and address this need with the necessary arrangements. (Significant)
- xi. A formal procedure should be implemented for recording all software installations, movements and disposals. (Requires attention)

### **2. Data Protection Act 1998**

- i. Improve communications to staff of the Data Protection Policy Handbook, awareness material and training packages. (Requires attention)
- ii. Introduce data protection information into employment terms and conditions and into job descriptions. (Requires attention)



- iii. Checks should be undertaken to establish if information is being processed in accordance with the authority's data protection policy and online privacy policy. (Requires attention)
- iv. Produce relevant procedures for staff in relation to updating and amending data where it is duplicated or held separately. (Requires attention)
- v. Develop procedures for monitoring data protection compliance on a periodic basis. (Requires attention)
- vi. Introduce a mechanism for addressing data protection issues. (Requires attention)
- vii. Introduce a procedure/system for recording details of requests made, how they were processed and what information was provided and/or withheld. (Requires attention)
- viii. Define retention periods for information sets and communicate this to staff. (Requires attention)



May 2006

Appendix B to report on  
Internal and External Audits : Data,  
Information Technology and Communications  
Shropshire and Wrekin Fire Authority  
Audit and Performance Management Committee  
7 September 2006

# **Data quality reviews (local government) - management arrangements**

**Checklist for small bodies**

May 2006

The Audit Commission is an independent body responsible for ensuring that public money is spent economically, efficiently and effectively, to achieve high-quality local and national services for the public. Our remit covers more than 15,000 bodies which between them spend nearly £125 billion of public money every year. Our work covers local government, housing, health, criminal justice and fire and rescue services.

As an independent watchdog, we provide important information on the quality of public services. As a driving force for improvement in those services, we provide practical recommendations and spread best practice. As an independent auditor, we monitor spending to ensure public services are good value for money.

<b>Document Control</b>	
Author	
Filename	DQ Checklist for smaller authorities

## Contents

<b>Introduction</b>	<b>4</b>
This checklist	4
Objectives	4
Scope	4
Audit approach	4
Resources and timescale	5
Quality control	5
Reporting	5
Auditor support	6
<b>Appendix 1 – Checklist for reviewing management arrangements for data quality at smaller bodies</b>	<b>7</b>



# Introduction

## This checklist

- 1 The purpose of this checklist is to provide a summarised approach for auditors in assessing the corporate management arrangements for data quality in smaller local government bodies. The checklist is based on stage 1 of the Commission's approach to the review of data quality at single tier, county councils and district councils. The stage 1 audit guidance is available on Acorn and provides further detail on the principles and good practice underpinning the review approach.
- 2 The annual planning guidance and relevant supplementary guidance sets out the extent to which auditors should apply the approach. Appointed auditors should refer to such guidance before proceeding with any work on data quality.

## Objectives

- 3 The objective of this work is to determine whether proper corporate management arrangements for data quality are in place. The findings will contribute to the auditor's conclusion under the Code of Audit Practice on an audited body's arrangements to secure value for money. The work relates specifically to the arrangements for 'monitoring and reviewing performance, including arrangements to ensure data quality'<sup>1</sup>.
- 4 The purpose of the work on management arrangements is to focus on the corporate data quality arrangements for the performance information prepared and used by the authority. The focus of the work is not to examine individual or departmental systems for producing specific performance indicators, nor to assess the accuracy of recording for individual indicators.

## Scope

- 5 This checklist approach may be used at local government bodies which are not subject to a CPA use of resources assessment. The checklist should **not** be used at single tier, county councils, district councils or police authorities.

## Audit approach

- 6 Using the checklist at Appendix 1, the auditor should reach a conclusion on the adequacy of the corporate management arrangements for data quality at the audited and inspected body, based on evidence obtained from the following sources:

---

<sup>1</sup> Code of Audit Practice 2005, section 3: Auditors' responsibilities in relation to the use of resources

- current knowledge of the body and its arrangements, including the results of previous work and reviews of performance indicators (CAKE)
  - a brief discussion with a relevant key contact at the audited body
- 7 Auditors are not required to answer every question on the checklist, but should use their judgement to determine which questions are of most importance, within the time available for this work.
- 8 For the purposes of the Code conclusion on value for money, auditors are required to make a 'yes/no' assessment in relation to the Code criterion on data quality ("The body has put in place arrangements to monitor the quality of its published performance information, and to report the results to members").
- 9 The checklist contains examples of what are considered to be adequate arrangements for data quality. If all, or the majority, of questions on the checklist have been answered positively, this may lead auditors to conclude, for the purposes of the VFM conclusion, that the body has proper arrangements in place.

## Resources and timescale

- 10 Resource estimates are set out in the planning guidance. As a guideline, it is expected this checklist should take one day to complete.
- 11 Work must be completed at a time which will allow for the timely completion of the VFM conclusion alongside the opinion on the accounts.

## Quality control

- 12 You must ensure that all work is subject to quality control. This includes ensuring:
- the timely completion of the work; and
  - that internal quality control processes are applied to assessments to ensure:
    - assessments are robust and supported by sufficient evidence;
    - judgements are consistent;
    - where applicable, reports arising from this work comply with the requirements set out in the auditor briefing on audit reporting (AB4/2006 Reporting by Auditors (LG Code), including the Commission's report writing guidance.

## Reporting

- 13 The results of the review will inform the Code conclusion on value for money, which is reported in the audit report, with any significant issues being highlighted in the report to those charged with governance.

## **Auditor support**

- 14** Auditor queries arising during the course of the reviews may be referred to the Audit Commission Technical Support Service (ACTS) for resolution. Queries should be e-mailed to [ACTS@audit-commission.gov.uk](mailto:ACTS@audit-commission.gov.uk). Your email should include details of actions you have already taken to resolve the query. All queries will be logged and monitored.

## Appendix 1 – Checklist for reviewing management arrangements for data quality at smaller bodies

Indicator of adequate data quality management arrangements	Adequate arrangements in place?
<b>Governance and leadership</b>	
Responsibility for data quality has been assigned within the organisation.	
The organisation's commitment to data quality (for example, the importance of, and arrangements for, securing the quality of key data) is outlined in key strategic documents, such as the corporate plan.	
Objectives for data quality management are developing, but may not yet be formalised in a strategy or plan.	
The organisation is working to improve data quality, but may not yet have defined milestones, targets or monitoring.	
Monitoring and review of data quality has been undertaken, although this may have been primarily on an ad hoc basis.	
Reports are produced as a result of these reviews, which are submitted for top management attention.	
The organisation has begun to consider data quality as part of its corporate risk management arrangements.	
The organisation can demonstrate that it has taken action to address the results of internal and external data quality reviews.	
<b>Policies and procedures</b>	
A data quality policy, or set of policies, is in place at the operational level. The policies have been designed to support the data quality objectives.	

<b>Indicator of adequate data quality management arrangements</b>	<b>Adequate arrangements in place?</b>
The data quality policy has been approved by senior management at least at a departmental level.	
There are a number of procedures and guidance notes in place, although these may not yet cover all aspects of data collection, recording, analysis and reporting, or may not be in place in all business areas.	
All relevant staff are aware of the data quality policy, operational procedures and guidance and have access to the documents.	
<b>Systems and processes</b>	
There may be some minor weaknesses in the systems for data collection, recording, analysis and reporting of performance information, but action is being taken to address these.	
The organisation recognises the importance of these systems, whether manual or computerised, operating on a 'right first time' principle. Some work may be needed to achieve this.	
Support for staff using these systems is provided, but it may be that improvements could be made (for example by making support more accessible or responsive).	
Any internal or external reviews of the systems have not identified significant weaknesses.	
Appropriate controls are in place for both manual and computerised systems, particularly where there is a dependency on spreadsheet systems.	
The organisation has some arrangements in place to review the effectiveness of controls.	
High-level reviews of data are carried out before reporting to directorate management and beyond, but this might not be consistent across the organisation.	
Security arrangements, including access control, are in place for the organisation's business critical performance information systems.	
There are procedure notes/manuals in place for the organisation's business critical performance information systems.	

<b>Indicator of adequate data quality management arrangements</b>	<b>Adequate arrangements in place?</b>
A business continuity plan is in place to provide protection for records and performance data which are vital to the continued effective functioning of the organisation.	
All instances of internal and external data sharing have been identified, but formal protocols may yet to have been developed.	
There is a framework in place for identifying and complying with all relevant legal, compliance and confidentiality standards.	
<b>People and skills</b>	
The organisation has undertaken an assessment of the data quality skills that it has in place across the workforce and identified potential gaps.	
Staff are clear about their responsibilities in relation to data quality.	
Staff with specific responsibilities for data input or data quality have received data quality training.	
There is evidence of review of the current data quality training provision but this has yet to be developed corporately.	
Some departments are addressing weaknesses identified from data quality reviews through training but this may still need to be developed corporately.	
<b>Data use</b>	
Reported data is fed back to those who generate it to reinforce understanding of the way it is used.	
Performance information is regularly used, to identify deviations from planned performance.	
There is timely action on performance shortfalls, and follow-up to ensure action has been taken.	
Definitions are generally applied correctly to all data items.	

<b>Indicator of adequate data quality management arrangements</b>	<b>Adequate arrangements in place?</b>
All data returns are supported by an audit trail, although there may be some weaknesses.	
There is evidence that controls are exercised over data to verify its accuracy.	
Reported data is generally submitted on a timely basis. Instances of data not being submitted on a timely basis are fully investigated and reported to management.	



# SHROPSHIRE

## Fire and Rescue Service

<b><u>CONTENTS</u></b>		<b>Page No</b>
<b>PART 1</b>	<b>TECHNOLOGY &amp; COMMUNICATIONS STRATEGY</b>	<b>BRIGADE ORDER ADMINISTRATION NO. 16</b>
<b>PART 2</b>	<b>SECURITY POLICY (INCLUDING AIRWAVE)</b>	
<b>PART 3</b>	<b>STANDARDS AND PROCEDURES</b>	<b>ADMINISTRATION</b>
<b>PART 4</b>	<b>INFORMATION MANAGEMENT STRATEGY</b>	
<b>PART 5</b>	<b>LEGISLATION, DEFINITIONS AND ACRONYMS</b>	
<b>PART 6</b>	<b>HANDBOOK</b>	<b>No 16</b>
		<b>INFORMATION COMMUNICATIONS TECHNOLOGY</b>







# SHROPSHIRE

## Fire and Rescue Service

<b><u>CONTENTS</u></b>	<b>Page No</b>
<b>PURPOSE</b>	
<b>STRATEGIC AIMS AND OBJECTIVES</b>	
<b>ROLES, RESPONSIBILITIES AND REVIEW</b>	
<b>INTRODUCTION</b>	
<b>PRIMARY POINTS</b>	
<b>PLANNING AND FUNDING ISSUES</b>	
<b>ACCESS AND USEABILITY</b>	
<b>STAFF FACILITIES</b>	
<b>SECURITY ISSUES</b>	
<b>ENERGY AND RESOURCE SAVING</b>	
<b>TEACHING AND PRESENTATIONS</b>	
<b>TRAINING</b>	
<b>APPENDIX A: CURRENT IT PROVISION IN THE BRIGADE</b>	
	<b>BRIGADE ORDER ADMINISTRATION NO. 16</b>
	<b>ADMINISTRATION</b>
	<b>PART 1</b>
	<b>TECHNOLOGY &amp; COMMUNICATIONS STRATEGY</b>





# SHROPSHIRE Fire and Rescue Service

<b><u>CONTENTS</u></b>	<b>Page No</b>
<b>PURPOSE</b>	<b>BRIGADE ORDER ADMINISTRATION NO. 16</b>
<b>STRATEGIC AIMS AND OBJECTIVES</b>	
<b>ROLES, RESPONSIBILITIES AND REVIEW</b>	
<b>INTRODUCTION</b>	<b>ADMINISTRATION</b>
<b>PURPOSE</b>	
<b>SCOPE</b>	
<b>RESPONSIBILITY</b>	
<b>POLICY GUIDELINES</b>	
<b>LEGISLATION</b>	<b>PART 2</b>
<b>USER REQUIREMENTS</b>	
<b>SOFTWARE</b>	
<b>HARDWARE</b>	
<b>INTERNET AND EMAIL</b>	
<b>BRIGADE RADIO (AIRWAVE)</b>	
<b>APPENDIX A: TEA2 LICENCE</b>	
<b>APPENDIX B: TERMINAL LOSS REPORTING FORM</b>	<b>SECURITY POLICY</b>





# SHROPSHIRE Fire and Rescue Service

<b><u>CONTENTS</u></b>	<b>Page No</b>
<b>PURPOSE</b>	
<b>STRATEGIC AIMS AND OBJECTIVES</b>	
<b>ROLES, RESPONSIBILITIES AND REVIEW</b>	
<b>DATA PROTECTION, FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS PROCEDURES</b>	
<b>REPORTING SECURITY ISSUES</b>	
<b>SECURING OFFICES, ROOMS AND FACILITIES</b>	
<b>SECURITY OF EQUIPMENT OFF- PREMISES</b>	
<b>CONTROL OF OPERATIONAL SOFTWARE POLICY AND CHANGE CONTROL POLICY</b>	
<b>REMOVAL OF USER ACCESS RIGHTS</b>	
<b>IT PURCHASING</b>	
<b>MANAGEMENT OF REMOVABLE MEDIA</b>	
<b>BUSINESS CONTINUITY PLANNING</b>	
<b>APPENDIX A: SECURITY INCIDENT/ WEAKNESS PRO- FORMA</b>	
<b>APPENDIX B: NETWORK ACCESS FORMS</b>	
<b>APPENDIX C: TERMINAL LOSS REPORTING FORM</b>	
	<b>BRIGADE ORDER ADMINISTRATION NO. 16</b>
	<b>ADMINISTRATION</b>
	<b>PART 3</b>
	<b>STANDARDS AND PROCEDURES</b>





# SHROPSHIRE

## Fire and Rescue Service

<b><u>CONTENTS</u></b>	<b>Page No</b>
<b>PURPOSE</b>	
<b>STRATEGIC AIMS AND OBJECTIVES</b>	
<b>ROLES, RESPONSIBILITIES AND REVIEW</b>	
<b>INTRODUCTION</b>	
<b>MANAGEMENT RESPONSIBILITY</b>	
<b>OBJECTIVES</b>	
<b>QUALITY SYSTEM OVERVIEW</b>	
<b>DOCUMENT CONTROL</b>	
<b>SUPPORT</b>	
<b>TRAINING</b>	
<b>CONTINUAL IMPROVEMENT</b>	
<b>APPENDIX A: MILESTONES</b>	
	<b>BRIGADE ORDER ADMINISTRATION NO. 16</b>
	<b>ADMINISTRATION</b>
	<b>PART 4</b>
	<b>INFORMATION MANAGEMENT STRATEGY</b>





# SHROPSHIRE

## Fire and Rescue Service

<b><u>CONTENTS</u></b>	<b>Page No</b>
<b>PURPOSE</b>	
<b>STRATEGIC AIMS AND OBJECTIVES</b>	
<b>ROLES, RESPONSIBILITIES AND REVIEW</b>	
<b>DATA PROTECTION ACT 1998</b>	
<b>FREEDOM OF INFORMATION ACT 2000</b>	
<b>ENVIRONMENTAL INFORMATION REGULATIONS 2005</b>	
<b>HEALTH AND SAFETY AT WORK ACT 1992</b>	
<b>COPYRIGHT, DESIGNS AND PATENTS ACT 1988</b>	
<b>COMPUTER MISUSE ACT 1990</b>	
<b>OBSCENE PUBLICATIONS ACT 1964</b>	
<b>CRIMINAL JUSTICE AND PUBLIC ORDER 1994</b>	
<b>TELECOMMUNICATIONS ACT 1984</b>	
<b>PROTECTION OF CHILDREN ACT 1978</b>	
<b>APPENDIX A: LIST OF DEFINITIONS</b>	
<b>APPENDIX B: LIST OF ACRONYMS</b>	
<b>APPENDIX C: REQUEST FOR DATA ACCESS PROFORMA</b>	
	<b>BRIGADE ORDER ADMINISTRATION NO. 16</b>
	<b>ADMINISTRATION</b>
	<b>PART 5</b>
	<b>LEGISLATION, DEFINITIONS &amp; ACRONYMS</b>



# Information Technology, Communications and Data User Handbook

## CONTENTS:

### 1 TECHNOLOGY AND COMMUNICATIONS STRATEGY

- Introduction
- Primary Points
- Planning and Funding Issues
- Access and Usability
- Staff Facilities
- Security Issues
- Energy and Resource Saving
- Teaching and Presentations
- Training
- Current IT provision in the Brigade

### 2 SECURITY POLICY

- Legislation
- User Requirements Policy
- Software Policy
- Hardware Policy
- Internet and Email Policy
- Airwave Policy

### 3 STANDARDS AND PROCEDURES

- Reporting Security Issues
- Securing Offices, Rooms and Facilities
- Security of Equipment Off-Premises
- Control of Operation Software Policy and Change Control Policy
- Removal of User Access Rights
- IT Purchasing
- Management of Removable Media
- Business Contingency Planning

### 4 INFORMATION MANAGEMENT STRATEGY

- Introduction
- Management Responsibility
- Objectives
- Quality System Overview



Document Control  
Support  
Training  
Continual Improvement

## **5 LEGISLATION, DEFINITIONS AND ACRONYMS**

Data Protection Act 1998  
Freedom of Information Act 2000  
Environmental Information Regulations 2005  
Health and Safety at Work Act 1992  
Copyright, Designs and Patents Act 1988  
Computer Misuse Act 1990  
Obscene Publications Act 1964  
Criminal Justice and Public Order Act 1994  
Telecommunications Act 1984  
Protection of Children Act 1978  
List of Definitions  
List of Acronyms

## **EMPLOYEE AGREEMENT – ICT USAGE POLICY**



Internal Audit Statement/Comment	Adequate arrangements now in place? (Y – Yes / N - No)	Level of Provision (FLPN) <sup>1</sup>	Evidence
<b>SCC Audit 2005/06</b>			
1. The IT strategy should be finalised and approved as soon as possible. (Requires attention)	Y	L	IT Strategy is now consolidated within Brigade Order 16. The Order is currently in the process of consultation with internal stakeholders.
2. Management should ensure that all staff are aware of the security incident procedure and implement a formal process to record and escalate incidents as appropriate. (Requires attention)	Y	L	The security policy is now fully documented within Brigade Order 16 Part 2. Staff awareness is to be raised through the ITCD User Handbook.
3. The draft network access request form should be finalised (Requires attention)	Y	L	The network access policy is now fully documented within Brigade Order 16 Part 3. Staff awareness is to be raised through the ITCD User Handbook.
4. A formal process of notifying IT of staff leavers should be implemented to ensure that access for staff leaving the authority is removed promptly (Requires attention)	Y	L	The IT authorised user policy is now fully documented within Brigade Order 16 Part 3. Staff awareness is to be raised through the ITCD User Handbook.

<sup>1</sup> Note:

**F** – Arrangements are **FULLY** in place and have been reviewed

**L** – Arrangements are **LARGELY** in place but have not been reviewed

**P** – Arrangements are only **PARTIALLY** in place and are still being implemented

**N** – **NO** action has yet been taken





5. A process should be defined to ensure that leavers have deleted all personal information from their mailbox, computer and network drive prior to leaving the authority. (Requires attention)	Y	L	The IT authorised user policy is now fully documented within Brigade Order 16 Part 3. Staff awareness is to be raised through the ITCD User Handbook.
6. Formal guidance should be written to ensure that staff are aware of their responsibilities for securing the equipment and information contained on IT. (Requires attention)	Y	L	The user policy for securing information and equipment is now fully documented within Brigade Order 16 Part 3. Staff awareness is to be raised through the ITCD User Handbook.
7. IT should be involved in the full procurement cycle and not just the specification stage. (Requires attention)	Y	L	The role of the ITC Dept in IT procurement is now fully documented within Brigade Order 16 Part 1.
8. The authority should consider the advantages of installing an automatic fire extinguishing system in the server room. <b>(Significant)</b>	Y	F	A number of options have been considered. These range from £8-9k, to provide a chemical system to the equipment room only, to £25-35k, to provide an inert gas system to the equipment, UPS and generator rooms, including provision of fire dampers to the generator air intake and exhaust vents. Formal quotations received are being considered as part of a broader business continuity strategy that gives consideration to the implementation of a duplicate off-site server room for greater resilience.
9. The back up tapes should be stored in a secure off-site location. <b>(Significant)</b>	Y	F	Back-up tapes/discs are now stored in a fire-proof secure safe located away from the Brigade's HQ building.



10. The Authority should produce a business continuity plan (BCP) as a matter of urgency as this is a significant area of risk. The plan should identify the criticality of key systems and the timeframes by which these should be available in the event of an incident and address this need with the necessary arrangements. <b>(Significant)</b>	Y	L	A business continuity plan has been completed. Contingency options to mitigate significant risk are being considered. An option currently being evaluated will involve the establishment of a fall-back control room and duplicate server room at Telford Central Fire Station.
11. A formal procedure should be implemented for recording all software installations, movements and disposals. (Requires attention)	Y	L	A formal procedure recording all software installations, movements and disposals is now fully documented within Brigade Order 16; Part 3. Staff awareness is to be raised through the ITCD User Handbook.
<b>Data Protection Act 1998</b>			
1. Improve communications to staff of the Data Protection Policy Handbook, awareness material and training packages. (Requires attention)	Y	L	Data protection policy is now fully documented within Brigade Order 16 Part 5. Staff awareness is to be raised through the ITCD User Handbook.
2. Introduce data protection information into employment terms and conditions and into job descriptions. (Requires attention)	Y	L	Data protection information has now been introduced into employment terms and conditions and into job descriptions. This is further reinforced within the ITCD User Handbook.
3. Checks should be undertaken to establish if information is being processed in accordance with the authority's data protection policy and online privacy policy. (Requires attention)	Y	P	A review of information processing has taken place and a new procedure introduced to streamline processes in accordance with the Authority's revised data protection and online privacy policies. These arrangements are set out within Brigade Order 16 Part 3 and will be reinforced through the new ITCD User Handbook.



4. Produce relevant procedures for staff in relation to updating and amending data where it is duplicated or held separately. (Requires attention)	Y	P	Procedures for staff in relation to updating and amending data etc are now documented within Brigade Order 16 Part 3. Staff awareness is to be raised through the ITCD User Handbook. In addition, a detailed data process mapping exercise is currently underway.
5. Develop procedures for monitoring data protection compliance on a periodic basis. (Requires attention)	Y	L	Procedures for procedures for monitoring data protection compliance on a periodic basis are now documented within Brigade Order 16 Part 4.
6. Introduce a mechanism for addressing data protection issues. (Requires attention)	Y	L	A mechanism for addressing data protection issues is documented within Brigade Order 16 Part 3. Staff awareness of the new mechanism will be raised through the ITCD User Handbook.
7. Introduce a procedure/system for recording details of requests made, how they were processed and what information was provided and/or withheld. (Requires attention)	Y	L	A new procedure for recording details of requests made, how they were processed and what information is provided and/or withheld has been introduced. The procedure is documented within Brigade Order 16 Part 3. Staff awareness of the new mechanism will be raised through the ITCD User Handbook.
8. Define retention periods for information sets and communicate this to staff. (Requires attention)	Y	L	A procedure that defines retention periods for information sets is documented within Brigade Order 16 Part 5. Staff awareness of the new procedure will be raised through the ITCD User Handbook.



Audit Commission Data Quality Review (Indicator of adequate data quality management arrangements)	Adequate arrangements in place (Y/N)	Level of Provision (FLPN) <sup>2</sup>	Evidence
<b>Governance and leadership</b>			
Responsibility for data quality has been assigned within the organisation.	Y	L	Brigade Order 16 Part 4. Responsibility has been assigned corporately and is assessed departmentally through the process mapping exercise.
The organisation's commitment to data quality (for example, the importance of, and arrangements for, securing the quality of key data) is outlined in key strategic documents, such as the corporate plan.	Y	L	Brigade Order 16 Part 4. Performance Plan 2006 - 08 pages 13, 16, and 27. The Fire and Rescue National Framework page 68.
Objectives for data quality management are developing, but may not yet be formalised in a strategy or plan.	Y	L	Objectives for the Fire and Rescue Service are set within the National Framework. Brigade Order 16 Part 4 sets out the activities to deliver these objectives.

<sup>2</sup> Note:

**F** – Arrangements are **FULLY** in place and have been reviewed

**L** – Arrangements are **LARGELY** in place but have not been reviewed

**P** – Arrangements are only **PARTIALLY** in place and are still being implemented

**N** – **NO** action has yet been taken



The organisation is working to improve data quality, but may not yet have defined milestones, targets or monitoring.	Y	L	Objectives for the Fire and Rescue Service are set within the National Framework. Brigade Order 16 Part 4 sets out the activities, milestones and monitoring arrangements. Tender process for Management Information System (MIS) and Performance Management System (PMS)
Monitoring and review of data quality has been undertaken, although this may have been primarily on an ad hoc basis.	Y	P	The review policy is set out in Brigade Order 16 Part 4. Performance Indicator collation process incorporates a data integrity check.
Reports are produced as a result of these reviews, which are submitted for top management attention.	Y	P	Brigade Order 16 Part 4 stipulates policy, reviews to be submitted.
The organisation has begun to consider data quality as part of its corporate risk management arrangements.	Y	L	Is considered as part of the organisation's risk management arrangements.
The organisation can demonstrate that it has taken action to address the results of internal and external data quality reviews.	Y	L	Internal review undertaken in Aug 2005. Shropshire County Council Audit and Consultancy – Shropshire Fire and Rescue Service Audit Report 2004/05 Recommendation follow-up 2005/06, results reported to Audit & Performance Management Committee (A&PMC). Up until the 2004/05 reporting year the Department of Communities & Local Government (DCLG) sampled 20% of all Fire Damage Report 1 (FDR1) forms submitted and will be increasing this percentage in the future.



<b>Policies and procedures</b>			
A data quality policy, or set of policies, is in place at the operational level. The policies have been designed to support the data quality objectives.	Y	L	Brigade Order 16 Part 6 (ITCD Handbook)
The data quality policy has been approved by senior management at least at a departmental level.	Y	L	Brigade Order 16, originally issued 08/01, recently subjected to strategic review currently undergoing formal consultation prior to reissue with accompanying ITCD User Handbook.
There are a number of procedures and guidance notes in place, although these may not yet cover all aspects of data collection, recording, analysis and reporting, or may not be in place in all business areas.	Y	L	Brigade Order 16 procedures and guidance and accompanying handbook.
All relevant staff are aware of the data quality policy, operational procedures and guidance and have access to the documents.	Y	L	Brigade Order 16 procedures and guidance and accompanying handbook (personnel are requested to acknowledge awareness of handbook), The Pink, Terms of Reference of the <b>TecCom</b> - the <b>Technology Steering Committee</b> for Electronic Data, Information Technology and Communications. (formerly Information Strategy User Group - ISUG).
<b>Systems and processes</b>			
There may be some minor weaknesses in the systems for data collection, recording, analysis and reporting of performance information, but action is being taken to address these.	Y	L	Strategic review undertaken in Aug 2005. Systems mapping is being undertaken within the Brigade - Brigade Order 16 Part 4.



The organisation recognises the importance of these systems, whether manual or computerised, operating on a 'right first time' principle. Some work may be needed to achieve this.	Y	L	Brigade Order 16 Part 4 and 6
Support for staff using these systems is provided, but it may be that improvements could be made (for example by making support more accessible or responsive).	Y	P	ISUG in place since 2003, group recently restructured (TecCom) to provide a greater focus on data quality. Departmental Manual for systems under development.
Quarterly Performance Monitoring report to Policy Group and Audit and Performance Management Committee.	N	F	Strategic Review undertaken in Aug 2005 and has led to an improvement programme being implemented. The MIS and PMS tender exercise is currently ongoing.
Quarterly Performance Monitoring report to Policy Group and Audit and Performance Management Committee.	Y	P	Strategic Review undertaken in Aug 2005 and has led to an improvement programme being implemented. Brigade Order 16 Part 4. Controls are in place for manual scrutiny key data processes (FDR1, BVPI's).
Quarterly Performance Monitoring report to Policy Group and Audit and Performance Management Committee.	Y	L	Brigade Order 16 Part 4 sets out proposed new arrangements which will be reviewed on completion of the process mapping exercise.
Quarterly Performance Monitoring report to Policy Group and Audit and Performance Management Committee.	Y	L	Reporting to Policy Group on a quarterly basis, prior to A&PMC. Senior Management are consulted prior to this.



Security arrangements, including access control, are in place for the organisation's business critical performance information systems.	Y	F	Brigade Order 16 Part 2. Staff awareness is to be raised though the ITCD User Handbook.
There are procedure notes/manuals in place for the organisation's business critical performance information systems.	Y	P	Procedural guidance in place for Performance reporting system. Complete Brigade wide manuals for all systems under development.
A business continuity plan is in place to provide protection for records and performance data which are vital to the continued effective functioning of the organisation.	Y	F	Brigade Order 16 Part 3. Back-up tapes/discs are stored off-site in a fire-proof secure safe.
All instances of internal and external data sharing have been identified, but formal protocols may yet to have been developed.	Y	P	Data Sharing has been identified as part of the Brigade Partnership process and risk assessed accordingly. Brigade Order 5 Part 1. Strategic Review undertaken in Aug 2005 and has led to an improvement programme (process mapping) being implemented to identify all internal and external data sharing.
There is a framework in place for identifying and complying with all relevant legal, compliance and confidentiality standards.	Y	F	Brigade order 16 Part 5.
<b>People and skills</b>			
The organisation has undertaken an assessment of the data quality skills that it has in place across the workforce and identified potential gaps.	Y	P	The organisation is currently undertaking a process mapping exercise, which will include a skills gap analysis. Personal Development and Achievement Review (PDAR) process.





Staff are clear about their responsibilities in relation to data quality.	Y	L	Brigade Order 16 Part 4 and 6 (personnel are requested to acknowledge awareness of handbook).
Staff with specific responsibilities for data input or data quality have received data quality training.	N	P	The organisation is currently undertaking a process mapping exercise which will include a skills gap analysis which will lead to targeted data quality training.
There is evidence of review of the current data quality training provision but this has yet to be developed corporately.	N	P	The organisation is currently undertaking a process mapping exercise which will include a skills gap analysis which will lead to targeted data quality training.
Some departments are addressing weaknesses identified from data quality reviews through training but this may still need to be developed corporately.	Y	L	The PDAR process is in place to address any identified training needs. Corporately this will be further underpinned through the process mapping exercise.
<b>Data use</b>			
Reported data is fed back to those who generate it to reinforce understanding of the way it is used.	Y	L	Key performance data is reported to staff by means of corporate documents and reports (Annual Performance Plans are issued to all stations/departments).
Performance information is regularly used, to identify deviations from planned performance.	Y	F	Quarterly Performance Monitoring report to Policy Group and A&PMC.
There is timely action on performance shortfalls, and follow-up to ensure action has been taken.	Y	F	Quarterly Performance Monitoring report to Policy Group and A&PMC. Action is documented within the Station and Departmental Business Plans



Definitions are generally applied correctly to all data items.	Y	L	Brigade order 16 Part 5 includes a list of definitions.
All data returns are supported by an audit trail, although there may be some weaknesses.	N	F	The organisation is currently undertaking a process mapping exercise which will identify the audit trail.
There is evidence that controls are exercised over data to verify its accuracy.			Brigade Order 16 Part 4. Controls are in place for manual scrutiny of key data processes (FDR1, BVPIs).
Reported data is generally submitted on a timely basis. Instances of data not being submitted on a timely basis are fully investigated and reported to management.	Y	F	Quarterly Performance Monitoring report to Policy Group and A&PMC. Fire and Rescue Service's annual statistical returns to the DCLG. Brigade Order 1, Part 4.

