

# **Your Business @ Risk Surveys**

**Humberstone Police Authority**

**Audit 2006/07**

External audit is an essential element in the process of accountability for public money and makes an important contribution to the stewardship of public resources and the corporate governance of public services.

Audit in the public sector is underpinned by three fundamental principles:

- auditors are appointed independently from the bodies being audited;
- the scope of auditors' work is extended to cover not only the audit of financial statements but also value for money and the conduct of public business; and
- auditors may report aspects of their work widely to the public and other key stakeholders.

The duties and powers of auditors appointed by the Audit Commission are set out in the Audit Commission Act 1998 and the Local Government Act 1999 and the Commission's statutory Code of Audit Practice. Under the Code of Audit Practice, appointed auditors are also required to comply with the current professional standards issued by the independent Auditing Practices Board.

Appointed auditors act quite separately from the Commission and in meeting their statutory responsibilities are required to exercise their professional judgement independently of both the Commission and the audited body.

### **Status of our reports to the Council**

The Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission explains the respective responsibilities of auditors and of the audited body. Reports prepared by appointed auditors are addressed to members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any member or officer in their individual capacity; or
- any third party.

### **Copies of this report**

If you require further copies of this report, or a copy in large print, in Braille, on tape, or in a language other than English, please call 0844 798 7070.

© Audit Commission 2007

For further information on the work of the Commission please contact:

Audit Commission, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ

Tel: 020 7828 1212 Fax: 020 7976 6187 Textphone (minicom): 020 7630 0421

[www.audit-commission.gov.uk](http://www.audit-commission.gov.uk)

# Contents

Introduction	4
Main conclusions	4
<b>Appendix 1 – Detailed user survey results</b>	<b>12</b>
<b>Appendix 2 – Detailed IT staff survey results</b>	<b>18</b>
<b>Appendix 3 – Action plan</b>	<b>26</b>

## Introduction

- 1 The growth in computer use, the anticipated increase in new technologies, greater public access and more joined up working also means increased risks for public sector bodies. Computer viruses, IT fraud, hacking, invasion of privacy and downloading of unsuitable material from the internet remain real threats to many organisations. Confidence in technologies that are influencing the way we live and work is being eroded and organisations must address these issues if the increased use of new technology is not to be matched by a similar increase in IT abuse.
- 2 An Audit Commission report, published in 2005, concluded that although organisations have got better at establishing anti-fraud frameworks, cultures and strategies, failures in basic controls are still a problem and the upsurge in the use of newer technologies has not been matched by enhanced security measures.
- 3 The Audit Commission has developed an online survey, designed to help organisations to:
  - raise awareness of the risks associated with their increasing use of technology;
  - gauge the level of knowledge within their organisations of such risks;
  - highlight areas where risks are greatest; and
  - take positive action to reduce risks.
- 4 In partnership with the Humberside Police Force (HPF), we ran two online surveys during May 2007. This report summarises the responses by IT users and IT staff at HPF (see Appendix 1) and indicates where further action may be necessary.
- 5 Our conclusions are based upon responses from 329 IT users and 17 IT staff at HPF. IT users were asked to complete a different and less technical set of questions than those answered by IT staff.

## Main conclusions

- 6 Overall, results are largely positive. In many of the areas covered by our survey, there appears to be a high level of understanding by respondents to the survey of IT risks and security.
- 7 Most IT users believe that HPF takes the threat of virus infection seriously and the user name and password control system is working well. However, 2 per cent claim to have suffered a virus infection on their machine.

- 8 The financial loss and reputational damage sections of the survey, attracted some mixed views from IT users. Twenty-seven per cent of IT users were aware of the anti-fraud policy but less than 6 per cent claimed to know what the main elements of the policy were. A high proportion of IT users knew that controls existed to restrict access to inappropriate internet sites and most IT users knew there was a Data Protection policy and its implications. However, there were mixed views over whether IT users have access to written protocols covering email usage and language.
- 9 There were mixed views concerning loss of user confidence, particularly around what staff responsibilities were in relation to the Information Security (IS) policy.
- 10 Responses from IT staff also indicated some areas for improvement. The main areas include better internal procedures to minimise the risk of deliberate damage by employees leaving the organisation. Improvements are also needed in the areas of business continuity and information security.
- 11 Key messages are also summarised in Table 1 - IT users and Table 2 - IT staff together with those areas where HPF might improve its current arrangements. We have highlighted a number of actions that have been discussed with HPF and an agreed action plan. The detailed responses are shown at Appendix 1.

**Table 1 Key messages IT user survey**

A summary of responses to our survey.

Positive messages	Areas requiring attention	Action to be discussed
<b>Business disruption risk</b>		
<p>Most users (86 per cent) think that the HPF takes the threat of virus infection very seriously. Virus protection software is installed on machines. The password system seems to be working well with 97 per cent of users having to change their passwords on a regular basis.</p>	<p>IT users had mixed views as to whether arrangements existed which:</p> <ul style="list-style-type: none"> <li>• required more than two passwords to access the systems and computers that they used to do their jobs;</li> <li>• on how to report a virus infection if I suffer an infection on my machine; and</li> <li>• authorised them to enter the HPF's computer rooms.</li> </ul> <p>Also 2 per cent claim to have suffered a virus infection on their machine.</p>	<p>R1 Present findings to Information Security Policy Group (ISPG) and agree an appropriate action plan to mitigate areas of weakness.</p>
<b>Financial loss risk</b>		
<p>Over 80 per cent of IT users claim that access to the information is only provided to those who need it. 93 percent of IT users knew the HPF's rules covering private use of IT facilities and in particular, what is and what isn't acceptable.</p>	<p>Twenty-seven per cent of the IT users believed that HPF has an anti-fraud strategy, while the rest didn't know. Only 6 per cent claimed to know what the main elements of the strategy were.</p> <p>IT users had mixed views as to whether their computer is clearly security-marked.</p>	<p>R2 There is a need to remind all users to review the anti-fraud strategy and its key elements.</p>

Positive messages	Areas requiring attention	Action to be discussed
<b>Reputational damage risk</b>		
<p>A high proportion of IT users:</p> <ul style="list-style-type: none"> <li>• are allowed access to the internet only by connections provided by the HPF;</li> <li>• have had it made clear to them that the HPF's policy is that accessing or storing unsuitable material is a disciplinary matter;</li> <li>• the use of unlicensed software is prohibited;</li> <li>• know HPF has a documented data protection policy;</li> <li>• know that the downloading of unsuitable material and misuse of personal data is a disciplinary matter;</li> <li>• their responsibilities under the Data Protection Act had been explained to them; and</li> <li>• have been informed that the misuse of personal data will be treated as a disciplinary offence by my organisation.</li> </ul>	<p>IT users had mixed views concerning whether:</p> <ul style="list-style-type: none"> <li>• internal auditors or HPF's own IT staff checked the software on their machines; and</li> <li>• they have access to internet and email usage and language protocols.</li> </ul>	<p>R3 Review whether staff training programmes provide appropriate coverage.</p>

Positive messages	Areas requiring attention	Action to be discussed
<b>Legislative implications</b>		
<p>Most IT users stated they were aware of the main implications of the following legislation:</p> <ul style="list-style-type: none"> <li>• Freedom of Information Act;</li> <li>• Human Rights Act (HRA); and</li> <li>• Data Protection Act (DPA).</li> </ul>	<p>Sixty-one per cent of IT users said they were aware of the main implications of the Computer Misuse Act (CMA) while the majority of staff was unaware of the Public Interest Disclosure Act (PIDA).</p>	<p>As R3.</p>
<b>Loss of user confidence risk</b>		
<p>This is the weakest area in the IT user's survey but here were positive responses around the HPF having the following procedures in place:</p> <ul style="list-style-type: none"> <li>• an Information Security (IS) policy; and</li> <li>• someone in my organisation is specifically responsible for IT security.</li> </ul>	<p>IT users had mixed views concerning whether:</p> <ul style="list-style-type: none"> <li>• they have been provided with a copy of the IS policy;</li> <li>• what their responsibilities were in relation to the Information Security policy; and</li> <li>• senior management was committed the IS policy and its observance.</li> </ul>	<p>R4 Review and improve IS arrangements by ensuring all staff are aware of the IS policy and informing them of their responsibilities in relation to it.</p>

Source: Audit Commission

**Table 2 Key messages IT staff survey**

A brief summary of responses to our survey.

Positive messages	Areas requiring attention	Action to be discussed
<b>Business disruption risk</b>		
<p>A very high proportion of IT staff know:</p> <ul style="list-style-type: none"> <li>• the HPF takes the threat of a virus infection very seriously;</li> <li>• user registration and sign on procedures prevent unauthorised access to networks;</li> <li>• servers and network equipment are sited securely and adequate protection is offered;</li> <li>• a firewall protects networks, systems and information from intrusion from outside;</li> <li>• physical entry controls prevent unauthorised access to IT facilities;</li> <li>• amendment to a program or system must go through our change control process; and</li> <li>• backups of data on all servers are taken frequently.</li> </ul>	<p>Only 29.4 per cent of IT staff thought there were measures in place to restrict the impact of a virus. In addition, IT staff had mixed views as to whether HPF:</p> <ul style="list-style-type: none"> <li>• procedures for recovering from a virus infection have been documented;</li> <li>• network logs are inspected periodically by network staff;</li> <li>• have appointed an IT security officer;</li> <li>• internal procedures minimise the risk of deliberate damage by employees leaving the HPF;</li> <li>• all IT staff are trained in our change control requirements; and</li> <li>• has a clear business continuity plan, which is based on a robust risk analysis and all staff named in it are aware of their responsibilities.</li> </ul>	<p>R5 Review the issues identified by IT staff in the previous columns and take appropriate action to address them, in particular ensuring that business continuity arrangements are addressed as a matter of priority.</p>

Positive messages	Areas requiring attention	Action to be discussed
<b>Financial loss risk</b>		
<p>All IT staff were clear about rules covering private use of IT facilities and in particular what is and what isn't acceptable. Also access to systems is only provided to those who need it.</p>	<p>IT staff were unclear about which systems were most at risk of fraud and whether they had been afforded additional protection.</p>	<p>As R2.</p>
<b>Reputational damage risk</b>		
<p>A high proportion of IT staff:</p> <ul style="list-style-type: none"> <li>• know that the downloading of unsuitable material and misuse of personal data is a disciplinary matter;</li> <li>• have access to internet and email usage protocols;</li> <li>• users in the HPF are prevented from gaining access to system utilities;</li> <li>• know HPF has a documented data protection policy;</li> <li>• know all users are required to sign a confidentiality undertaking as part of their conditions of service;</li> <li>• know that misuse of personal data is treated as a disciplinary offence; and</li> <li>• their computer has a lock out facility to be used when left unattended.</li> </ul>	<p>IT staff also had mixed views concerning whether:</p> <ul style="list-style-type: none"> <li>• Internal Auditors undertake reviews of software on users' PCs;</li> <li>• the asset register is up to date, as are all enterprise/site license numbers;</li> <li>• responsibilities under the Data Protection Act have been explained to me; and</li> <li>• systems containing personal data are registered with the Information Commissioner.</li> </ul>	<p>As R3.</p> <p>R6 Ensure that the asset register and all license/enterprise numbers are updated.</p>

Positive messages	Areas requiring attention	Action to be discussed
<b>Legislative implications</b>		
<p>All IT staff stated they were aware of the main implications of Data Protection Act and the majority following legislation:</p> <ul style="list-style-type: none"> <li>• Freedom of Information Act (FOI);</li> <li>• Human Rights Act (HRA); and</li> <li>• Computer Misuse Act (CMA).</li> </ul>	<p>Only 41.2 per cent IT staff said they were aware of the main implications of the Public Interest Disclosure Act (PIDA).</p>	<p>As R3.</p>
<b>Loss of user confidence risk</b>		
<p>This is the weakest area in the IT user's survey but here were positive responses around the HPF having an up to date Information Security policy.</p>	<p>IT staff had mixed views concerning whether:</p> <ul style="list-style-type: none"> <li>• clearly defined responsibilities in relation to the Information Security (IS) policy;</li> <li>• senior management commitment to the IS policy and its observance; and</li> <li>• information on where to access clear written procedures for reporting a security incident.</li> </ul>	<p>As R4.</p>

Source: Audit Commission

## Appendix 1 – Detailed user survey results

Q1 responses are not recorded as these simply set out the part of the HPF the respondent was from.

<b>Q2</b>	<b>The risk of business disruption</b>	<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	My organisation takes the threat of a virus infection very seriously.	86%	1%	12%	1%
	Virus protection software is installed on my machine.	82%	0%	18%	0%
	Virus protection software is regularly updated on my machine.	41%	1%	59%	0%
	I have been given clear instructions about dealing with emailed files from external sources.	64%	27%	8%	1%
	I am sent an alert when new viruses are discovered and am told what to do and what not to do.	21%	43%	33%	4%
	I know how to report a virus infection if I suffer an infection on my machine.	61%	28%	11%	1%
	I have suffered a virus infection on my machine.	2%	83%	14%	1%
	Whenever I have suffered a virus infection, my machine was cleansed and restored quickly.	1%	2%	20%	77%

Q2	The risk of business disruption	Yes	No	Don't know	Not applicable
	To log on to my machine I must enter a user name and password.	98%	1%	0%	1%
	To log on to my organisation's network I must enter a user name and password.	92%	5%	2%	0%
	I am forced to change my password by the system on a regular basis eg every month.	97%	2%	1%	0%
	To access the computers and systems I use to do my job I must remember more than two passwords.	74%	25%	1%	0%
	I have not written my password(s) down.	59%	40%	0%	1%
	I am not authorised to enter our computer rooms.	47%	16%	32%	4%

14 Your Business @ Risk Surveys | Appendix 1 – Detailed user survey results

<b>Q3 The risk of financial loss</b>					
		<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	My organisation has an anti-fraud strategy.	27%	0%	73%	0%
	I know what the key elements of the strategy are.	6%	39%	50%	5%
	I only have access to the information I need to do my job.	80%	16%	5%	0%
	I am prevented from installing any software on my machine.	90%	1%	9%	0%
	I am prevented from copying software from my machine.	82%	2%	16%	0%
	My computer is clearly security-marked.	55%	11%	33%	0%
	I know what are my organisation's rules are covering private use of IT facilities and in particular what is and what isn't acceptable.	93%	2%	5%	0%

<b>Q4 The risk of reputational damage</b>		<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	I am allowed access to the internet only by connections provided by my organisation.	92%	4%	3%	0%
	I have been informed that my access to the internet will be monitored.	95%	2%	3%	1%
	It has been made clear to me that my organisation's policy is that accessing or storing unsuitable material is a disciplinary matter.	98%	1%	1%	0%
	Emails sent to me from outside my organisation that contain very large files or executable programs etc. are prevented from reaching me.	55%	1%	41%	4%
	I have access to written protocols covering email usage and language.	66%	6%	28%	0%
	I have been informed by my organisation that the use of unlicensed software is prohibited.	89%	4%	7%	0%
	I am prevented from installing software on my machine.	88%	1%	11%	0%

16 Your Business @ Risk Surveys | Appendix 1 – Detailed user survey results

<b>Q4 The risk of reputational damage</b>					
		<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	Internal Auditors or IT staff in my organisation have checked the software on my machine.	31%	2%	67%	0%
	My organisation has a documented data protection policy.	84%	1%	16%	0%
	My organisation has appointed a data protection officer.	70%	0%	30%	0%
	I have been required to sign a confidentiality undertaking as part of my conditions of service.	84%	6%	10%	0%
	My responsibilities under the Data Protection Act have been explained to me.	90%	6%	4%	0%
	I have been informed that the misuse of personal data will be treated as a disciplinary offence by my organisation.	99%	1%	1%	0%
	My PC is automatically timed out after a short period of inactivity and my password and user name must be entered to resume the session.	93%	4%	3%	0%
<b>Q5 I am aware of the main implications of the following legislation.</b>					
	• The Computer Misuse Act				61%
	• The Freedom of Information Act				84%
	• The Human Rights Act				80%
	• The Public Interest Disclosure Act				32%
	• The Data Protection Act				97%

<b>Q6</b>	<b>Loss of public or user confidence</b>	<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	My organisation has an Information Security policy.	66%	0%	34%	0%
	I have been provided with a copy of the policy.	18%	49%	30%	2%
	I have been informed about the policy and what I must and must not do.	36%	36%	26%	2%
	Senior management in my organisation is committed to the policy and its observance.	38%	2%	59%	1%
	I know where to find written procedures for reporting a security incident.	32%	44%	24%	0%
	Someone in my organisation is specifically responsible for IT security.	69%	1%	30%	0%

## Appendix 2 – Detailed IT staff survey results

Q1	Which ICT Department do you work in?	
	Corporate ICT	53.3%
	Departmental ICT	46.7%

Q2	The risk of business disruption	Yes	No	Don't know	Not applicable
	My organisation takes the threat of a virus infection very seriously.	94.1%	0.0%	5.9%	0.0%
	Our policy is to install virus protection software on all our machines.	76.5%	5.9%	17.6%	0.0%
	Staff are provided with regular updates to virus protection software.	64.7%	11.8%	17.6%	5.9%
	Staff have been given clear instructions about dealing with emailed files from external sources.	75.0%	12.5%	12.5%	0.0%
	Staff are alerted when new viruses are discovered and are advised as to what they must do.	29.4%	35.3%	23.5%	11.8%
	We have clear procedures in place for reporting a virus incident.	52.9%	17.6%	23.5%	5.9%

Q2	The risk of business disruption (continued)	Yes	No	Don't know	Not applicable
	Our procedures for recovering from a virus infection have been documented.	12.5%	18.8%	68.8%	0.0%
	Our virus software is automatically updated by the software vendor.	70.6%	0.0%	29.4%	0.0%
	In the event of a virus outbreak measures are in place to restrict the impact of that virus eg we make router changes to restrict virus infection.	29.4%	5.9%	64.7%	0.0%
	A firewall protects our networks, systems and information from intrusion from outside.	100.0%	0.0%	0.0%	0.0%
	Our firewall prevents large files and executable programs from reaching our networks.	76.5%	5.9%	17.6%	0.0%
	Our user registration and sign-on procedures prevent unauthorised access to our networks.	100.0%	0.0%	0.0%	0.0%
	Proper password management is enforced by the system on all users.	100.0%	0.0%	0.0%	0.0%
	Our dial-up connections are secure.	76.5%	0.0%	17.6%	5.9%

20 Your Business @ Risk Surveys | Appendix 2 – Detailed IT staff survey results

Q2	The risk of business disruption (continued)	Yes	No	Don't know	Not applicable
	Network management staff have been appointed.	87.5%	6.3%	6.3%	0.0%
	We have appointed an IT security officer.	52.9%	23.5%	23.5%	0.0%
	A detailed daily log of network activity is maintained.	41.2%	5.9%	52.9%	0.0%
	Network logs are inspected periodically by network staff.	58.8%	0.0%	41.2%	0.0%
	Sensitive programs and information are given additional protection.	93.8%	0.0%	6.3%	0.0%
	Security violations are reported to IT security staff immediately by our security systems.	58.8%	0.0%	41.2%	0.0%
	Our web site vulnerability is checked every month.	11.8%	11.8%	76.5%	0.0%
	Physical entry controls prevent unauthorised access to our IT facilities.	94.1%	0.0%	5.9%	0.0%
	Our servers and network equipment are sited securely and adequate protection is offered.	94.1%	0.0%	5.9%	0.0%

<b>Q2</b>	<b>The risk of business disruption</b>	<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	Our internal procedures minimise the risk of deliberate damage by employees leaving the organisation.	47.1%	11.8%	41.2%	0.0%
	Any amendment to a program or system must go through our change control process.	100.0%	0.0%	0.0%	0.0%
	Our change control processes are well documented.	88.2%	0.0%	11.8%	0.0%
	All IT staff are trained in our change control requirements.	52.9%	29.4%	17.6%	0.0%
	Backups of data on all servers are taken frequently.	88.2%	0.0%	11.8%	0.0%
	Backup arrangements are properly documented.	70.6%	5.9%	23.5%	0.0%
	User and IT staff have been trained in how to conduct backups of servers.	58.8%	17.6%	23.5%	0.0%
	Monitoring of backups ensures that management is alerted when backups of remote servers do not take place.	64.7%	0.0%	35.3%	0.0%
	My organisation has a clear business continuity plan.	35.3%	17.6%	47.1%	0.0%
	All staff named in the business continuity plan know of its existence and their role in it.	29.4%	11.8%	52.9%	5.9%
	Our continuity plan is based upon a robust risk analysis process.	18.8%	18.8%	56.3%	6.3%

22 Your Business @ Risk Surveys | Appendix 2 – Detailed IT staff survey results

<b>Q3 The risk of financial loss</b>					
		<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	The systems most at risk from fraud have been identified.	41.2%	0.0%	58.8%	0.0%
	The systems most at risk are afforded additional protection.	52.9%	0.0%	47.1%	0.0%
	We have a documented access control policy.	76.5%	5.9%	17.6%	0.0%
	Access to systems is only provided to those who need it.	100.0%	0.0%	0.0%	0.0%
	We have controls to prevent the copying or removal of software.	76.5%	11.8%	11.8%	0.0%
	Hardware is clearly security-marked.	76.5%	5.9%	17.6%	0.0%
	My organisation has clear rules covering private use of IT facilities and in particular what is and what isn't acceptable.	100.0%	0.0%	0.0%	0.0%

<b>Q4 The risk of reputational damage</b>					
		<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	Staff are only allowed to access the Internet through our authorised ISP.	100.0%	0.0%	0.0%	0.0%
	Internet activity logs are reviewed by managers.	76.5%	0.0%	23.5%	0.0%
	We bar access to internet sites we deem to be unsuitable.	94.1%	5.9%	0.0%	0.0%
	Our policies make it clear to all staff that the downloading or storage of unsuitable material is a disciplinary matter.	100.0%	0.0%	0.0%	0.0%

<b>Q4</b>	<b>The risk of reputational damage</b>				
		<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	Protocols for internet and email use have been developed and are available to all users.	88.2%	0.0%	11.8%	0.0%
	My organisation has made it clear to all staff that use of unlicensed software is prohibited.	94.1%	0.0%	5.9%	0.0%
	Security software that prevents the installation of any program except by authorised IT staff is installed on all PCs and laptops.	94.1%	5.9%	0.0%	0.0%
	Our Internal Auditors undertake reviews of software on users' PCs.	35.3%	0.0%	64.7%	0.0%
	Users in my organisation are prevented from gaining access to system utilities.	94.1%	0.0%	5.9%	0.0%
	Our asset register is up to date, as are all enterprise/site license numbers.	58.8%	0.0%	41.2%	0.0%
	My organisation has a documented Data Protection Policy.	88.2%	0.0%	11.8%	0.0%
	My organisation has appointed a data protection officer.	70.6%	0.0%	29.4%	0.0%

24 Your Business @ Risk Surveys | Appendix 2 – Detailed IT staff survey results

<b>Q4 The risk of reputational damage</b>					
		<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	All users are required to sign a confidentiality undertaking as part of their conditions of service.	81.3%	0.0%	18.8%	0.0%
	My responsibilities under the Data Protection Act have been explained to me.	76.5%	23.5%	0.0%	0.0%
	Misuse of personal data is treated as a disciplinary offence.	88.2%	0.0%	11.8%	0.0%
	PC's are timed out after a period of inactivity.	82.4%	17.6%	0.0%	0.0%
	My computer has a lock out facility to be used when left unattended.	94.1%	5.9%	0.0%	0.0%
	Systems containing personal data are registered with the Information Commissioner.	29.4%	0.0%	64.7%	5.9%

<b>Q5 I am aware of the main implications of the following legislation.</b>	
• The Computer Misuse Act	82.4%
• The Freedom of Information Act	82.4%
• The Human Rights Act	82.4%
• The Public Interest Disclosure Act	41.2%
• The Data Protection Act	100.0%

<b>Q6 The risk of loss of public or user confidence</b>					
		<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
	My organisation has an up to date Information Security policy.	70.6%	0.0%	29.4%	0.0%
	Staff are informed about the policy and what they must and must not do.	68.8%	0.0%	31.3%	0.0%
	Senior management is committed to the policy and its observance.	58.8%	0.0%	41.2%	0.0%
	An officer group manages the implementation of information security.	58.8%	11.8%	29.4%	0.0%
	Regular independent reviews of information security are undertaken.	41.2%	0.0%	58.8%	0.0%
	We comply with BS7799 standards.	5.9%	5.9%	88.2%	0.0%
	There are clear written procedures for reporting and following up all security incidents.	52.9%	5.9%	35.3%	5.9%

## Appendix 3 – Action plan

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
6	R1 Present findings to Information Security Policy Group (ISPG) and agree an appropriate action plan to mitigate areas of weakness.	3	Head of Information Services (Graham Dawson)	yes		31 December 2008
6	R2 There is a need to remind all users to review the anti-fraud strategy and its key elements.	2	ISPG	yes		31 March 2008
7	R3 Review whether staff training programmes provide appropriate coverage.	2	Head of Information Compliance (Richard Heatley)	yes		31 March 2008

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
8	R4 Review and improve IS arrangements by ensuring all staff are aware of the IS policy and informing them of their responsibilities in relation to it.	2	ISPG	yes		31 March 2008
9	R5 Review the issues identified by IT staff in the previous columns and take appropriate action to address them, in particular ensuring that business continuity arrangements are addressed as a matter of priority.	2	ISPG	yes		31 March 2008
10	R6 Ensure that the asset register and all license/enterprise numbers are updated.	2	Head of Information Services (Graham Dawson)	yes		31 March 2008