Audit Summary Report

January 2007

Your Business @ Risk Survey

Sedgefield Borough Council

Audit 2006/2007

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 0845 056 0566.

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

Contents

Introduction

1 The growth in the use of newer technologies to give greater public access has resulted in 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 Sedgefield Borough Council, we ran the above online survey in mid September 2006. This brief report summarises the responses by staff at the council. The full survey results are reproduced in Appendix 1 with a traffic light system to highlight both positive messages and identify any areas of significant weakness where further action is necessary.

Main findings and conclusions

5 Our conclusions are based upon responses from around 420 users and all 20 ICT staff from a total of approximately 820 council employees requested to take part in the survey. Overall, the results are positive and any concerns are mostly around lack of awareness. In most areas the council's users score highly and better than the national average - as indicated by the Commission's national database which currently contains almost 15,000 responses from around 80 public sector organisations.

6 The ICT department is a reasonably sized department which has to meet the same modern day demands as a larger council. It therefore does needs to be more flexible and adaptable due to limited capacity and skills. The survey has highlighted some IT risks and gaps in the knowledge base of professional ICT staff.

7 There are areas where further improvements can be made. As the survey is based on the perceptions of users and ICT staff, the issues that arise often relate to the need to improve communication, provide more information and training. However, it may also point to areas where improved procedures are required. The main areas highlighted by the survey include the following.

- Absence of IT policies, for example, Information security and email.
- Business continuity arrangements.
- Promoting the anti-fraud strategy.
- Knowledge of key areas of relevant legislation.

8 Key messages are drawn out in Table 1 below and we have summarised the recommendations and included management responses discussed and agreed with officers. Appendix 1 provides a summary of the survey questions and the results for the council.

Recommendations

Recommendations	
R1	*Improve awareness for all staff on reporting computer virus incidents.*
R2	*Consider discussing the results of the ICT staff survey with all department staff.*
R3	*Consider the appointment of a dedicated IT security officer.*
R4	*Ensure that formal change control procedures are developed.*
R5	*Improve awareness and make more information readily available to address business continuity arrangements.*
R6	*Improve awareness for all staff on the anti-fraud strategy.*
R7	*Ensure an access control policy is developed.*
R8	*Inform staff of Council policy on use of email.*
R9	*Improve awareness of the requirements of the Data Protection Act legislation*
R10	*Reassess the use of PC timeout controls and consider implementing this feature.*
R11	*Raise the level of IT legislation awareness through improved induction and ongoing training programmes for all staff.*
R12	*Develop and issue an Information Security policy.*
R13	*Develop procedures for reporting IT security incidents.*

The way forward

9 The council may find it beneficial to carry out this survey again at a future date to measure any improvements that have been made.

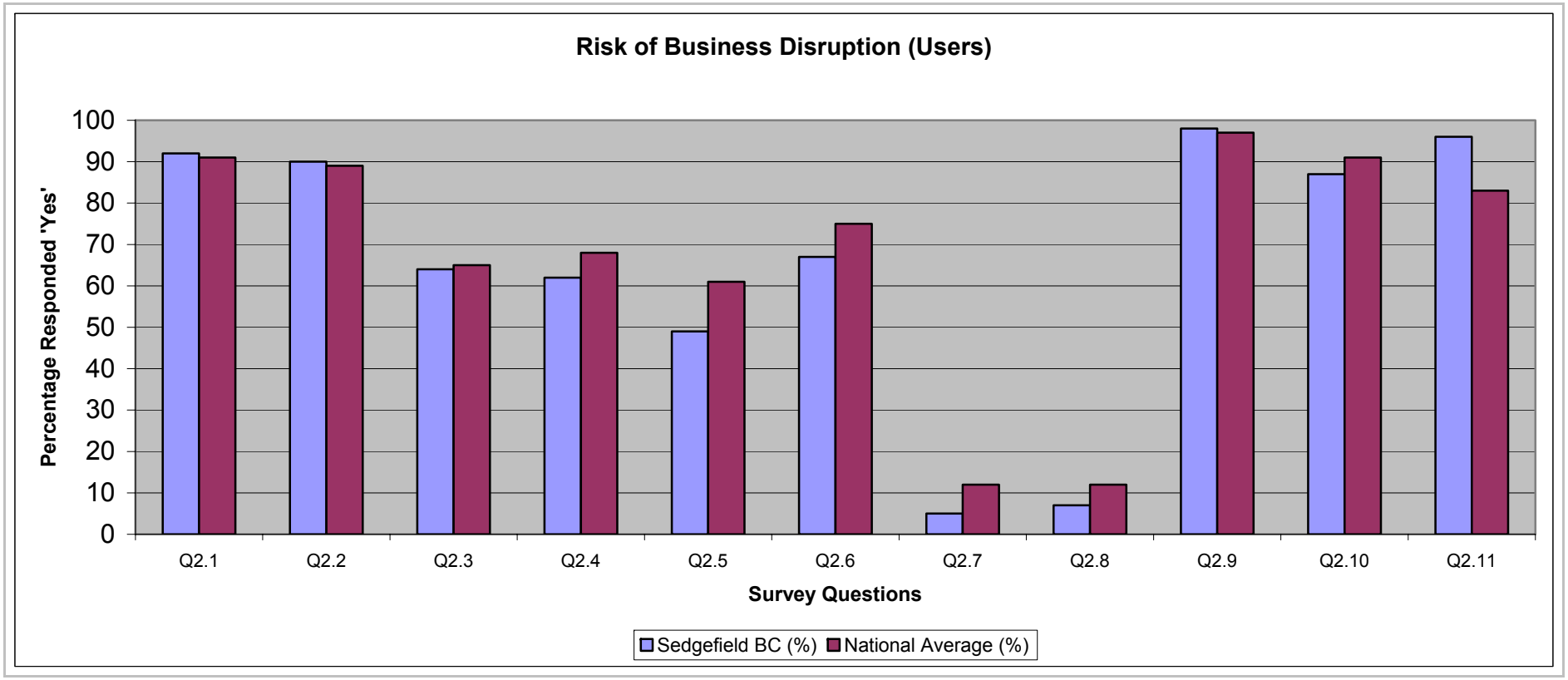
Table 1 Key messages

A brief summary of responses to our survey covering both dedicated ICT staff and departmental business systems users

Business Disruption Risk		
Positive messages	**Areas requiring attention**	**Suggested Action**
A high number of users (95 per cent) replied positively at how the council takes the threat of computer virus infection very seriously.	Users (67 per cent) are not significantly aware of the procedures for reporting virus infections. Nationally this is 75 per cent.	Improve awareness for all staff on reporting computer virus incidents.
There is a small team which manages virus related type issues seamlessly in the background. Most users and some ICT staff will not be aware this service is delivered.	ICT staff provided an average response of 60 per cent displaying a lack of information about having procedures to address virus infections should they occur.	Consider discussing the results of the ICT staff survey with all department staff.
Virus protection software is installed on machines and regularly updated. This explains the high number of users not knowing this task is carried out and it is not seen as a weakness.	70 per cent of ICT respondents were misinformed about the appointment of an IT security officer. There is no dedicated post although the role tasks are carried out ad-hoc by some of the ICT staff on an informal basis.	Consider the appointment of a dedicated IT security officer.
5 per cent users (nationally 12 per cent) claim to have suffered a virus infection on their machine which is a good result (Q2.7/2.8 – see appendix for survey questions).	The two most significant IT risk areas in the survey where ICT respondents highlighted an absence of procedures and awareness are:	
ICT staff scored highly in most areas. Due to the dedicated responsibilities of certain ICT staff (network/firewall/anti-virus software management) or specific system requirements (server backups), the instances where ICT staff did not know a clear answer to some of the questions is not seen as a significant risk.	• the absence of formal change control procedures, an average of 60 per cent of ICT respondents didn't know; and	Ensure that formal change control procedures are developed.
	• the absence of business continuity arrangements (average 50 per cent). A disaster recovery plan for IT facilities is in the early stages of development.	Improve awareness and make more information readily available to address business continuity arrangements.
Password use and maintenance follows best practice. Individual machines and the council's network require the use of username and password for access. Password changes are enforced.		

Figure 1 Risk of Business Disruption (Users)

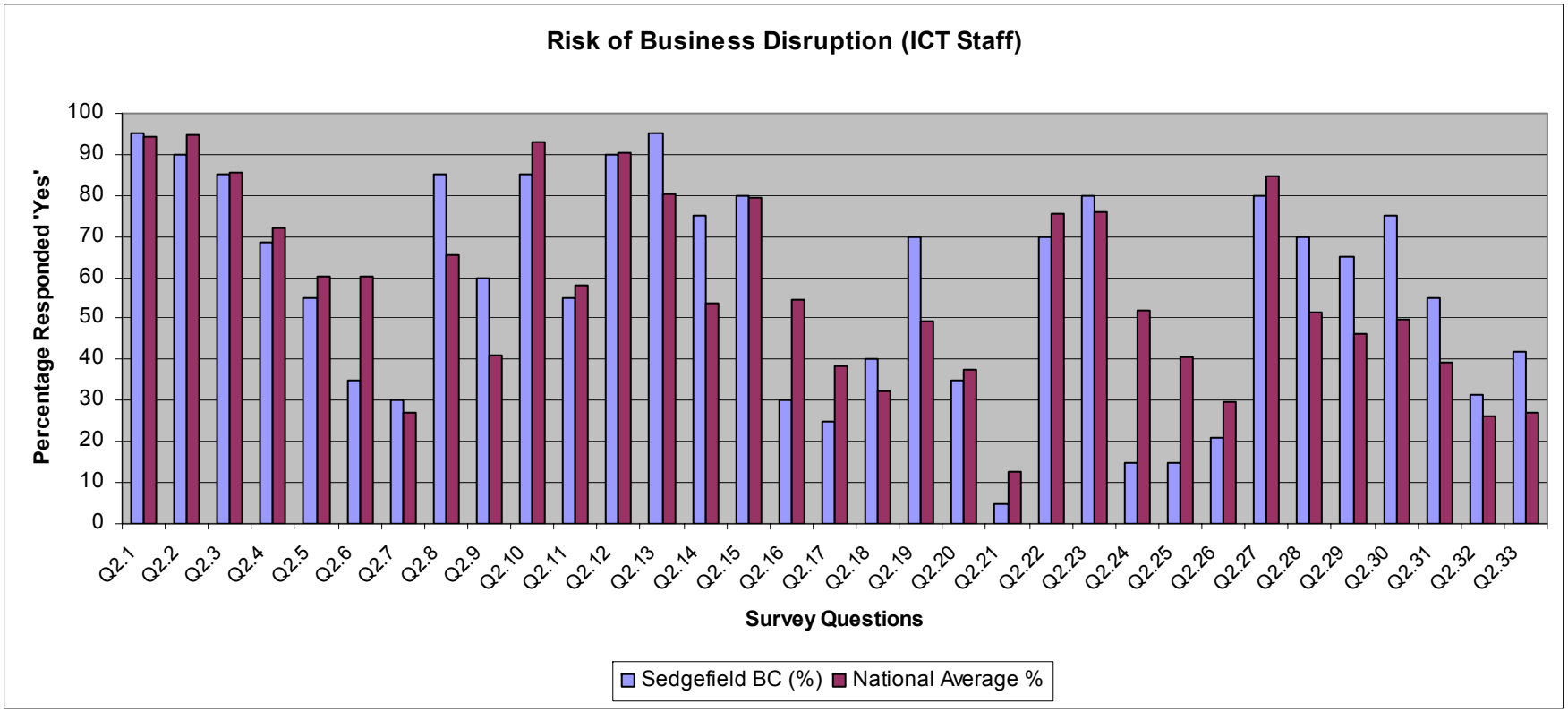
Results for council versus national results



Source: YB@R: Audit Commission

(Responses to Q2.7 & 2.8 on computer virus infection are better if lower than the national average).

Figure 2 ICT Staff Results: Risk of Business Disruption

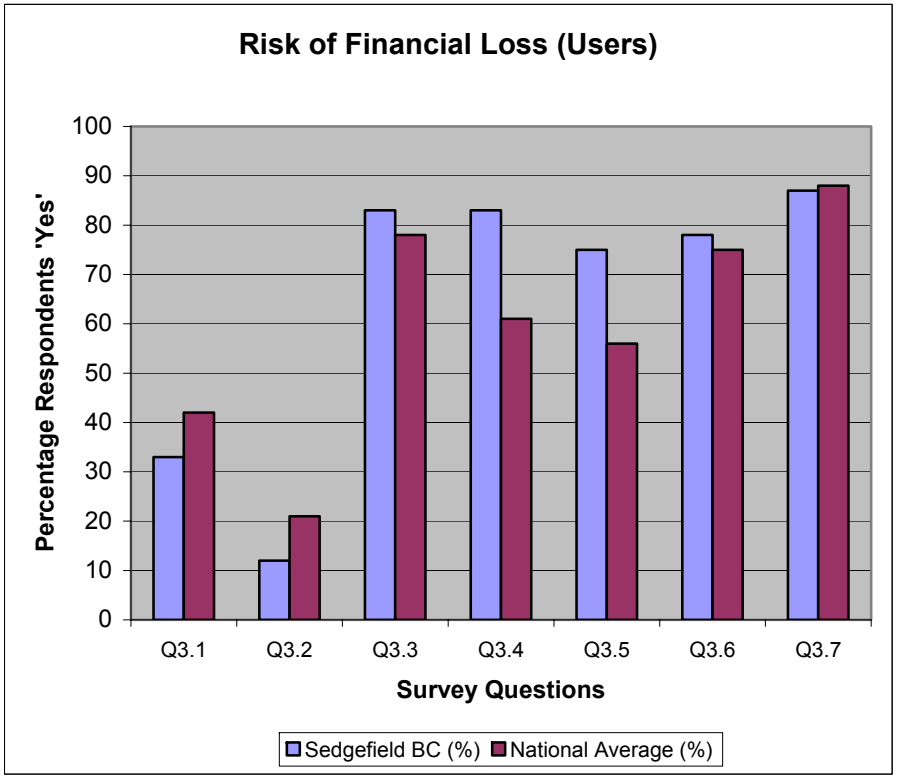


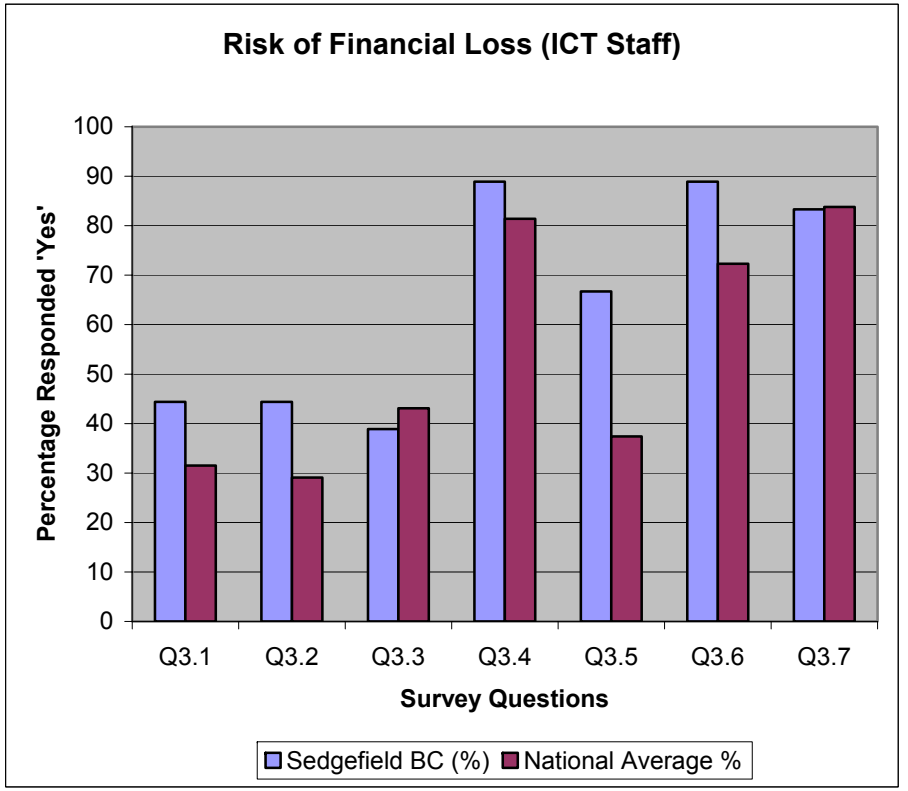
Source: YB@R: Audit Commission

Financial Loss Risk		
Positive messages	**Areas requiring attention**	**Suggested Action**
A high percentage of users (83 per cent) claim they have access to the information they need to do their job (national average 78 per cent). The council has been reasonably clear in informing all staff what rules exist regarding private use of ICT facilities, 87 per cent of users and 83 per cent of ICT staff confirm they have been informed. Both are good scores but just below the national average. Measures are in place to prevent staff copying software from and to their machines.	Approximately 67 per cent of user respondents are not aware of the existence or content of the council's anti-fraud strategy. 50 per cent of ICT staff do not know if there is a formal access control policy.	Improve awareness for all staff on the anti-fraud strategy. Ensure an access control policy is developed.

Figure 3 Risk of Financial Loss

Council versus national results





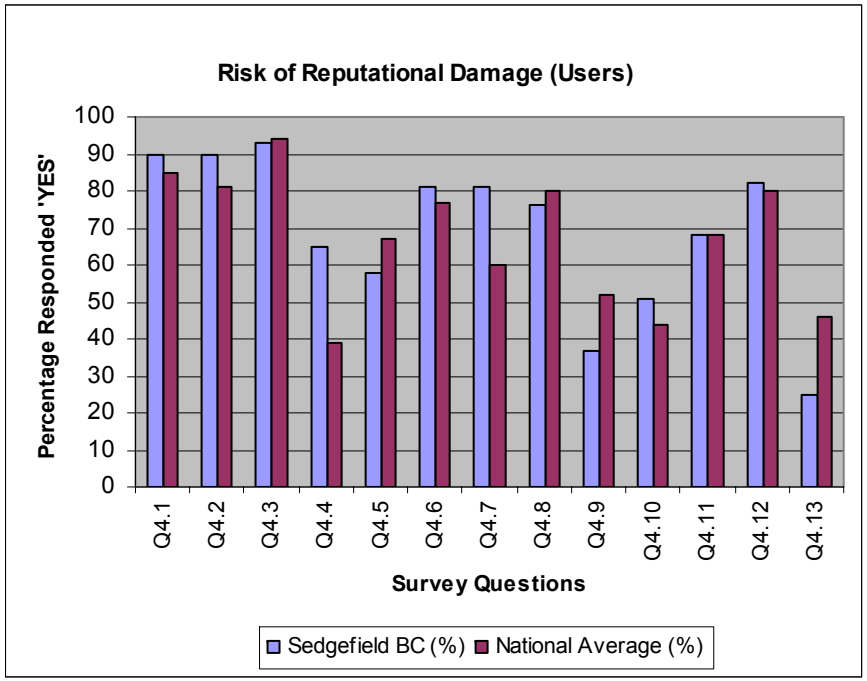
Source: YB@R: Audit Commission

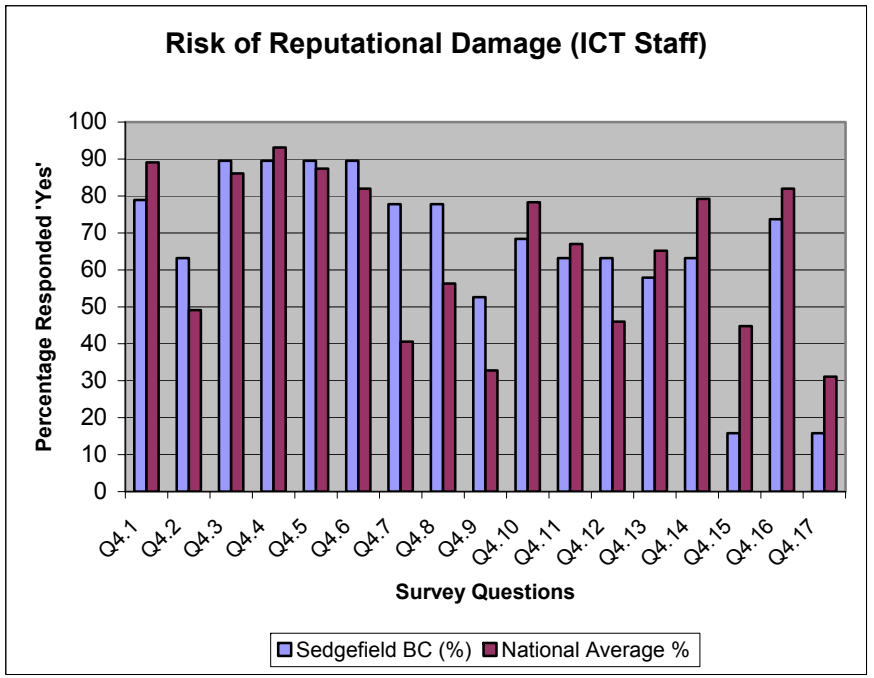
Reputational Damage Risk

Positive messages	Areas requiring attention	Suggested Action
A very high proportion of IT users: • know that their internet activity is monitored; • know that the downloading of unsuitable material and misuse of personal data is a disciplinary matter; • have access to internet and email usage protocols; and • know that the use of unlicensed software is prohibited. Misuse of personal data is well understood to be a disciplinary offence by users (82 per cent) but only 63 per cent by ICT staff which is below the national average of 79 per cent.	42 per cent of user respondents are not aware of or have access to written protocols covering email usage and language. 24 per cent of users and 32 per cent of ICT staff confirmed their lack of knowledge about a documented data protection policy. Approximately 49 per cent users and 37 per cent ICT staff are unaware of confidentiality requirements. 32 per cent user respondents and 42 per cent ICT respondents have not had their responsibilities under the Data Protection Act explained to them. There is a distinct lack of awareness around the Data Protection Act. PCs are not times out after a short period of inactivity. 60 per cent of users and 58 per cent ICT respondents confirmed this and it reflects the actual absence of controls in this area due to previous problems.	Inform staff of Council policy on use of email. Improve awareness of the requirements of the Data Protection Act legislation. Reassess the use of PC timeout controls and consider implementing this feature.

Figure 4 Risk of Reputational Damage

Council versus national results



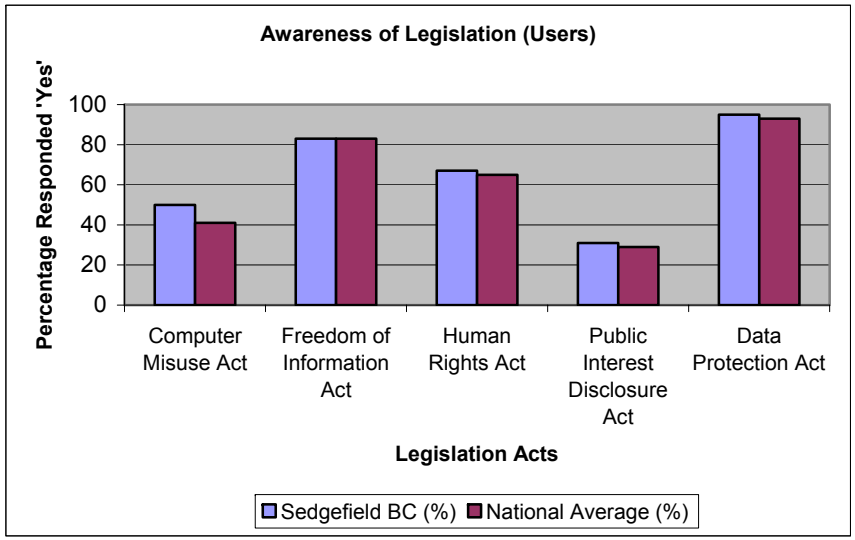


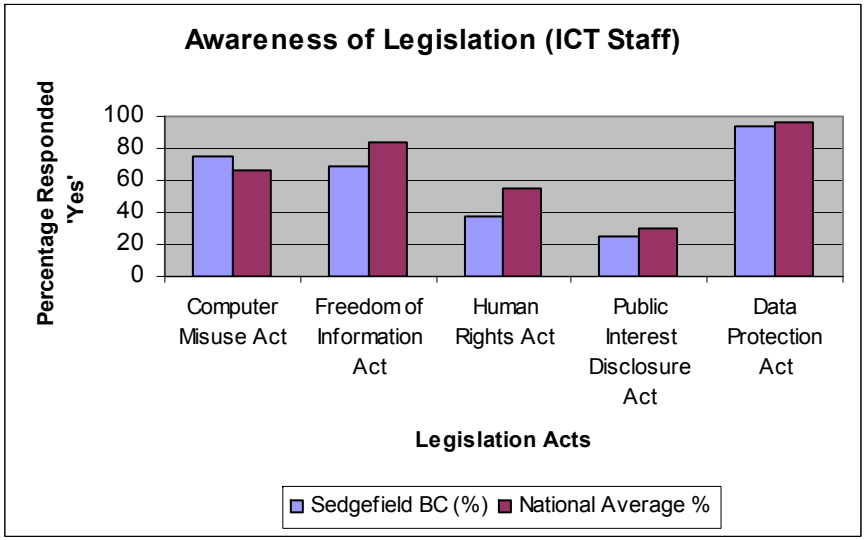
Source: YB@R: Audit Commission

Awareness of implications of legislation	Areas requiring attention	Suggested Action
User respondents scored well above the national average for their group covering all five legislation acts.	ICT staff respondents scored lower than the national average in awareness of four of the five IT related legislation acts.	Raise the level of IT legislation awareness through improved induction and ongoing training programmes for all staff.

Figure 5 Awareness of Implications of Legislation

Council versus national results



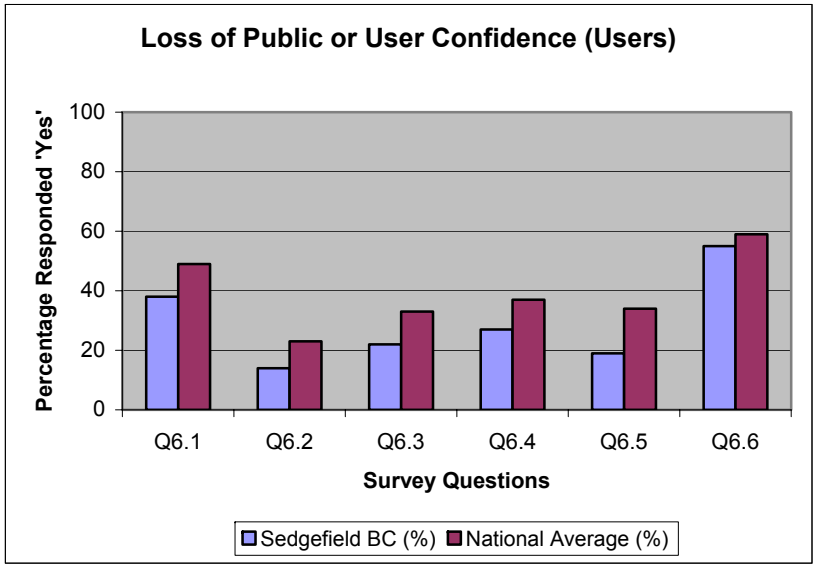


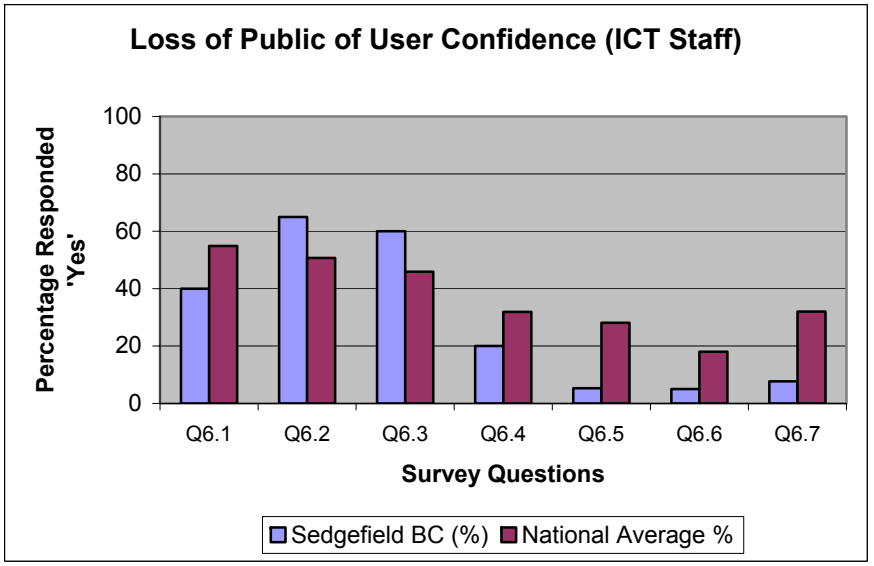
Source: YB@R: Audit Commission

Loss of User Confidence Risk		
Positive messages	**Areas requiring attention**	**Suggested Action**
Both sets of respondents scored less well in this section. ICT staff do understand the principles of information security and the development of an information security policy is still in progress.	The Council is in the process of developing an Information Security policy. There are no immediate plans to progress towards implementing BS7799 as the process is extensive and they have limited capacity. The lack of knowledge in this area accurately reflects the survey results. There is a lack of awareness of documented procedures for reporting an IT security incident (80 per cent ICT staff don't know and 36 per cent users).	Develop and issue an Information Security policy. Develop procedures for reporting IT security incidents.

Figure 6 Loss of User Confidence

Council versus national results





Source: YB@R: Audit Commission

Appendix 1 – Detailed survey results

Key
Good/satisfactory
Scope for improvement
Weakness identified

User survey

Q1	**Which Department do you work in? (only complete if agreed by your Authority/Trust)**	
	Councillors	0%
	Chief Executives	5%
	Resources	42%
	Housing	16%
	Neighbourhood Services	18%
	Leisure Services	19%

Note: Rounding up of responses may result in some scores slightly exceeding 100%.

Q2 The risk of business disruption

Virus protection is handled by dedicated staff seamlessly in the background and most users will not be aware. This may explain the high number of 'Don't know' responses.

		Yes	*No*	*Don't know*	*Not Applicable*
2.1	My organisation takes the threat of a virus infection very seriously	92%	0%	8%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.2	Virus protection software is installed on my machine	90%	0%	10%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.3	Virus protection software is regularly updated on my machine	64%	0%	35%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.4	I have been given clear instructions about dealing with emailed files from external sources	62%	28%	9%	1%
		Yes	*No*	*Don't know*	*Not Applicable*
2.5	I am sent an alert when new viruses are discovered and am told what to do and what not to do	49%	23%	27%	2%

		Yes	*No*	*Don't know*	*Not Applicable*
2.6	I know how to report a virus infection if I suffer an infection on my machine	67%	21%	12%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.7	I have suffered a virus infection on my machine	5%	83%	11%	2%
		Yes	*No*	*Don't know*	*Not Applicable*
2.8	Whenever I have suffered a virus infection, my machine was cleansed and restored quickly	7%	2%	17%	73%
		Yes	No	Don't know	Not Applicable
2.9	To log on to my machine I must enter a user name and password	98%	2%	0%	0%
		Yes	No	Don't know	Not Applicable
2.10	To log on to my organisation's network I must enter a user name and password	87%	8%	4%	1%
		Yes	No	Don't know	Not Applicable
2.11	I am forced to change my password by the system on a regular basis eg. every month	96%	2%	1%	0%

Q3 The risk of financial loss

		Yes	*No*	*Don't know*	*Not Applicable*
3.1	My organisation has an anti-fraud strategy.	33%	0%	67%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.2	I know what the key elements of the strategy are.	12%	27%	57%	4%
		Yes	*No*	*Don't know*	*Not Applicable*
3.3	I only have access to the information I need to do my job	83%	11%	6%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.4	I am prevented from installing any software on my machine	83%	1%	16%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.5	I am prevented from copying software from my machine	75%	3%	22%	0%

The Council maintains a full inventory of ICT equipment. The survey question may be implying the use of security markers, for example, which is not an action taken.

		Yes	No	Don't know	Not Applicable
3.6	My computer is clearly security-marked.	78%	4%	18%	0%

		Yes	No	Don't know	Not Applicable
3.7	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	87%	4%	8%	0%

Q4 The risk of reputational damage

		Yes	*No*	*Don't know*	*Not Applicable*
4.1	I am allowed access to the internet only by connections provided by my organisation.	90%	5%	5%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.2	I have been informed that my access to the internet will be monitored.	90%	5%	5%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.3	It has been made clear to me that my organisation's policy is that accessing or storing unsuitable material is a disciplinary matter	93%	3%	3%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.4	Emails sent to me from outside my organisation that contain very large files or executable programs etc. are prevented from reaching me	65%	4%	29%	3%
		Yes	*No*	*Don't know*	*Not Applicable*
4.5	I have access to written protocols covering e-mail usage and language.	58%	10%	32%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.6	I have been informed by my organisation that the use of unlicensed software is prohibited.	81%	7%	12%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.7	I am prevented from installing software on my machine.	81%	1%	17%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.8	My organisation has a documented data protection policy	76%	0%	24%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.9	My organisation has appointed a data protection officer	37%	1%	62%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.10	I have been required to sign a confidentiality undertaking as part of my conditions of service	51%	26%	22%	1%

		Yes	*No*	*Don't know*	*Not Applicable*
4.11	My responsibilities under the Data Protection Act have been explained to me.	68%	24%	8%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.12	I have been informed that the misuse of personal data will be treated as a disciplinary offence by my organisation.	82%	12%	5%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.13	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.	25%	60%	15%	0%

Q5 I am aware of the main implications of the following legislation:

5.1	• The Computer Misuse Act	50%
5.2	• The Freedom of Information Act	83%
5.3	• The Human Rights Act	67%
5.4	• The Public Interest Disclosure Act	31%
5.5	• The Data Protection Act	95%

Q6 Loss of public or user confidence

An Information Security Policy is still in development and the council does not have a post to cover IT security.

		Yes	*No*	*Don't know*	*Not Applicable*
6.1	My organisation has an Information Security policy	38%	3%	59%	0%
		Yes	*No*	*Don't know*	*Not Applicable*
6.2	I have been provided with a copy of the policy.	14%	49%	32%	6%
		Yes	*No*	*Don't know*	*Not Applicable*
6.3	I have been informed about the policy and what I must and must not do.	22%	40%	32%	6%
		Yes	*No*	*Don't know*	*Not Applicable*
6.4	Senior management in my organisation is committed to the policy and its observance.	27%	3%	67%	3%
		Yes	*No*	*Don't know*	*Not Applicable*
6.5	I know where to find written procedures for reporting a security incident.	19%	44%	36%	1%

		Yes	*No*	*Don't know*	*Not Applicable*
6.6	Someone in my organisation is specifically responsible for IT security	55%	2%	42%	0%

ICT staff survey

Key

Good/satisfactory

Scope for improvement

Weakness identified

Q1	**Which ICT Department do you work in?**		
		Corporate ICT	100%
		Departmental ICT	0 %

Q2 The risk of business disruption

The ICT department has within it a small team whose role it is to manage any issues related to anti-virus software, email and internet access (network). Some ICT staff not involved will be unaware this process is operating seamlessly in the background.

		Yes	*No*	*Don't know*	*Not Applicable*
2.1	My organisation takes the threat of a virus infection very seriously	95.0%	0.0%	5.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.2	Our policy is to install virus protection software on all our machines	90.0%	0.0%	10.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.3	Staff are provided with regular updates to virus protection software	85.0%	5.0%	10.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.4	Staff have been given clear instructions about dealing with emailed files from external sources	68.4%	10.5%	21.1%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.5	Staff are alerted when new viruses are discovered and are advised as to what they must do	55.0%	15.0%	30.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.6	We have clear procedures in place for reporting a virus incident	35.0%	30.0%	35.0%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
2.7	Our procedures for recovering from a virus infection have been documented	30.0%	25.0%	35.0%	10.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.8	Our virus software is automatically updated by the software vendor	85.0%	0.0%	15.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.9	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	60.0%	5.0%	35.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.10	A firewall protects our networks, systems and information from intrusion from outside	85.0%	0.0%	15.0%	0.0%

The ICT department based on business need and a risk assessment do let through large files.

		Yes	*No*	*Don't know*	*Not Applicable*
2.11	Our firewall prevents large files and executable programs from reaching our networks.	55.0%	25.0%	15.0%	5.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.12	Our user registration and sign-on procedures prevent unauthorised access to our networks	90.0%	0.0%	10.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.13	Proper password management is enforced by the system on all users	95.0%	0.0%	5.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.14	Our dial-up connections are secure	75.0%	0.0%	15.0%	10.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.15	Network management staff have been appointed	80.0%	0.0%	20.0%	0.0%

There is no appointed IT security officer post but the role is presently shared by various ICT staff.

		Yes	*No*	*Don't know*	*Not Applicable*
2.16	We have appointed an IT security officer	30.0%	30.0%	40.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.17	A detailed daily log of network activity is maintained.	25.0%	20.0%	50.0%	5.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.18	Network logs are inspected periodically by network staff	40.0%	15.0%	45.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.19	Sensitive programs and information are given additional protection.	70.0%	5.0%	25.0%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
2.20	Security violations are reported to IT security staff immediately by our security systems	35.0%	15.0%	50.0%	0.0%

Web site vulnerability is tested annually due to financial constraints.

		Yes	*No*	*Don't know*	*Not Applicable*
2.21	Our web site vulnerability is checked every month	5.0%	15.0%	75.0%	5.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.22	Physical entry controls prevent unauthorised access to our IT facilities	70.0%	0.0%	30.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.23	Our servers & network equipment are sited securely and adequate protection is offered.	80.0%	0.0%	20.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.24	Any amendment to a program or system must go through our change control process	15.0%	20.0%	60.0%	5.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.25	Our change control processes are well documented	15.0%	20.0%	60.0%	5.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.26	All IT staff are trained in our change control requirements	21.1%	26.3%	42.1%	10.5%

A team ICT staff are dedicated to performing backups and users are advised to backup to servers and not desktop PCs.

		Yes	*No*	*Don't know*	*Not Applicable*
2.27	Backups of data on all servers are taken frequently.	80.0%	0.0%	20.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.28	Backup arrangements are properly documented.	70.0%	0.0%	30.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.29	User and IT staff have been trained in how to conduct backups of servers.	65.0%	15.0%	20.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.30	Monitoring of backups ensures that management is alerted when backups of remote servers do not take place	75.0%	0.0%	25.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
2.31	My organisation has a clear business continuity plan.	55.0%	0.0%	45.0%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
2.32	All staff named in the business continuity plan know of its existence and their role in it.	31.6%	5.3%	57.9%	5.3%
		Yes	*No*	*Don't know*	*Not Applicable*
2.33	Our continuity plan is based upon a robust risk analysis process	42.1%	0.0%	52.6%	5.3%

Q3 The risk of financial loss

		Yes	*No*	*Don't know*	*Not Applicable*
3.1	The systems most at risk from fraud have been identified.	44.4%	0.0%	55.6%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.2	The systems most at risk are afforded additional protection.	44.4%	0.0%	55.6%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.3	We have a documented access control policy	38.9%	11.1%	50.0%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.4	Access to systems is only provided to those who need it.	88.9%	0.0%	11.1%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.5	We have controls to prevent the copying or removal of software.	66.7%	5.6%	27.8%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.6	Hardware is clearly security-marked.	88.9%	0.0%	11.1%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
3.7	My organisation has clear rules covering private use of IT facilities and in particular what is and what isn't acceptable	83.3%	11.1%	5.6%	0.0%

Q4 The risk of reputational damage

		Yes	*No*	*Don't know*	*Not Applicable*
4.1	Staff are only allowed to access the Internet through our authorised ISP	78.9%	0.0%	21.1%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.2	Internet activity logs are reviewed by managers.	63.2%	5.3%	31.6%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.3	We bar access to internet sites we deem to be unsuitable	89.5%	0.0%	10.5%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
4.4	Our policies make it clear to all staff that the downloading or storage of unsuitable material is a disciplinary matter	89.5%	5.3%	5.3%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.5	Protocols for internet and e-mail use have been developed and are available to all users.	89.5%	0.0%	10.5%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.6	My organisation has made it clear to all staff that use of unlicensed software is prohibited.	89.5%	0.0%	10.5%	0.0%

There is no software but extensive use of Windows 'policies' is made.

		Yes	*No*	*Don't know*	*Not Applicable*
4.7	Security software that prevents the installation of any program except by authorised IT staff is installed on all PCs and laptops.	77.8%	5.6%	16.7%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.8	Users in my organisation are prevented from gaining access to system utilities.	77.8%	0.0%	22.2%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.9	Our asset register is up to date, as are all enterprise / site license numbers	52.6%	0.0%	47.4%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.10	My organisation has a documented Data Protection Policy.	68.4%	0.0%	31.6%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.11	My organisation has appointed a data protection officer.	63.2%	0.0%	36.8%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.12	All users are required to sign a confidentiality undertaking as part of their conditions of service	63.2%	10.5%	26.3%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.13	My responsibilities under the Data Protection Act have been explained to me.	57.9%	21.1%	21.1%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.14	Misuse of personal data is treated as a disciplinary offence.	63.2%	0.0%	36.8%	0.0%
		Yes	*No*	*Don't know*	*Not Applicable*
4.15	PC's are timed out after a period of inactivity	15.8%	57.9%	26.3%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
4.16	My computer has a lock out facility to be used when left unattended.	73.7%	5.3%	21.1%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
4.17	Systems containing personal data are registered with the Information Commissioner.	15.8%	5.3%	78.9%	0.0%

Q5 I am aware of the main implications of the following legislation:

5.1	The Computer Misuse Act	75.0%
5.2	The Freedom of Information Act	68.8%
5.3	The Human Rights Act	37.5%
5.4	The Public Interest Disclosure Act	25.0%
5.5	The Data Protection Act	93.8%

Q6 The risk of loss of public or user confidence

An Information Security Policy is still in development

		Yes	*No*	*Don't know*	*Not Applicable*
6.1	My organisation has an up to date Information Security policy	40.0%	5.0%	55.0%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
6.2	Staff are informed about the policy and what they must and must not do.	35.0%	10.0%	50.0%	5.0%

		Yes	*No*	*Don't know*	*Not Applicable*
6.3	Senior management is committed to the policy and its observance.	30.0%	5.0%	60.0%	5.0%

		Yes	*No*	*Don't know*	*Not Applicable*
6.4	An officer group manages the implementation of information security.	20.0%	15.0%	65.0%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
6.5	Regular independent reviews of information security are undertaken.	22.2%	11.1%	66.7%	0.0%

There are no formal plans to progress towards BS7799.

		Yes	*No*	*Don't know*	*Not Applicable*
6.6	We comply with BS7799 standards.	5.3%	10.5%	84.2%	0.0%

		Yes	*No*	*Don't know*	*Not Applicable*
6.7	There are clear written procedures for reporting and following up all security incidents.	5.0%	15.0%	80.0%	0.0%