Performance Summary Report

November 2007

Your Business @ Risk Survey

Southampton City Council

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.
- 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, 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 report

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 non-executive directors/members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any director/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.

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 of the e-agenda, the anticipated increase in the use of 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 explosion in the use of new technology is not to be matched by a similar increase in IT abuse.

2 The Audit Commission's report - Your Business @ Risk - published in 2005, concluded that though 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 new technology has not been sufficiently addressed.

3 This report summarises the results of the online self assessment survey sent to all staff in April/May 2007. The report gives details of the survey responses and sets out risks identified by the exercise. An action plan is included to address the identified risks.

Audit approach

4 The Audit Commission has developed an online self-assessment tool, which is designed to help organisations:

- 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
- facilitate positive action to reduce risks.

5 In partnership with Southampton City Council, we conducted the online self-assessment survey in April/ May 2007. Twenty seven ICT staff and 874 users responded. The questions asked and responses are included in Appendix 1.

6 The survey is being undertaken at a number of other authorities audited by the Audit Commission and where appropriate we have compared Southampton City Council's results to the national results to date.

Main conclusions

7 The overriding message from the self-assessment tool is that ICT staff and users are confident that systems, policies and procedures are generally in place to minimise IT risks. The content of responses in most areas is favourable when compared with other authorities, being at or above average.

8 Users in particular respond very favourable compared to other authorities, displaying good awareness of the processes in place at the Council.

9 There is still scope for improvement. ICT staff seem less informed and less confident in processes regarding sabotage and business continuity than comparative authorities. Confidence in the processes surrounding the potential loss of public or user confidence seems also weak for both response groups in comparison to other authorities. Work should be undertaken to maximise the knowledge of ICT staff with regards to business continuity and the Council's security procedures. Additionally, the profile information security policy should be raised and the Council should try to ensure that all staff member are aware of senior management commitment to this policy and its implemented security procedures.

10 A brief summary and commentary on the results for each section of the survey are reported in the following section.

Next steps

11 An action plan has been prepared in consultation with Council staff and is attached at Appendix 3. Implementation of the action plan should help to address the risks identified and will guide the ongoing development of IT risk management processes. The report will be presented to the Council's Audit Committee.

Risk categories

12 The self-assessment tool is based on four main risk categories which may be the consequences of IT fraud or abuse:

- business disruption;
- financial loss;
- reputational damage; and
- loss of user confidence.

13 The key issues from the survey for each of the main categories are outlined below and the detailed results are attached in Appendix 1 and 2.

Business disruption

14 The risk of business disruption was broken down into three categories: virus infection, hacking and sabotage.

Virus infection

15 The threat of a virus infection is taken very seriously by Southampton City Council according to respondents. Virus protection software is installed on machines and staff are provided with regular updates. Clear instructions are given to staff about dealing with emailed files from external sources.

16 Users feel confident in knowing how to report a virus infection, but over half of ICT staff respondents did not know if recovery procedures from virus outbreaks are documented.

17 ICT staff were also not certain about measures in place for restricting the impact of viruses; only 69 per cent either responded negatively or that they did not know such measures existed. Although this is roughly in line with other authorities' responses, it is an important procedure to the authority.

18 A total of only 5 per cent of users reported to have suffered a virus infection on their computer, which is positively higher than of comparable authorities.

19 It is important that clear and consistent procedures and measures are in place to protect the Council from the adverse affects of IT virus infection.

Recommendation
R1 Ensure awareness of the formalised procedures for recovery and virus impact procedures.

Hacking

20 Most responses in this area were either above or in line with the average for other authorities, although some procedures are still seen as weak by ICT staff.

21 User respondents confirmed that there are proper user registration and sign-on procedures which prevent unauthorised access to the Council's networks. Though 34 per cent of users responded that they do not have to remember more than two passwords to access computers. This was particularly visible in the Chief Executive's and the Health, Care and Communities departments. This could increase the risk of unauthorised access. ICT staff felt generally very confident about the enforcement of password procedures, which is favourable against the trend of comparable authorities.

22 Firewall protection of systems is in place and prevents large files and executable programs from reaching internal networks.

23 Security of dial-up connections received an above average response from ICT staff as 63 per cent stated they were secure compared with 56 per cent nationally.

24 Only 33 per cent of ICT staff responded positively when asked if an IT security officer had been appointed, with 33 per cent responding negatively and 33 per cent lack awareness.

25 Over half of ICT staff did not know or thought that no daily log of network activity is maintained and 46 per cent thought that website vulnerability was not checked every month.

26 ICT staff's awareness of network log procedures and protection of sensitive programmes were low, but still in line with comparative authorities. This could be reviewed by the Council in order to ensure awareness of procedures is high with relevant staff members.

27 Only 3 per cent of ICT staff responded positively when asked if web site vulnerability is checked every month, suggesting very low awareness or the absence of relevant procedures in this area.

28 Increasing awareness of the ICT security officer and network security procedures amongst ICT staff would have a positive impact on the overall systems security.

Recommendations	
R2	*Increase awareness of the role and responsibilities of the ICT security officer.*
R3	*Review web site vulnerability procedures and ensure ICT staff are made aware of such processes.*

Sabotage

29 Some responses in this area were below average when compared with other authorities, although change control and backup processes are carried out appropriately, as identified by ICT staff.

30 An above national average of 96 per cent of ICT staff stated that any amendment to a program or system must go through a change control process and 84 per cent responded that change procedures are well documented. On the other hand, only half of respondents felt that staff were trained in change control procedures.

31 Although backups of data are taken regularly, as 92 per cent responded positively und 44 per cent thought the process was documented properly and even less (37 per cent) felt they had been trained appropriately in the relevant procedures.

32 Continuity plan awareness amongst ICT staff seems particularly weak. Only 22 per cent of respondents knew that a plan exists; this is far below the national average of 41 per cent. Additionally, only 15 per cent responded that staff named in the business continuity plan did know of its existence and their role in it and only 11 per cent believed that the plan was based upon robust risk analysis processes.

33 An increase in the awareness of documented back up procedures and raising the profile and awareness of business continuity plans and procedures would lessen the Council's risk in this area.

Recommendations	
R4	*Increase awareness and training of backup and control change procedures.*
R5	*Raise the profile and increase awareness of the business continuity plans and procedures.*

Financial loss

34 Risks relating to financial loss were broken down into two categories; financial loss as a result of fraud and as a result of theft and private work.

Fraud

35 All responses to this area were above the average for other authorities.

36 ICT staff stated that the systems most at risk of fraud have been identified and that those systems have been afforded additional protection and that vulnerable systems were afforded additional protection

37 There is scope for improvement. Although 40 per cent of users were aware of the anti-fraud strategy, only 16 per cent knew of the key elements within it. This is still in line with comparative authorities' average but indicates a national lack of awareness of organisational anti-fraud strategies. The responses were particularly negative in the departments: Chief Executive's, Health, Care and Communities, Environment. Councillors on the other hand seemed much better informed.

38 An increase in the awareness of anti-fraud policies and procedures would lessen the Council's risk in this area.

Recommendation
R6 Increase staff awareness regarding anti-fraud policies and procedures.

Theft and private work

39 Most responses to this area are in line with the average for other authorities.

40 Seventy three per cent of users stated that they were prevented from copying software from their machines, however, 78 per cent of ICT staff thought that either no controls were in place to prevent this or that they were not aware of any.

41 The majority of users stated that their computer was clearly security marked and knew what the authorities rules are for private use of IT facilities. Ninety one per cent of user respondents knew that private use of IT facilities was covered in the organisational rules, which was slightly above national average of 88 per cent.

Reputational damage

42 The risks relating to reputational damage were broken down into four categories; accessing unsuitable material, using unlicensed software, misuse of personal data and breach of the law.

Accessing unsuitable material

43 A large majority of respondents were clear that their access to the internet would be monitored and that the accessing or storing of unsuitable material was a disciplinary matter. Respondents were less clear about whether externally sent e-mails are ever prevented from reaching them, though this was in line with the national average.

44 Most of the respondents also had access to written protocols covering e-mail usage and language.

45 All ICT staff stated that internet activity logs are reviewed by managers. This is double the national average. ICT staff respondents also all agreed that policies and protocols for internet usage to staff are clear.

46 ICT staff seemed unaware that internet activity logs are reviewed by managers, as only 15 per cent responded that they knew such procedures existed.

47 Generally, the positive responses for this section are far above average in comparison to other authorities and this shows good practice from the Council.

Unlicensed software

48 The majority of respondents have been informed that the use of unlicensed software is prohibited and that users cannot gain access to system utilities.

49 The lack of awareness from both ICT staff and users with regards to whether Internal Audit reviews software on individual's machines is in line with national average and reflects the feeling that this knowledge might not be required for all staff members.

50 Only 23 per cent of ICT staff thought that the asset register and enterprise/ site licence numbers are up to date. The review of the asset register would lessen the risk of running unlicensed software on the Council's systems.

Recommendation
R7 Review the asset register and the software inventory records.

Misuse of personal data

51 Awareness of the Data Protection policy and the Data Protection Officer amongst users and ICT staff is good, when compared to other authorities.

52 Only 54 per cent of ICT staff responded that a confidentiality undertaking had to be signed and only 42 per cent of users responded that they were required to do so. Particularly in the Environment and Neighbourhoods departments as well as with Councillors the response rate of users who did not know if they were required to sign, was very high in comparison to other authorities. This should be part of every employee's terms and condition and does therefore not pose an immediate risk to the misuse of data but awareness of its existence especially amongst ICT staff should be increased.

53 The majority of staff were aware of their responsibilities under the Data Protection Act and knew that misuse of personal data was a disciplinary offence.

Breach of the law

54 The majority of respondents were aware of the implications of The Freedom of Information Act, The Human Rights Act and The Data Protection Act.

55 Forty nine per cent of users were aware of the implications of The Computer Misuse Act and only 35 per cent knew of the implications of the Public Interest Disclosure Act.

56 Although these figures seem to suggest low awareness, all responses were above the average for other authorities.

Loss of public or user confidence

57 Most of the user responses in this area were in line or above the average for other authorities; ICT staff responses reflected a rather negative view in this area.

58 The majority of respondents are aware of the Information Security policy, although only 19 per cent of users felt that they had been provided with a copy and 33 per cent knew their responsibilities and what it was about. This was in line with the comparative authorities. There are, however, still a significant number of staff who don't know about the policy or its contents.

59 Fifty seven per cent of users knew that there was someone within the organisation with specific responsibility for IT security. However, less than 40 per cent of users knew where to find written procedures for reporting a security incident.

60 Twenty two per cent of ICT staff and 40 per cent of user respondents think that senior management is committed to the Information Security policy.

61 Only 12 per cent of ICT staff believed that the Council complies with BS7799 standards which provide assurance of information system security arrangements and only 22 per cent were aware that an officer group manages the implementation of information security. This is far below average in comparison to other authorities.

62 Additionally, only 15 per cent of ICT staff respondents think that regular independent reviews of information security are undertaken.

63 The general lack of confidence and awareness of ICT staff in this area poses a risk in this area. Raising the profile and awareness of the management of information security would increase user confidence in the security of the Council's systems.

Recommendation
R8 Increase the profile and awareness of the management of information security.

Appendix 1 – Detailed survey results (staff)

Your.Business@Risk

ICT Staff Survey

Q1 Which ICT Department do you work in?

Corporate ICT	96.3%
Departmental ICT	3.7%

Q2 The risk of business disruption

	Yes	*No*	*Don't know*	*Not Applicable*
My organisation takes the threat of a virus infection very seriously	100.0%	0.0%	0.0%	0.0%
Our policy is to install virus protection software on all our machines	100.0%	0.0%	0.0%	0.0%
Staff are provided with regular updates to virus protection software	96.3%	3.7%	0.0%	0.0%
Staff have been given clear instructions about dealing with emailed files from external sources	85.2%	14.8%	0.0%	0.0%
Staff are alerted when new viruses are discovered and are advised as to what they must do	66.7%	25.9%	3.7%	3.7%
We have clear procedures in place for reporting a virus incident	70.4%	11.1%	18.5%	0.0%
Our procedures for recovering from a virus infection have been documented	29.6%	14.8%	55.6%	0.0%
Our virus software is automatically updated by the software vendor	80.0%	0.0%	20.0%	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	30.8%	7.7%	61.5%	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.	81.5%	11.1%	7.4%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*

Our user registration and sign-on procedures prevent unauthorised access to our networks	88.5%	7.7%	3.8%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Proper password management is enforced by the system on all users	92.6%	7.4%	0.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Our dial-up connections are secure	63.0%	7.4%	25.9%	3.7%
	Yes	*No*	*Don't know*	*Not Applicable*
Network management staff have been appointed	88.9%	0.0%	11.1%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
We have appointed an IT security officer	33.3%	33.3%	33.3%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
A detailed daily log of network activity is maintained.	33.3%	14.8%	51.9%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Network logs are inspected periodically by network staff	29.6%	7.4%	63.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Sensitive programs and information are given additional protection.	61.5%	3.8%	34.6%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Security violations are reported to IT security staff immediately by our security systems	51.9%	7.4%	40.7%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Our web site vulnerability is checked every month	3.7%	22.2%	74.1%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Physical entry controls prevent unauthorised access to our IT facilities	88.5%	3.8%	7.7%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Our servers & network equipment are sited securely and adequate protection is offered.	96.3%	0.0%	3.7%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Our internal procedures minimise the risk of deliberate damage by employees leaving the organisation	33.3%	33.3%	33.3%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Any amendment to a program or system must go through our change control process	96.3%	3.7%	0.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Our change control processes are well documented	84.6%	11.5%	3.8%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
All IT staff are trained in our change control requirements	50.0%	42.3%	7.7%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Backups of data on all servers are taken frequently.	92.3%	7.7%	0.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*

Backup arrangements are properly documented.	44.4%	14.8%	40.7%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
User and IT staff have been trained in how to conduct backups of servers.	37.0%	11.1%	48.1%	3.7%
	Yes	*No*	*Don't know*	*Not Applicable*
Monitoring of backups ensures that management is alerted when backups of remote servers do not take place	63.0%	7.4%	29.6%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has a clear business continuity plan.	22.2%	29.6%	48.1%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
All staff named in the business continuity plan know of its existence and their role in it.	14.8%	22.2%	59.3%	3.7%
	Yes	*No*	*Don't know*	*Not Applicable*
Our continuity plan is based upon a robust risk analysis process	11.1%	22.2%	66.7%	0.0%

Q3 The risk of financial loss

	Yes	*No*	*Don't know*	*Not Applicable*
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*
The systems most at risk are afforded additional protection.	37.0%	7.4%	51.9%	3.7%
	Yes	*No*	*Don't know*	*Not Applicable*
We have a documented access control policy	51.9%	7.4%	40.7%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Access to systems is only provided to those who need it.	84.6%	11.5%	3.8%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
We have controls to prevent the copying or removal of software.	22.2%	22.2%	55.6%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Hardware is clearly security-marked.	63.0%	22.2%	14.8%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has clear rules covering private use of IT facilities and in particular what is and what isn't acceptable	92.6%	0.0%	7.4%	0.0%

Q4 The risk of reputational damage

	Yes	*No*	*Don't know*	*Not Applicable*
Staff are only allowed to access the Internet through our authorised ISP	88.9%	11.1%	0.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Internet activity logs are reviewed by managers.	14.8%	33.3%	51.9%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
We bar access to internet sites we deem to be unsuitable	100.0%	0.0%	0.0%	0.0%

	Yes	*No*	*Don't know*	*Not Applicable*
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%
	Yes	*No*	*Don't know*	*Not Applicable*
Protocols for internet and e-mail use have been developed and are available to all users.	96.3%	3.7%	0.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has made it clear to all staff that use of unlicensed software is prohibited.	81.5%	11.1%	7.4%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Security software that prevents the installation of any program except by authorised IT staff is installed on all PCs and laptops.	59.3%	18.5%	22.2%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Our Internal Auditors undertake reviews of software on users' PCs.	18.5%	25.9%	55.6%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Users in my organisation are prevented from gaining access to system utilities.	81.5%	11.1%	7.4%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Our asset register is up to date, as are all enterprise / site license numbers	23.1%	26.9%	50.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has a documented Data Protection Policy.	74.1%	11.1%	14.8%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has appointed a data protection officer.	59.3%	11.1%	29.6%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
All users are required to sign a confidentiality undertaking as part of their conditions of service	53.8%	26.9%	19.2%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
My responsibilities under the Data Protection Act have been explained to me.	55.6%	44.4%	0.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Misuse of personal data is treated as a disciplinary offence.	66.7%	7.4%	25.9%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
PC's are timed out after a period of inactivity	70.4%	14.8%	14.8%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
My computer has a lock out facility to be used when left unattended.	88.9%	3.7%	7.4%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Systems containing personal data are registered with the Information Commissioner.	33.3%	3.7%	63.0%	0.0%

Q5	I am aware of the main implications of the following legislation:	
	· *The Computer Misuse Act*	84.0%
	· *The Freedom of Information Act*	88.0%
	· *The Human Rights Act*	60.0%
	· *The Public Interest Disclosure Act*	44.0%
	· *The Data Protection Act*	92.0%

Q6	The risk of loss of public or user confidence			
	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has an up to date Information Security policy	55.6%	14.8%	29.6%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Staff are informed about the policy and what they must and must not do.	40.7%	22.2%	37.0%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Senior management is committed to the policy and its observance.	22.2%	22.2%	51.9%	3.7%
	Yes	*No*	*Don't know*	*Not Applicable*
An officer group manages the implementation of information security.	22.2%	22.2%	55.6%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
Regular independent reviews of information security are undertaken.	15.4%	23.1%	61.5%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
We comply with BS7799 standards.	11.5%	23.1%	65.4%	0.0%
	Yes	*No*	*Don't know*	*Not Applicable*
There are clear written procedures for reporting and following up all security incidents.	22.2%	18.5%	59.3%	0.0%

Appendix 2 – Detailed survey results (users)

Your.Business@Risk

User Survey

Q1 Which Department do you work in?

Department 1	7%
Department 2	27%
Department 3	17%
Department 4	10%
Department 5	23%
Department 6	15%
Department 7	1%
Department 8	0%
Department 9	0%

Q2 The risk of business disruption

	Yes	*No*	*Don't know*	*Not Applicable*
My organisation takes the threat of a virus infection very seriously	92%	1%	8%	0%
Virus protection software is installed on my machine	92%	0%	7%	1%
Virus protection software is regularly updated on my machine	73%	0%	26%	1%
I have been given clear instructions about dealing with emailed files from external sources	74%	18%	8%	0%
I am sent an alert when new viruses are discovered and am told what to do and what not to do	56%	19%	22%	3%
I know how to report a virus infection if I suffer an infection on my machine	74%	17%	8%	1%
I have suffered a virus infection on my machine	5%	85%	9%	2%
Whenever I have suffered a virus infection, my machine was cleansed and restored quickly	6%	2%	11%	82%
To log on to my machine I must enter a user name and password	97%	2%	0%	1%

To log on to my organisation's network I must enter a user name and password	94%	3%	2%	1%
	Yes	*No*	*Don't know*	*Not Applicable*
I am forced to change my password by the system on a regular basis eg. every month	92%	7%	1%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
To access the computers and systems I use to do my job I must remember more than 2 passwords	65%	34%	0%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I have not written my password(s) down	70%	29%	0%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I am not authorised to enter our computer rooms	42%	14%	30%	14%

Q3 **The risk of financial loss**

	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has an anti-fraud strategy.	40%	0%	59%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I know what the key elements of the strategy are.	16%	34%	46%	4%
	Yes	*No*	*Don't know*	*Not Applicable*
I only have access to the information I need to do my job	79%	14%	7%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I am prevented from installing any software on my machine	73%	8%	18%	1%
	Yes	*No*	*Don't know*	*Not Applicable*
I am prevented from copying software from my machine	66%	5%	28%	1%
	Yes	*No*	*Don't know*	*Not Applicable*
My computer is clearly security-marked.	79%	5%	16%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
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	91%	3%	6%	0%

Q4 **The risk of reputational damage**

	Yes	*No*	*Don't know*	*Not Applicable*
I am allowed access to the internet only by connections provided by my organisation.	93%	3%	4%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I have been informed that my access to the internet will be monitored.	84%	10%	6%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
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%
	Yes	*No*	*Don't know*	*Not Applicable*

Emails sent to me from outside my organisation that contain very large files or executable programs etc. are prevented from reaching me	59%	5%	35%	1%
	Yes	*No*	*Don't know*	*Not Applicable*
I have access to written protocols covering e-mail usage and language.	83%	3%	14%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I have been informed by my organisation that the use of unlicensed software is prohibited.	87%	4%	8%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I am prevented from installing software on my machine.	72%	6%	19%	2%
	Yes	*No*	*Don't know*	*Not Applicable*
Internal Auditors or IT staff in my organisation have checked the software on my machine.	46%	5%	48%	1%
	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has a documented data protection policy	85%	0%	14%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has appointed a data protection officer	52%	1%	47%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I have been required to sign a confidentiality undertaking as part of my conditions of service	42%	30%	27%	1%
	Yes	*No*	*Don't know*	*Not Applicable*
My responsibilities under the Data Protection Act have been explained to me.	74%	18%	7%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I have been informed that the misuse of personal data will be treated as a disciplinary offence by my organisation.	87%	8%	4%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
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.	88%	10%	2%	1%

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

• *The Computer Misuse Act*	49%
• *The Freedom of Information Act*	95%
• *The Human Rights Act*	68%
• *The Public Interest Disclosure Act*	35%
• *The Data Protection Act*	95%

Q6 **Loss of public or user confidence**

	Yes	*No*	*Don't know*	*Not Applicable*
My organisation has an Information Security policy	52%	1%	47%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
I have been provided with a copy of the policy.	19%	46%	31%	3%
	Yes	*No*	*Don't know*	*Not Applicable*

I have been informed about the policy and what I must and must not do.	33%	33%	31%	3%
	Yes	*No*	*Don't know*	*Not Applicable*
Senior management in my organisation is committed to the policy and its observance.	40%	1%	57%	2%
	Yes	*No*	*Don't know*	*Not Applicable*
I know where to find written procedures for reporting a security incident.	38%	35%	27%	0%
	Yes	*No*	*Don't know*	*Not Applicable*
Someone in my organisation is specifically responsible for IT security	57%	3%	40%	0%

Appendix 3 – Action plan

Page no.	Recommendation	Priority: Low/Med/ High	Responsibility	Agreed	Comments	Date to be completed
6	R1 Ensure awareness among ICT staff of the formalised procedures for recovery and virus impact procedures.	Med	IT Strategy & Planning Group	Yes	The ICT staff who are responsible for recovery after a major virus incident are very aware of the recovery procedures. However, some of our ICT staff cannot be considered to be 'technical' and therefore may not be aware that such procedures exist. We will produce a short document that informs ICT staff of the existence of the virus recovery procedures, with links to the full document, and circulate it to all ICT staff through our monthly Team Brief. This will raise awareness of the procedures' existence.	End of September 2007
7	R2 Increase awareness among ICT staff of the role and responsibilities of the ICT security officer.	Med	IT Strategy & Planning Group	Yes	Southampton City Council does not have an ICT Security Officer post. Instead, the responsibility for the role resides within the IT Strategy and Planning Group. We publicised this fact to ICT staff through our monthly Team Brief in July 2007. We will re-emphasise where the ICT Security role exists within ITS by including another article in our monthly Team Brief.	End of September 2007

Page no.	Recommendation	Priority: Low/Med/ High	Responsibility	Agreed	Comments	Date to be completed
7	R3 Review web site vulnerability procedures and ensure ICT staff are made aware of such processes.	Med	IT Strategy & Planning Group	Yes	Our Web team have deployed SecureSphere which checks for website vulnerabilities on a daily basis. Staff within the Web team are therefore aware of our procedures in this respect. However, other ICT staff may not be aware of our daily vulnerability checking. We will produce a short document that informs ICT staff of the existence of SecureSphere and what it does, and will circulate it through our monthly Team Brief.	End of September 2007
8	R4 Increase awareness and training of backup and control change procedures among ICT staff.	Med	Service Delivery Group	Yes	We are currently reviewing our Back Up and Change Control procedures to align them both with ITIL. When they have been finalised, we will add them to our ICT web pages and then publicise them to all ICT staff through the monthly Team Brief.	End of September 2007
8	R5 Raise the profile and increase awareness of the business continuity plans and procedures among ICT staff.	Med	IT Strategy & Planning Group	Yes	Our Business Continuity Plans are updated annually and are held on a shared drive to which all ICT staff have access. We will produce a short document that informs ICT staff about the current Business Continuity Plan and will publicise it to all ICT Staff through our monthly Team Brief.	End of September 2007
9	R6 Increase awareness of all staff regarding anti-fraud policies and procedures.	Med	Chief Internal Auditor/Head of HR	Yes	The anti-fraud policies and procedures have been revised and approved by the Audit Committee. Staff are being informed through a number of mechanisms including Team Brief and Management/Staff Training.	End of October 2007

Page no.	Recommendation	Priority: Low/Med/ High	Responsibility	Agreed	Comments	Date to be completed
10	R7 Review the asset register and the software inventory records.	Med	Service Delivery Group	Yes	Our asset register and software inventory records have recently been audited in preparation for the imminent strategic services partnership with Capita. We will inform ICT staff of this through our monthly Team Brief. We can use Microsoft SMS to remotely interrogate users' desktops to determine what software is installed.	End of September 2007
11	R8 Increase the profile and awareness of the management of information security among ICT staff.	Med	IT Strategy & Planning Group	Yes	We have had an Information Security Policy in place for some years which is based on BS7799. We are working towards compliance with this standard. We will combine this recommendation with recommendation 2 above which seeks to raise awareness of the role of IT Security Officer. Since June 2007, independent reviews of our network security have been carried out by a PCI approved external tester. The next test is due to take place in September. We will produce a short document to inform ICT staff that our security measures are regularly tested and will publicise it through our monthly Team Brief.	End of September 2007