Your Business @ Risk

Bromsgrove District Council

Audit 2008-2009

audit commission

Contents

Introduction

1 Your Business at Risk (YB@R) is a web-based survey that helps auditors and public sector organisations to focus on the business risks associated with information and communications technology (ICT). The survey is part of a portfolio of tools developed by the Audit Commission's Good Conduct and Counter Fraud and IT Knowledge Networks.

2 The Graham Committee report on the Standards of Conduct in Public Life endorsed these tools and recommended that they be used throughout the whole of the public sector.

3 Despite improvements in the percentages of organisations which have developed ICT security policies (for example), recent national studies have shown that as few as 20 per cent of staff have actually been provided with a copy and only 33 per cent have been informed about the policy and its implications for them. This has been accompanied by a significant increase in the inappropriate use of the internet and email, virus infections continuing to pose a huge risk and widespread ICT fraud still being committed resulting in financial loss and reputational damage.

4 The existence of policies and procedures is not enough. Examining how well policies and procedures are embedded is necessary to gain assurance that they are effective.

5 The YB@R web based survey helps organisations and auditors to focus on business risks such as major business disruption, reputational damage, financial loss and the erosion of user confidence in technology.

6 Using the assessment tool has a number of benefits in terms of; gauging the levels of IT awareness among staff; providing the ability to measure improvement over time; and highlight areas where you may need to improve governance and reduce risk.

Audit approach

7 This audit takes the form of two web based surveys. One is aimed at users of ICT, and the other at ICT staff. These are issued to authorities and Trusts for internal circulation to relevant groups of staff, for them to complete within an agreed timeframe.

8 The results are then collated and a summary report issued. Recommendations are made as appropriate and presented in the relevant sections of the main conclusions and in an action plan as an appendix.

Main conclusions

9 Following examination and collation of the survey results, the main conclusions which can be drawn are set out below.

10 Overall the response to each survey was good. For the ICT users survey there were 67 responses (from a total of 287 active users) - representing 23 per cent of users. For the ICT staff survey there were 6 responses from a total of 11 IT department members, representing 54 per cent of ICT staff. The surveys were carried out between 26 July and 8 August 2008 inclusive, but it was necessary to extend this period until the 12 September 2008 due to a relatively low initial response.

The risk of business disruption

11 All ICT users responding said that they were forced to enter a user name and password to log on, and that their passwords were compulsorily changed every month. Ninety per cent of ICT users reported that Virus protection software is installed on their machines. Forty-six per cent did not know whether it was regularly updated. Only 3 per cent reported that they had actually suffered a virus infection on their machine.

12 Twenty-two per cent of ICT users said that they did not know whether the organisation takes the threat of a virus infection very seriously.

13 Twenty-seven per cent said they had not been given clear instructions about dealing with emailed files from external sources, and this was compounded by 14 per cent who responded that they didn't know, indicating that they too were unaware of how to deal with files from external sources. Only half of the respondents to the ICT staff survey said that users had been given clear instructions about dealing with emailed files from external sources.

14 Forty-two per cent of users said that they were not sent an alert when new viruses are discovered and are not told what to do and what not to do, with only 35 per cent saying that they were alerted and told what to do. Only 50 per cent of ICT staff responding said that users are alerted when new viruses are discovered and are advised as to what they must do.

15 An overwhelming 82 per cent of ICT user respondents said that they had to remember more than two passwords to access the systems needed for them to do their jobs. Under these circumstances there is a high risk that passwords will be written down and left next to terminals, and 36 per cent of users reported that this was the case. ICT staff appear either unaware or in denial over this because all of them who responded said that user registration and sign-on procedures prevent unauthorised access to networks. This suggests that the risk highlighted by the numbers of users reporting that they write their passwords down has not yet been accepted by ICT staff.

16 In terms of physical security, there are further issues of awareness in that there were 27 per cent of ICT user survey respondents who said that they did not know that they were not authorised to enter computer rooms.

17 Amongst IT staff, there were issues of awareness around the organisations arrangements for Business Continuity Planning (BCP). Only a third of responding IT staff said that there was a clear BCP, that there was awareness amongst staff named within it of its existence and their role in it, or that it is based upon a robust risk analysis process.

Recommendation

R1 The Council should take action to ensure that the risk of business disruption due to IT failure is minimise by:

- conducting an awareness raising exercise highlighting the threats associated with computer virus infection;
- issue clear instructions to all staff about dealing with emailed files from external sources;
- issue clear guidance to staff on what to do in the event of a computer virus outbreak;
- issue password good practice guidance to reinforce with staff that they should not be writing passwords down;
- reduce wherever possible, the number of passwords required for staff to log in to their systems;
- raise awareness of physical access controls covering computer rooms; and
- conduct an awareness raising exercise covering the Councils' BCP, clarifying roles and responsibilities.

18 The expected benefit of this recommendation is:

- minimisation of the risk of business disruption due to IT failure.

The implementation of this recommendation will have a high impact with low cost. It should be implemented by [TBA].

The risk of financial loss

19 Information access controls appear appropriately set, with 85 per cent of ICT user respondents reporting that they only have access to the information needed to do their jobs. Eight-eight per cent also reported that they were prevented from installing software on their machines, and 75 per cent that they were prevented from copying software from their machines. There was also a good degree of awareness (at 87 per cent) of the organisation's rules covering private use of IT facilities.

20 Twenty-two per cent of ICT user respondents said that they didn't know whether the Council has an anti-fraud strategy. Only 17 per cent of IT staff responding said that the systems most at risk from fraud have been identified.

21 Whilst 78 per cent of respondents were aware that there is an anti fraud strategy, 52 per cent were unaware of what the key elements of the strategy were.

Recommendation
R2 Reduce the risk of financial loss due to fraud by: • conducting an awareness raising exercise covering the Councils anti fraud strategy; and • identify which systems are most at risk form fraud, ensuring that these are adequately protected.

22 The expected benefit of this recommendation is:

- the reduction of the Councils' exposure to risk due to IT related fraud.

The implementation of this recommendation will have a high impact with low cost. It should be implemented by [TBA].

The risk of reputational damage

23 There are appropriate levels of control covering access to the Internet with 92 per cent of ICT users reporting that access to the internet is only available via connections provided by the Council. Users are also made aware that access to the internet is be monitored with 82 per cent reporting that this is the case. Eighty-eight per cent of users are also aware that the Councils' policy is that accessing or storing unsuitable material is a disciplinary matter. However, only 16 per cent of IT staff responding said that Internet activity logs are reviewed by managers.

24 The majority of users (75 per cent) were aware that emails from outside the Council that contain very large files or executable programs are prevented from reaching them. General awareness of protocols covering email usage was good with 76 per cent of respondents reporting that they had access to written protocols covering email usage and language.

25 Use of unlicensed software and controls on the users' ability to install their own software are also well in place.

26 There was poor awareness as to whether software installations are audited or checked (45 per cent of responding users and 16 per cent of IT staff), and of whether there is an appointed data protection officer (65 per cent). However, the majority of users said that they had had responsibilities under the Data Protection Act explained to them, and that they had been informed that the misuse of personal data will be treated as a disciplinary offence.

27 Eighty-three per cent of responding IT staff said that they did not know whether systems containing personal data are registered with the Information Commissioner.

Recommendation
R3 The Council should reduce the risk of reputational damage due to IT systems abuse by: • implementing periodic reviews of Internet access logs by managers; • conducting and awareness raising exercise highlighting arrangements for auditing software installations; and • raising the profile of the Councils' data protection arrangements, and the responsibilities of all staff in this area.

28 The expected benefit of this recommendation is:

- the reduction of the Councils' exposure to the risk of reputational damage resulting from the abuse of its IT systems.

The implementation of this recommendation will have a high impact with low cost. It should be implemented by [TBA].

Awareness of Legislation

29 Reported levels of awareness of the Freedom on information Act (86 per cent) and the Data Protection Acts (97 per cent) were good. However, there is work to be done in raising awareness of the following legislation.

- The Computer Misuse Act (35 per cent awareness).
- The Human Rights Act (59 per cent awareness).
- The Public Interest Disclosure Act (29 per cent awareness)

Recommendation
R4 The Council should raise awareness of key legislation, specifically: • The Computer Misuse Act; • The Human Rights Act; and • The Public Interest Disclosure Act.

30 The expected benefit of this recommendation is:

- the raised awareness amongst Council staff of their responsibilities under the above acts, and the subsequent reduction of risk of non compliance.

The implementation of this recommendation will have a high impact with low cost. It should be implemented by [TBA].

Risk of Loss of public or user confidence

31 Forty-five per cent of ICT users reported that they were aware of an Information Security policy, with only 29 per cent saying that they had been provided with a copy. Only a third said that they had been informed about the policy and what they must and must not do. Only 32 per cent of ICT user respondents felt that senior management is committed to the policy and its observance, and only 34 per cent said that they were aware of where to find written procedures for reporting a security incident. To compound this, only half of responding IT staff said that there is an up to date Information Security policy.

32 Only 47 per cent of ICT users expressed awareness of someone within the Council with specific responsibility for IT security. Amongst IT staff, there was also a lack of awareness of IT security arrangements with only 17 per cent expressing awareness of who manages the implementation of information security, zero awareness of information security reviews, low (17 per cent) awareness of compliance with IT security standards and written procedures for reporting and following up all security incidents.

Recommendation

R5 The Council should reduce the risk of loss of public or user confidence by:

- conducting an awareness raising exercise covering staff responsibilities under the Councils' information security policy; and
- raising appropriate awareness of IT security standards, management arrangements, and reviews amongst all Council staff.

33 The expected benefit of this recommendation is:

- reduction of risk exposure relating to loss of public or user confidence in the Councils ability to control access to information and IT systems.

The implementation of this recommendation will have a high impact with low cost. It should be implemented by [TBA].

Appendix 1 – Survey Responses

The full results of the surveys are set out below in terms of percentages of respondents.

User Survey				
The risk of business disruption				
My organisation takes the threat of a virus infection very seriously	Yes 77%	No 0%	Don't know 22%	Not Applicable 2%
Virus protection software is installed on my machine	Yes 90%	No 0%	Don't know 10%	Not Applicable 0%
Virus protection software is regularly updated on my machine	Yes 54%	No 0%	Don't know 46%	Not Applicable 0%
I have been given clear instructions about dealing with emailed files from external sources	Yes 58%	No 27%	Don't know 14%	Not Applicable 2%
I am sent an alert when new viruses are discovered and am told what to do and what not to do	Yes 35%	No 42%	Don't know 20%	Not Applicable 3%
I know how to report a virus infection if I suffer an infection on my machine	Yes 78%	No 17%	Don't know 3%	Not Applicable 2%
I have suffered a virus infection on my machine	Yes 3%	No 78%	Don't know 13%	Not Applicable 5%
Whenever I have suffered a virus infection, my machine was cleansed and restored quickly	Yes 5%	No 2%	Don't know 16%	Not Applicable 78%
To log on to my machine I must enter a user name and password	Yes 100%	No 0%	Don't know 0%	Not Applicable 0%
To log on to my organisation's network I must enter a user name and password	Yes 75%	No 22%	Don't know 3%	Not Applicable 0%

Appendix 1 – Survey Responses

The risk of business disruption				
I am forced to change my password by the system on a regular basis eg. every month	Yes 100%	No 0%	Don't know 0%	Not Applicable 0%
To access the computers and systems I use to do my job I must remember more than 2 passwords	Yes 82%	No 18%	Don't know 0%	Not Applicable 0%
I have not written my password(s) down	Yes 64%	No 36%	Don't know 0%	Not Applicable 0%
I am not authorised to enter our computer rooms	Yes 34%	No 31%	Don't know 27%	Not Applicable 8%

The risk of financial loss				
My organisation has an anti-fraud strategy.	Yes 78%	No 0%	Don't know 22%	Not Applicable 0%
I know what the key elements of the strategy are.	Yes 45%	No 30%	Don't know 22%	Not Applicable 3%
I only have access to the information I need to do my job	Yes 85%	No 10%	Don't know 3%	Not Applicable 2%
I am prevented from installing any software on my machine	Yes 88%	No 2%	Don't know 10%	Not Applicable 0%
I am prevented from copying software from my machine	Yes 75%	No 0%	Don't know 25%	Not Applicable 0%
My computer is clearly security-marked.	Yes 83%	No 0%	Don't know 17%	Not Applicable 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	Yes 87%	No 5%	Don't know 8%	Not Applicable 0%

The risk of reputational damage				
I am allowed access to the internet only by connections provided by my organisation.	Yes 92%	No 3%	Don't know 5%	Not Applicable 0%
I have been informed that my access to the internet will be monitored.	Yes 82%	No 10%	Don't know 8%	Not Applicable 0%
It has been made clear to me that my organisation's policy is that accessing or storing unsuitable material is a disciplinary matter	Yes 88%	No 10%	Don't know 2%	Not Applicable 0%
Emails sent to me from outside my organisation that contain very large files or executable programs etc. are prevented from reaching me	Yes 75%	No 5%	Don't know 20%	Not Applicable 0%
I have access to written protocols covering email usage and language.	Yes 76%	No 8%	Don't know 15%	Not Applicable 0%
I have been informed by my organisation that the use of unlicensed software is prohibited.	Yes 80%	No 10%	Don't know 8%	Not Applicable 2%
I am prevented from installing software on my machine.	Yes 88%	No 0%	Don't know 12%	Not Applicable 0%
Internal Auditors or IT staff in my organisation have checked the software on my machine.	Yes 45%	No 2%	Don't know 53%	Not Applicable 0%
My organisation has a documented data protection policy	Yes 81%	No 0%	Don't know 19%	Not Applicable 0%
My organisation has appointed a data protection officer	Yes 65%	No 0%	Don't know 35%	Not Applicable 0%

Appendix 1 – Survey Responses

The risk of reputational damage				
I have been required to sign a confidentiality undertaking as part of my conditions of service	Yes 40%	No 28%	Don't know 27%	Not Applicable 5%
My responsibilities under the Data Protection Act have been explained to me.	Yes 75%	No 18%	Don't know 7%	Not Applicable 0%
I have been informed that the misuse of personal data will be treated as a disciplinary offence by my organisation.	Yes 83%	No 13%	Don't know 3%	Not Applicable 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.	Yes 42%	No 45%	Don't know 13%	Not Applicable 0%

I am aware of the main implications of the following legislation:	
The Computer Misuse Act	35%
The Freedom of Information Act	90%
The Human Rights Act	59%
The Public Interest Disclosure Act	29%
The Data Protection Act	98%

Loss of public or user confidence				
My organisation has an Information Security policy	Yes 45%	No 0%	Don't know 55%	Not Applicable 0%
I have been provided with a copy of the policy.	Yes 25%	No 40%	Don't know 30%	Not Applicable 5%
I have been informed about the policy and what I must and must not do.	Yes 33%	No 32%	Don't know 32%	Not Applicable 3%
Senior management in my organisation is committed to the policy and its observance.	Yes 32%	No 0%	Don't know 67%	Not Applicable 2%

Loss of public or user confidence				
I know where to find written procedures for reporting a security incident.	Yes 34%	No 37%	Don't know 29%	Not Applicable 0%
Someone in my organisation is specifically responsible for IT security	Yes 47%	No 0%	Don't know 53%	Not Applicable 0%

ICT Staff Survey

The risk of business disruption				
My organisation takes the threat of a virus infection very seriously	Yes 100.0%	No 0.0%	Don't know 0.0%	Not Applicable 0.0%
Our policy is to install virus protection software on all our machines	Yes 100.0%	No 0.0%	Don't know 0.0%	Not Applicable 0.0%
Staff are provided with regular updates to virus protection software	Yes 100.0%	No 0.0%	Don't know 0.0%	Not Applicable 0.0%
Staff have been given clear instructions about dealing with emailed files from external sources	Yes 50.0%	No 16.7%	Don't know 33.3%	Not Applicable 0.0%
Staff are alerted when new viruses are discovered and are advised as to what they must do	Yes 50.0%	No 33.3%	Don't know 16.7%	Not Applicable 0.0%
We have clear procedures in place for reporting a virus incident	Yes 66.7%	No 33.3%	Don't know 0.0%	Not Applicable 0.0%
Our procedures for recovering from a virus infection have been documented	Yes 16.7%	No 66.7%	Don't know 16.7%	Not Applicable 0.0%
Our virus software is automatically updated by the software vendor	Yes 66.7%	No 16.7%	Don't know 16.7%	Not Applicable 0.0%

The risk of business disruption				
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	Yes 20.0%	No 40.0%	Don't know 40.0%	Not Applicable 0.0%
A firewall protects our networks, systems and information from intrusion from outside	Yes 100.0%	No 0.0%	Don't know 0.0%	Not Applicable 0.0%
Our firewall prevents large files and executable programs from reaching our networks.	Yes 66.7%	No 16.7%	Don't know 0.0%	Not Applicable 16.7%
Our user registration and sign-on procedures prevent unauthorised access to our networks	Yes 100.0%	No 0.0%	Don't know 0.0%	Not Applicable 0.0%
Proper password management is enforced by the system on all users	Yes 83.3%	No 0.0%	Don't know 16.7%	Not Applicable 0.0%
Our dial-up connections are secure	Yes 83.3%	No 0.0%	Don't know 16.7%	Not Applicable 0.0%
Network management staff have been appointed	Yes 83.3%	No 0.0%	Don't know 16.7%	Not Applicable 0.0%
We have appointed an IT security officer	Yes 20.0%	No 40.0%	Don't know 40.0%	Not Applicable 0.0%
A detailed daily log of network activity is maintained.	Yes 50.0%	No 33.3%	Don't know 16.7%	Not Applicable 0.0%
Network logs are inspected periodically by network staff	Yes 50.0%	No 33.3%	Don't know 16.7%	Not Applicable 0.0%
Sensitive programs and information are given additional protection.	Yes 50.0%	No 33.3%	Don't know 16.7%	Not Applicable 0.0%
Security violations are reported to IT security staff immediately by our security systems	Yes 83.3%	No 0.0%	Don't know 16.7%	Not Applicable 0.0%

The risk of business disruption				
Our web site vulnerability is checked every month	Yes 33.3%	No 0.0%	Don't know 66.7%	Not Applicable 0.0%
Physical entry controls prevent unauthorised access to our IT facilities	Yes 66.7%	No 33.3%	Don't know 0.0%	Not Applicable 0.0%
Our servers & network equipment are sited securely and adequate protection is offered.	Yes 83.3%	No 0.0%	Don't know 16.7%	Not Applicable 0.0%
Our internal procedures minimise the risk of deliberate damage by employees leaving the organisation	Yes 66.7%	No 0.0%	Don't know 33.3%	Not Applicable 0.0%
Any amendment to a program or system must go through our change control process	Yes 50.0%	No 16.7%	Don't know 33.3%	Not Applicable 0.0%
Our change control processes are well documented	Yes 33.3%	No 33.3%	Don't know 33.3%	Not Applicable 0.0%
All IT staff are trained in our change control requirements	Yes 33.3%	No 16.7%	Don't know 50.0%	Not Applicable 0.0%
Backups of data on all servers are taken frequently.	Yes 100.0%	No 0.0%	Don't know 0.0%	Not Applicable 0.0%
Backup arrangements are properly documented.	Yes 50.0%	No 16.7%	Don't know 33.3%	Not Applicable 0.0%
User and IT staff have been trained in how to conduct backups of servers.	Yes 66.7%	No 0.0%	Don't know 33.3%	Not Applicable 0.0%
Monitoring of backups ensures that management is alerted when backups of remote servers do not take place	Yes 100.0%	No 0.0%	Don't know 0.0%	Not Applicable 0.0%
My organisation has a clear business continuity plan.	Yes 33.3%	No 33.3%	Don't know 33.3%	Not Applicable 0.0%

Appendix 1 – Survey Responses

The risk of business disruption				
	Yes	No	Don't know	Not Applicable
All staff named in the business continuity plan know of its existence and their role in it.	33.3%	16.7%	50.0%	0.0%
	Yes	No	Don't know	Not Applicable
Our continuity plan is based upon a robust risk analysis process	33.3%	33.3%	33.3%	0.0%

The risk of financial loss				
	Yes	No	Don't know	Not Applicable
The systems most at risk from fraud have been identified.	16.7%	16.7%	66.7%	0.0%
	Yes	No	Don't know	Not Applicable
The systems most at risk are afforded additional protection.	33.3%	33.3%	33.3%	0.0%
	Yes	No	Don't know	Not Applicable
We have a documented access control policy	33.3%	66.7%	0.0%	0.0%
	Yes	No	Don't know	Not Applicable
Access to systems is only provided to those who need it.	50.0%	16.7%	33.3%	0.0%
	Yes	No	Don't know	Not Applicable
We have controls to prevent the copying or removal of software.	50.0%	16.7%	16.7%	16.7%
	Yes	No	Don't know	Not Applicable
Hardware is clearly security-marked.	66.7%	16.7%	16.7%	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	83.3%	0.0%	16.7%	0.0%

The risk of reputational damage				
	Yes	No	Don't know	Not Applicable
Staff are only allowed to access the Internet through our authorised ISP	83.3%	0.0%	16.7%	0.0%
	Yes	No	Don't know	Not Applicable
Internet activity logs are reviewed by managers.	16.7%	16.7%	66.7%	0.0%
	Yes	No	Don't know	Not Applicable
We bar access to internet sites we deem to be unsuitable	83.3%	0.0%	16.7%	0.0%

The risk of reputational damage				
	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	66.7%	0.0%	33.3%	0.0%
	Yes	No	Don't know	Not Applicable
Protocols for internet and email use have been developed and are available to all users.	83.3%	16.7%	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.	50.0%	0.0%	50.0%	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.	83.3%	16.7%	0.0%	0.0%
	Yes	No	Don't know	Not Applicable
Our Internal Auditors undertake reviews of software on users' PCs.	16.7%	33.3%	50.0%	0.0%
	Yes	No	Don't know	Not Applicable
Users in my organisation are prevented from gaining access to system utilities.	83.3%	16.7%	0.0%	0.0%
	Yes	No	Don't know	Not Applicable
Our asset register is up to date, as are all enterprise / site license numbers	33.3%	33.3%	33.3%	0.0%
	Yes	No	Don't know	Not Applicable
My organisation has a documented Data Protection Policy.	60.0%	20.0%	20.0%	0.0%
	Yes	No	Don't know	Not Applicable
My organisation has appointed a data protection officer.	60.0%	0.0%	40.0%	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	16.7%	50.0%	33.3%	0.0%
	Yes	No	Don't know	Not Applicable
My responsibilities under the Data Protection Act have been explained to me.	50.0%	50.0%	0.0%	0.0%

The risk of reputational damage				
Misuse of personal data is treated as a disciplinary offence.	Yes 66.7%	No 0.0%	Don't know 33.3%	Not Applicable 0.0%
PC's are timed out after a period of inactivity	Yes 60.0%	No 20.0%	Don't know 20.0%	Not Applicable 0.0%
My computer has a lock out facility to be used when left unattended.	Yes 83.3%	No 0.0%	Don't know 16.7%	Not Applicable 0.0%
Systems containing personal data are registered with the Information Commissioner.	Yes 0.0%	No 16.7%	Don't know 83.3%	Not Applicable 0.0%

I am aware of the main implications of the following legislation:	
The Computer Misuse Act	100.0%
The Freedom of Information Act	100.0%
The Human Rights Act	60.0%
The Public Interest Disclosure Act	20.0%
The Data Protection Act	100.0%

The risk of loss of public or user confidence				
My organisation has an up to date Information Security policy	Yes 50.0%	No 0.0%	Don't know 50.0%	Not Applicable 0.0%
Staff are informed about the policy and what they must and must not do.	Yes 50.0%	No 16.7%	Don't know 33.3%	Not Applicable 0.0%
Senior management is committed to the policy and its observance.	Yes 50.0%	No 0.0%	Don't know 50.0%	Not Applicable 0.0%
An officer group manages the implementation of information security.	Yes 16.7%	No 16.7%	Don't know 66.7%	Not Applicable 0.0%
Regular independent reviews of information security are undertaken.	Yes 0.0%	No 33.3%	Don't know 66.7%	Not Applicable 0.0%

The risk of loss of public or user confidence				
	Yes	No	Don't know	Not Applicable
We comply with BS7799 standards.	16.7%	16.7%	66.7%	0.0%
	Yes	No	Don't know	Not Applicable
There are clear written procedures for reporting and following up all security incidents.	16.7%	33.3%	50.0%	0.0%

Appendix 2 – Action Plan

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
6	R1 The Council should take action to ensure that the risk of business disruption due to IT failure is minimise by: • conducting an awareness raising exercise highlighting the threats associated with computer virus infection; • issue clear instructions to all staff about dealing with emailed files from external sources; • issue clear guidance to staff on what to do in the event of a computer virus outbreak; • issue password good practice guidance to reinforce with staff that they should not be writing passwords down; • reduce *wherever possible*, the number of passwords required for staff to log in to their systems; • raise awareness of physical access controls covering computer rooms; and • conduct an awareness raising exercise covering the Councils' BCP, clarifying roles and responsibilities.	3	Head of E-Gov and Customer Service Head of E-Gov and Customer Service Head of E-Gov and Customer Service Head of E-Gov and Customer Service Head of E-Gov and Customer Service Head of E-Gov and Customer Service Director of Partnerships and Projects	Y Y Y N N Y	Council to issue an e-connect (all council employee email) and include section on the intranet to raise awareness of computer virus protection Council to issue an e-connect (all council employee email) and include section on the intranet to explain how to deal with external files – Council anti-virus system does stop all external mail which potentially carry viruses Council to issue an e-connect (all council employee email) and include section on the intranet to raise security of passwords issue. To have one single password is deemed as being less secure than having a couple of passwords to remember – some systems force a particular method of password set up. Staff have entry into the main ICT office (where staff sit for support etc) – access to the server is restricted using a secure electronic key system. To request Director issues e-connect once procedure in place	December 2008

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
7	R2 Reduce the risk of financial loss due to fraud by: • conducting an awareness raising exercise covering the Councils anti fraud strategy; and • identify which systems are most at risk form fraud, ensuring that these are adequately protected.	3	Head of Financial Services	Y N	To include awareness of the anti fraud strategy in the next quarterly fraud newsletter. Picked up as part of the internal audit risk assessment during the annual plan development.	December 2008
8	R3 The Council should reduce the risk of reputational damage due to IT systems abuse by: • implementing periodic reviews of Internet access logs by managers; • conducting and awareness raising exercise highlighting arrangements for auditing software installations; and • raising the profile of the Councils' data protection arrangements, and the responsibilities of all staff in this area.	3	Head of E-Government and Customer Services	Y N Y	To produce monthly reports for HOS to detail internet access by staff. Staff do not have the function on their system to install software – this has to be installed via ICT department. To issue E-connect and to include on the intranet section on data protection and staff responsibilities	December 2008 January 2009
8	R4 The Council should raise awareness of key legislation, specifically: • The Computer Misuse Act; • The Human Rights Act; and • The Public Interest Disclosure Act.	2	Head of Financial Services	Y	To issue E-connect and to include on the intranet section key legislation for staff to be made aware of	January 2009

Appendix 2 – Action Plan

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
9	R5 The Council should reduce the risk of loss of public or user confidence by: • conducting an awareness raising exercise covering staff responsibilities under the Councils' information security policy; and • raising appropriate awareness of IT security standards, management arrangements, and reviews amongst all Council staff.	2	Head of E-Government and Customer Services	Y Y	To issue E-connect and to include on the intranet section on security of information and staff responsibilities To issue E-connect and to include on the intranet section on security standards and management arrangements	January 2009 January 2009

The Audit Commission

The Audit Commission is an independent watchdog, driving economy, efficiency and effectiveness in local public services to deliver better outcomes for everyone.

Our work across local government, health, housing, community safety and fire and rescue services means that we have a unique perspective. We promote value for money for taxpayers, covering the £180 billion spent by 11,000 local public bodies.

As a force for improvement, we work in partnership to assess local public services and make practical recommendations for promoting a better quality of life for local people.

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