AUDIT COMMITTEE

Committee Report

PORTFOLIO AREA: FINANCE & PERFORMANCE MANAGEMENT

Date of Meeting: **18 April 2007**

Public

Key Decision: **No** **Recorded in Forward Plan:** **No**

Inside Policy Framework

Title: **Your Business At Risk – Audit Commission Report**
Report of: **Director of Corporate Services**
Report reference: **CORP13/07**

Summary:

This report contains an assessment carried out by the Audit Commission on the Council's awareness to, and preparedness to respond to, the risk posed to its Information and Business computer systems.

Recommendations:

The Audit Committee is asked to receive the report and make appropriate comment.

Contact Officer: John Nutley **Ext:** x7250

CITY OF CARLISLE

To: The Chairman and Members of the Audit Committee
18 April 2007

CORP13/07

YOUR BUSINESS AT RISK – AUDIT COMMISSION REPORT

1. BACKGROUND INFORMATION AND OPTIONS

i. The Audit Commission issued a paper in 2005 called "YB@R" or Your Business at Risk. The purpose of this paper was to alert public bodies of the risk new technology pose to organisations.

ii. In this report notice was served that they intended a future assessment against the points that were raised.

iii. In January of this year the Audit Commission, in conjunction with the ICT Unit, conducted an on-line survey to carry out that assessment. The results of the survey are presented in Appendix 1.

iv. It is pleasing to note that the arrangements the ICT Unit has put in place around the Council's ICT facilities and services have scored "above average".

v. However, there is no room for complacency and although overall scoring well, the report has noted some areas for improvement. The full details are carried in the report

vi. An Action Plan to address these has been developed and is shown in Appendix 2. The actions proposed will be agreed with the Audit Commission in follow up meetings.

2. RECOMMENDATIONS

The Audit Committee is asked to receive the report and make appropriate comment.

3. IMPLICATIONS

- Staffing/Resources – None
- Financial – None
- Legal – None
- Corporate
- Risk Management – No new risks are introduced by approving the statement
- Equality Issues – None
- Environmental – None
- Crime and Disorder – None

ANGELA BROWN
Director of Corporate Services

Contact Officer: John Nutley Ext: 7250

Appendix 2 – Provisional Action Plan

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
5	R1 Implement forced password changes on the network and applications in line with ISO27001. (was BS7799)	3	Network & Infrastructure Manager		An assessment of the apropriateness of this recommendation will be carried out during the formulation of the new Council ICT Security Policy	
5	R2 Raise awareness of the email policy amongst users.	3	Network & Infrastructure Manager	Y	A programme will be developed to remind all existing users and new starters of the importance of this policy	
5	R3 Ensure that all IT Staff have a clear understanding of Change Control Procedures.	3	Head of ICT	Y	The implementation of the ITIL standard for ICT operation will ensure that this takes place	
5	R4 Improve awareness for all staff on the anti-fraud strategy.	3	Head of ICT		Further investigation into this recommendation is required	
5	R5 Ensure that PCs are set up to prevent the installation and copying of software and raise awareness of the risks to all users.	3	Network & Infrastructure Manager	Y	This will be incorporated into the Council's new ICT Security Policy	
5	R6 Ensure that all users have read, understood and signed a confidentiality agreement.	3	Head of ICT		Subject to dicussion with HR	
5	R7 Check PCs to ensure they are set to time out after a short period of inactivity	3	Network & Infrastructure	Y	This will be incorporated into the Council's new ICT Security Policy	

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
			Manager			
5	R8 Increase IT legislation awareness through improved induction and ongoing training programmes.	3	Head of ICT		Subject to discussion with HR & Information Manager	
5	R9 Develop and issue an Information Security policy.	3	Head of ICT		Subject to discussion with Information Manager	
5	R10 Develop procedures for reporting IT security incidents.	3	Network & Infrastructure Manager	Y	The implementation of the ITIL standard for ICT operation will ensure that this takes place	

Audit Summary Report

24th January 2007

Last saved: 14/02/2007 14:36:00

Your Business at Risk Survey

Carlisle City 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 Carlisle City Council, we ran the above online survey in January 2007. 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 where results are better than the national average and identify any areas of significant weakness where further action is necessary.

Main findings and conclusions

5 Our conclusions are based upon responses from 163 users and 7 ICT staff from a total of approximately 600 council employees requested to take part in the survey. Overall, the results are better than average and concerns are mostly around the lack of robust password management and the need to raise awareness of the guidance which is available. The Commission's national database currently contains almost 15,000 responses from around 80 public sector organisations. These results however do not mean that improvements cannot be made at Carlisle.

6 The survey has highlighted gaps amongst IT staff with regard to the Change Control procedures as well as the lack of a security policy. Due to the small sample size and with the outcomes reported as percentages, a single adverse reply to any question results in a variation of 14.3 per cent and this should be taken into consideration in reviewing the responses.

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 Information security policy;
- security on individual PCs;
- promoting the anti-fraud strategy; and
- knowledge of key areas of relevant legislation.

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

Recommendations

Recommendations	
R1	*Implement forced password changes on the network and applications in line with ISO27001. (was BS7799)*
R2	*Raise awareness of the email policy amongst users.*
R3	*Ensure that all IT Staff have a clear understanding of Change Control Procedures.*
R4	*Improve awareness for all staff on the anti-fraud strategy.*
R5	*Ensure that PCs are set up to prevent the installation and copying of software and raise awareness of the risks to all users.*
R6	*Ensure that all users have read, understood and signed a confidentiality agreement.*
R7	*Check PCs to ensure they are set to time out after a short period of inactivity*
R8	*Increase IT legislation awareness through improved induction and ongoing training programmes.*
R9	*Develop and issue an Information Security policy.*
R10	*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.

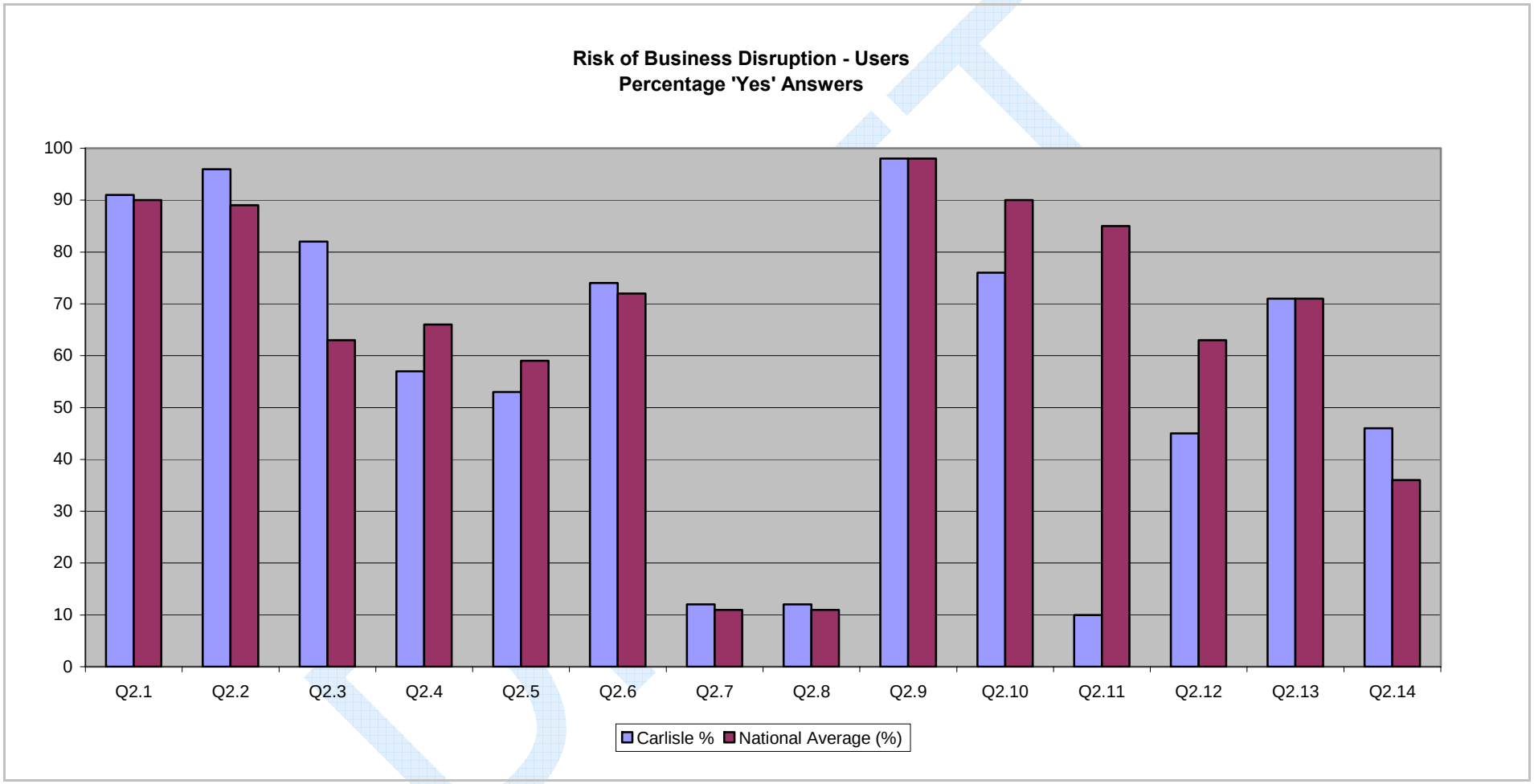
Table 1 Key messages

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**
Most users and IT staff think the council takes the threat of virus infection very seriously and are aware that virus protection is installed on their machine and regularly updated. IT staff were confident that they all knew how to conduct backups on the servers, and that these were regular and properly documented.	Only 10% of users are forced to change their passwords regularly compared to the national average of 85%. In addition only 42.9% of IT staff feel that proper password management is enforced by the system on all users. A weak area highlighted in the survey by ICT staff, reinforced by users, is that staff have not been given clear instruction about dealing with emailed files from external sources. IT staff were not clear about Change Control Procedures, responses were below the national average.	Implement forced password changes on the network and applications in line with ISO27001. (was BS7799) Raise awareness of the security and email policies amongst users. Ensure that all IT Staff have a clear understanding of Change Control Procedures.

Risk of business disruption (users)

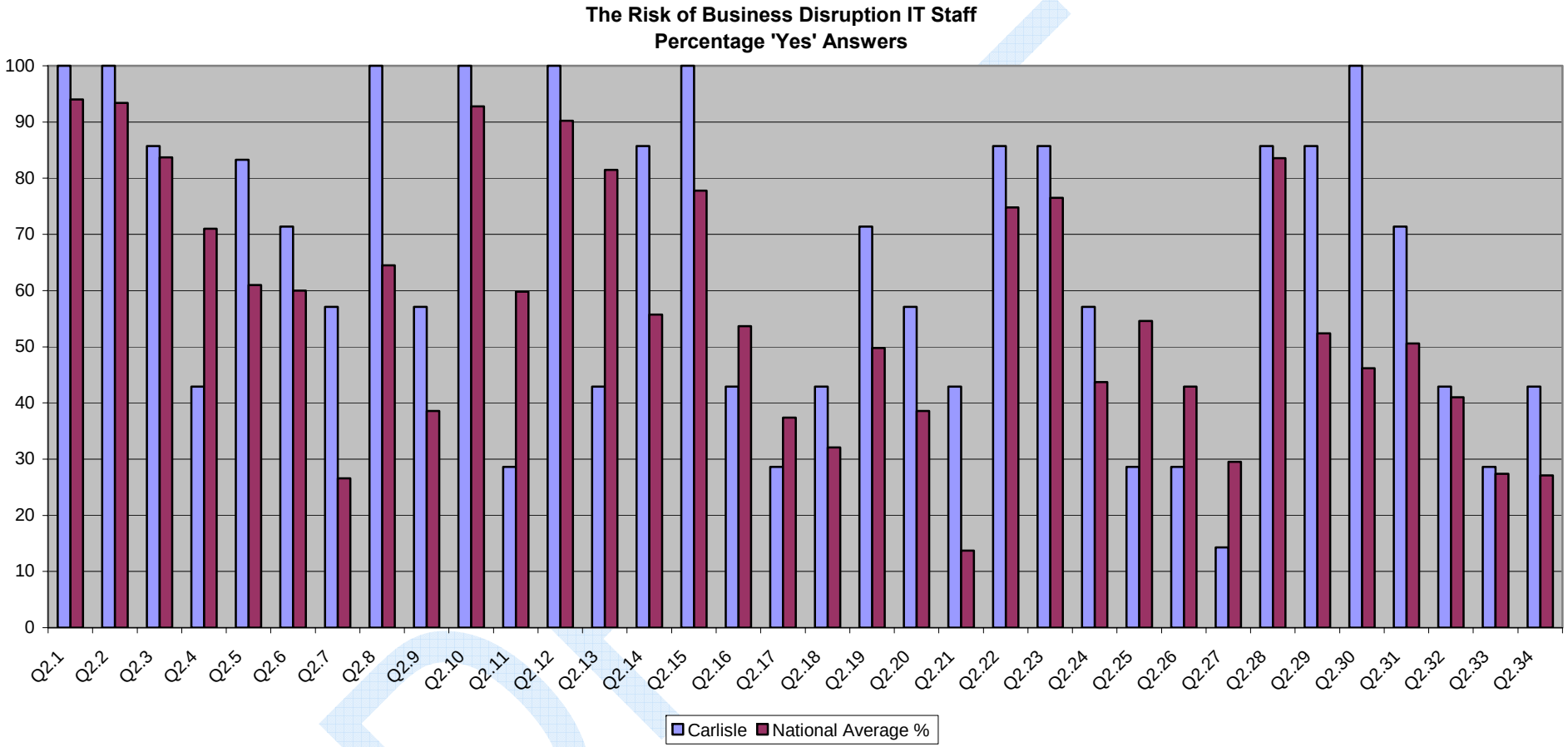
Results for council versus national results



Source: YB@R: Audit Commission

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

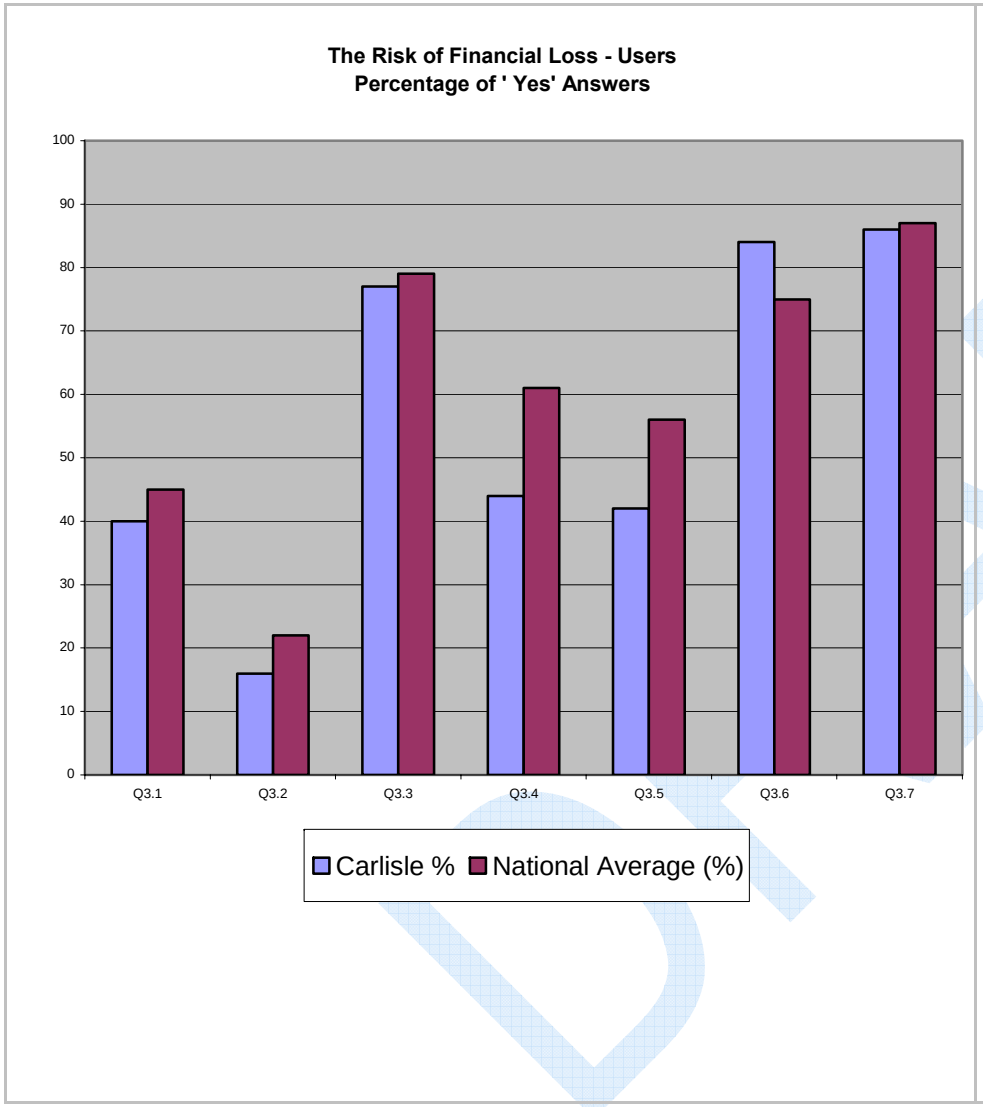
Figure 1 ICT staff results: risk of business disruption

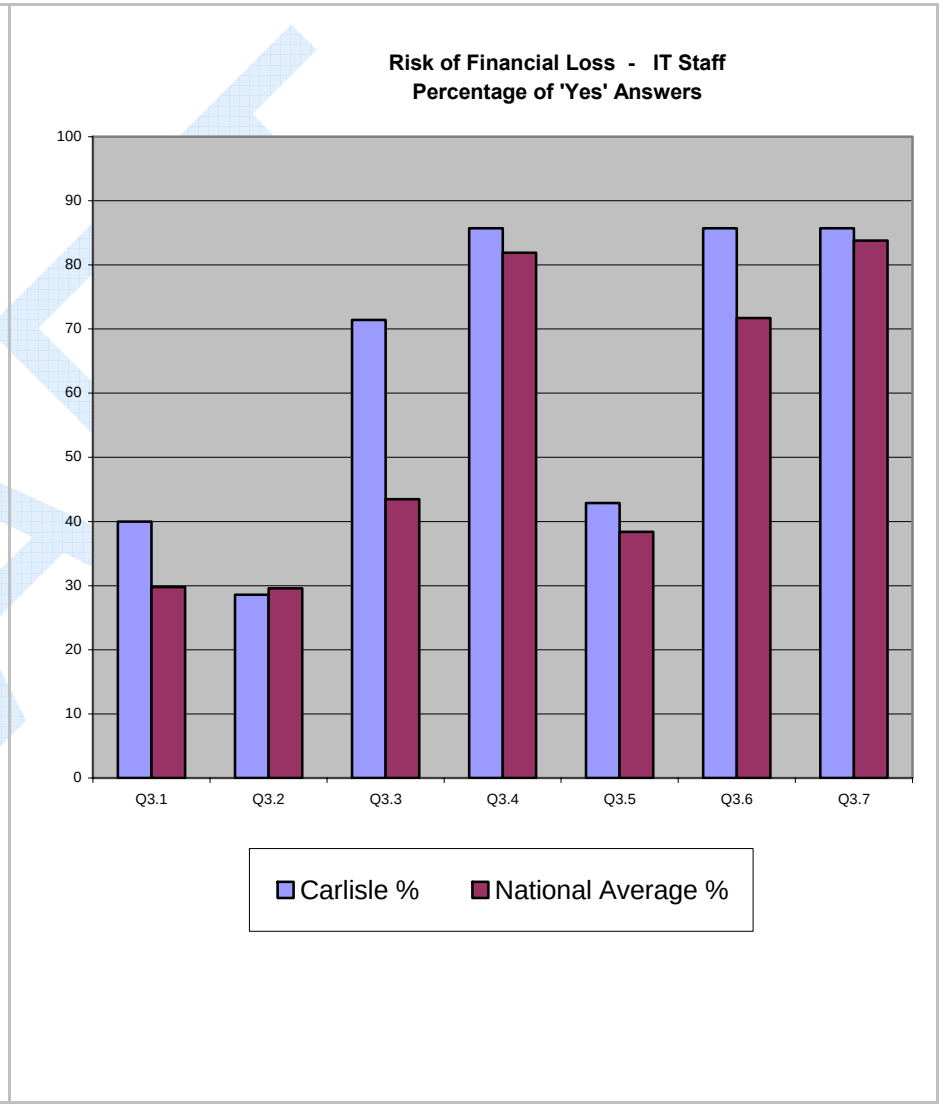


Source: YB@R: Audit Commission

Financial loss risk		
Positive messages	**Areas requiring attention**	**Suggested action**
A high percentage of IT staff (71.4%) said there was a documented Access Control Policy compared with a national average of 43.5%. Both users and IT staff indicated that hardware was clearly marked. Both users and IT staff were aware of the rules governing private use of IT facilities. .	Approximately 59 per cent of user respondents are not aware of the existence or content of the council's anti-fraud strategy. Only 44% of users think that they are prevented from installing software on their machines and only 42% say they are prevented from copying software from their machines.	Improve awareness for all staff on the anti-fraud strategy. Ensure that PCs are set up to prevent the installation and copying of software and raise awareness of the risks to all users.

Risk of financial loss Council versus national results





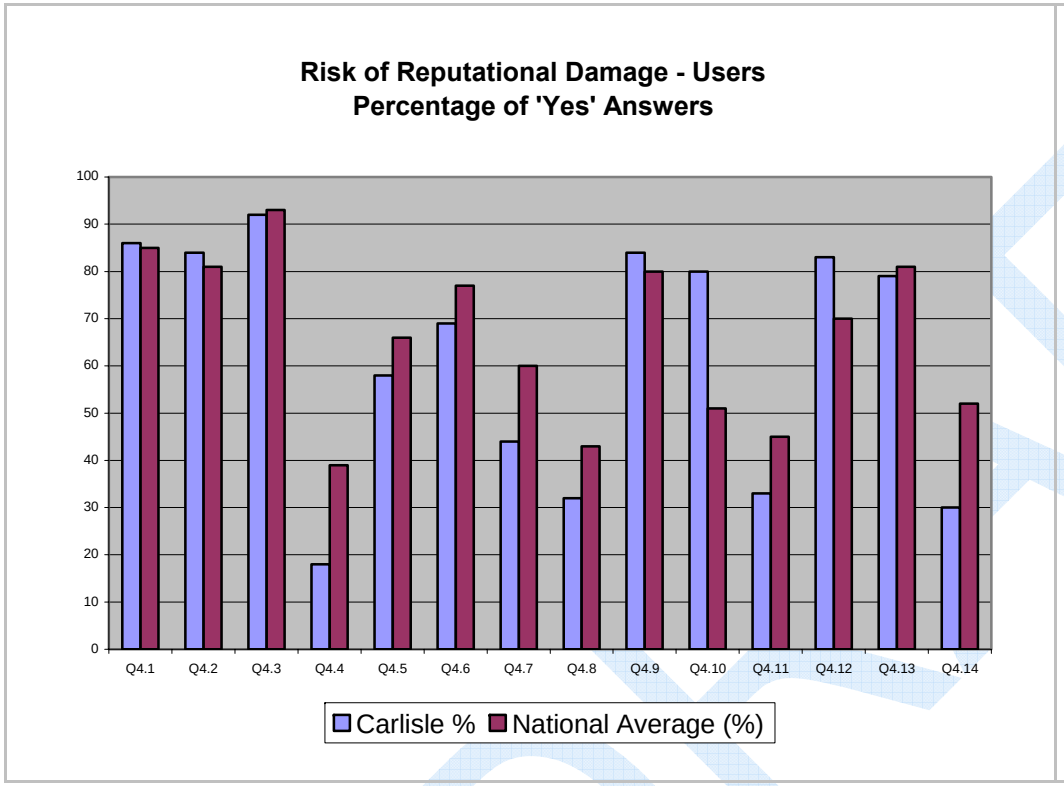
Source: YB@R: Audit Commission

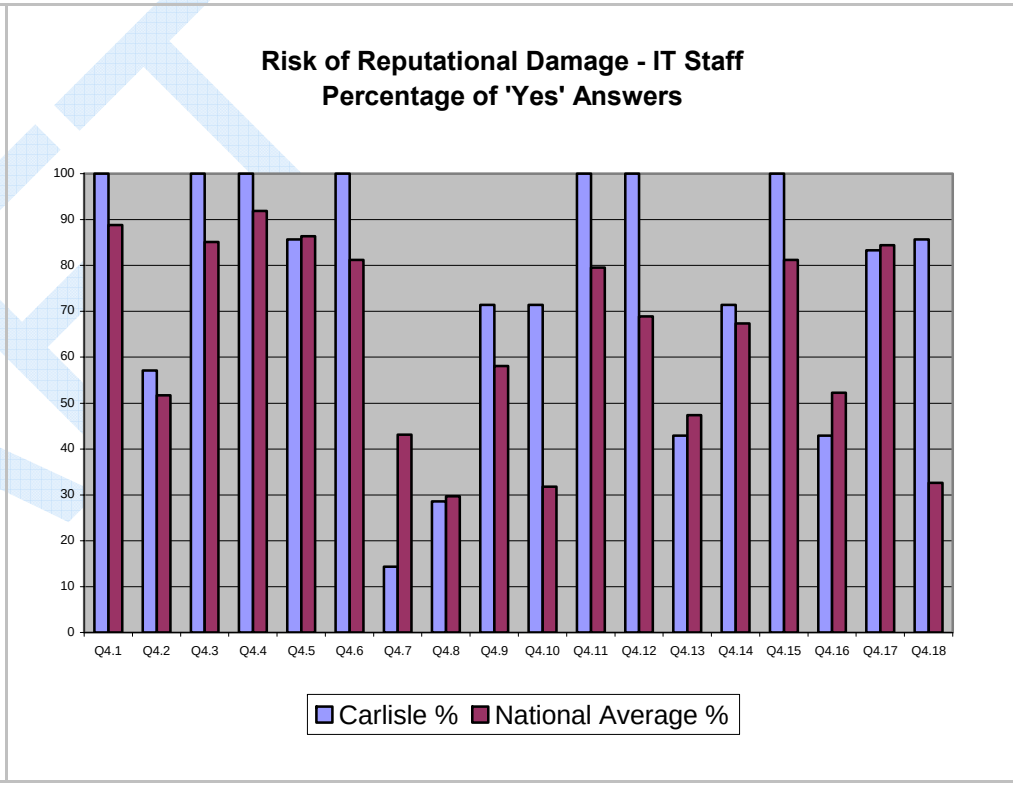
Carlisle City Council

Reputational damage risk		
Positive messages	**Areas requiring attention**	**Suggested action**
100% of IT staff know the rules regarding access to the internet, and what cannot be looked at or downloaded. They are also aware of the data protection policy and that there is a data protection officer. They are clear that misuse of personal data is a disciplinary offence and that unlicenced software is prohibited. This is above the national average. Over 80% of users are aware of the data protection act and have had it explained, they are also aware of the existence of the data protection officer. Users are also clear about the internet usage policy.	Both users and IT staff indicate that there is nothing to stop them installing software on their PCs. Only 33% of users have signed a confidentiality agreement. Users are not aware that large files and executable programmes, emailed to them may not reach them due to security. 62% of users said that their PCs do not time out after a short period of inactivity	See R5 above Ensure that all users have read, understood and signed a confidentiality agreement. See R2 above Check PCs to ensure they are set to time out after a short period of inactivity

Figure 2 Risk of reputational damage

Council versus national results



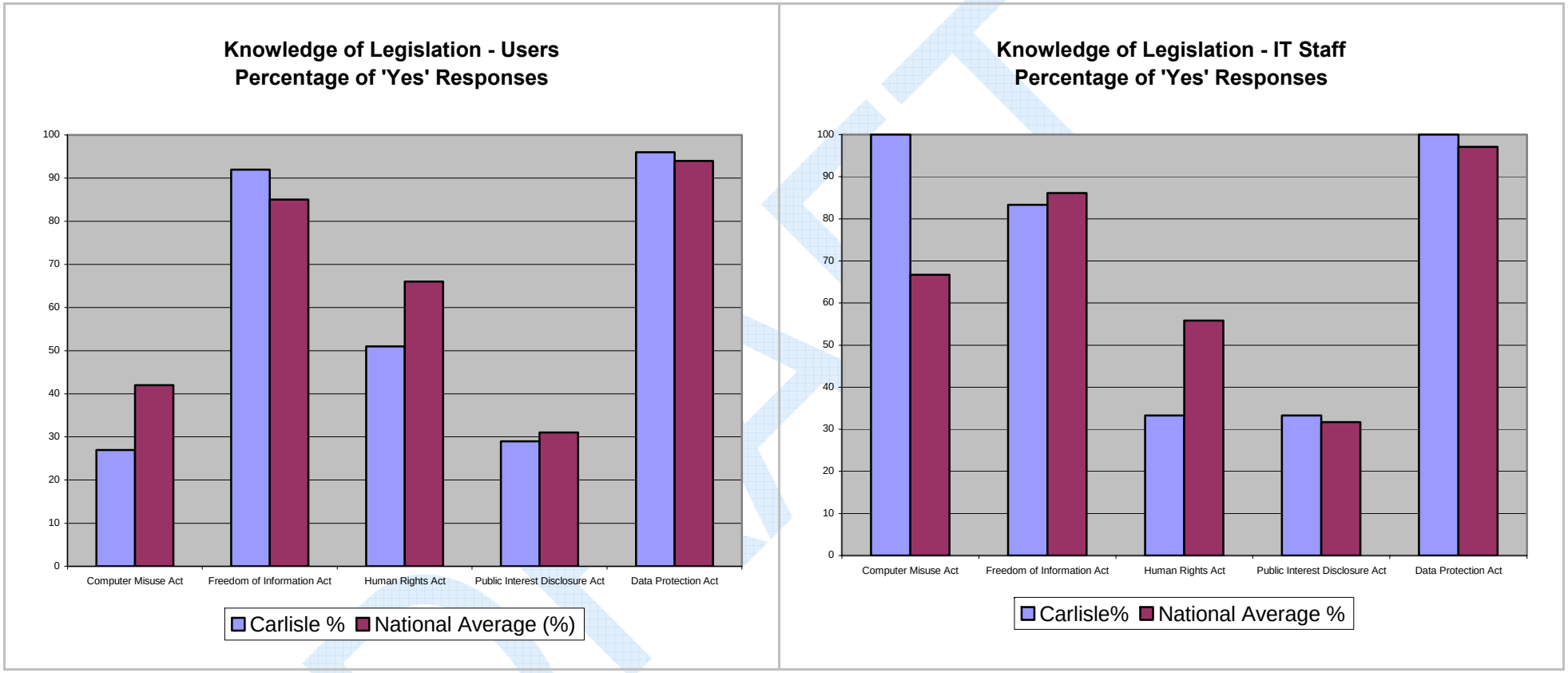


Source: YB@R: Audit Commission

Awareness of implications of legislation	Areas requiring attention	Suggested action
A high proportion of all respondents scored well to knowing about: • The Freedom of Information Act; and • The Data Protection Act. IT staff scored 100% for the Computer Misuse Act	Only 27% of users are aware of the Computer Misuse Act and about 51% are aware of The Human Rights Act. An average of 31% of respondents from both groups was positive in knowing something about the Interest Public Disclosure Act. Only 33% of IT staff were aware of the Human Rights Act	Increase IT legislation awareness through improved induction and ongoing training programmes.

Figure 3 Awareness of implications of legislation

Council versus national results

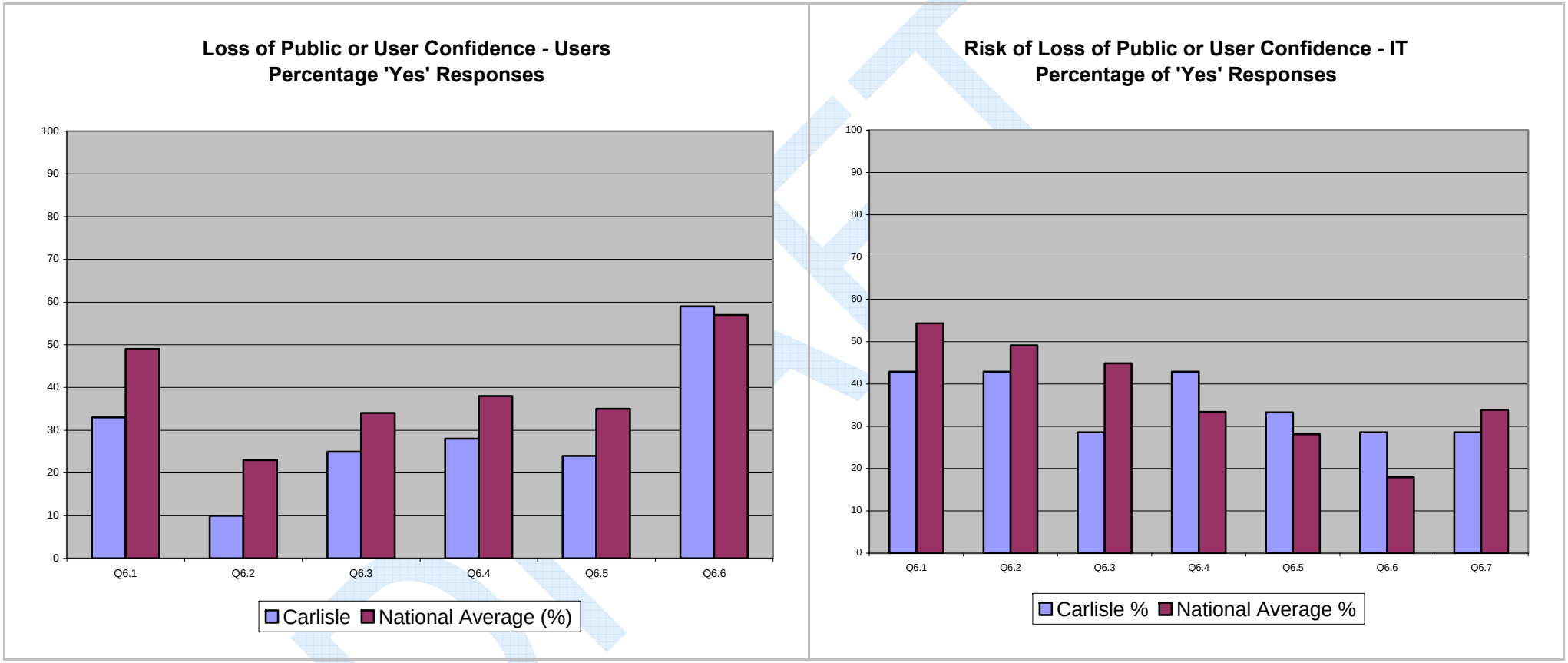


Source: YB@R: Audit Commission

Loss of user confidence risk		
Positive messages	**Areas requiring attention**	**Suggested action**
There is some knowledge of the management of security within the organisation.	64% of Users and 42.9% of IT staff do not know if there is a security policy. 74% of users do not know where to find written instructions for reporting a security incident.	Develop and issue an Information Security policy. Develop procedures for reporting IT security incidents.

Figure 4 Loss of user confidence

Council versus national results



Source: YB@R: Audit Commission

Appendix 1 – Detailed survey results

National average or above

Further work required to reach national average

Identified risk

Your.Business@Risk

User Survey

Q1 Which Department do you work in? (only complete if agreed by your Authority / Trust)

People Policy Performance	12%
Community Services	25%
Corporate Services	20%
Legal and democratic Services	9%
Development Services	28%
Elected Members	5%
Department 7	0%
Department 8	1%
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	91%	0%	9%	0%
Virus protection software is installed on my machine	96%	2%	2%	0%
Virus protection software is regularly updated on my machine	82%	1%	17%	0%
I have been given clear instructions about dealing with emailed files from external sources	57%	25%	17%	1%
I am sent an alert when new viruses are discovered and am told what to do and what not to do	53%	22%	25%	1%
I know how to report a virus infection if I suffer an infection on my machine	74%	17%	9%	1%
I have suffered a virus infection on my machine	12%	79%	8%	1%
Whenever I have suffered a virus infection, my machine was cleansed and restored quickly	12%	1%	11%	77%
To log on to my machine I must enter a user name and password	98%	2%	0%	1%
To log on to my organisation's network I must enter a user name and password	76%	9%	9%	6%
I am forced to change my password by the system on a regular basis eg. every month	10%	90%	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	45%	53%	1%	1%
I have not written my password(s) down	71%	28%	1%	0%
I am not authorised to enter our computer rooms	46%	17%	32%	5%

Q3 The risk of financial loss

	Yes	No	Don't know	Not Applicable
My organisation has an anti-fraud strategy.	40%	1%	58%	1%
I know what the key elements of the strategy are.	16%	31%	45%	8%
I only have access to the information I need to do my job	77%	9%	13%	1%
I am prevented from installing any software on my machine	44%	21%	34%	1%
I am prevented from copying software from my machine	42%	7%	49%	2%
My computer is clearly security-marked.	84%	2%	14%	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	86%	6%	8%	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.	86%	7%	7%	1%
I have been informed that my access to the internet will be monitored.	84%	9%	7%	0%
It has been made clear to me that my organisation's policy is that accessing or storing unsuitable material is a disciplinary matter	92%	4%	4%	0%
Emails sent to me from outside my organisation that contain very large files or executable programs etc. are prevented from reaching me	18%	19%	61%	1%
I have access to written protocols covering e-mail usage and language.	58%	9%	33%	0%
I have been informed by my organisation that the use of unlicensed software is prohibited.	69%	17%	14%	0%
I am prevented from installing software on my machine.	44%	22%	35%	0%

	Yes	No	Don't know	Not Applicable
Internal Auditors or IT staff in my organisation have checked the software on my machine.	32%	8%	60%	1%
My organisation has a documented data protection policy	84%	1%	14%	0%
My organisation has appointed a data protection officer	80%	1%	20%	0%
I have been required to sign a confidentiality undertaking as part of my conditions of service	33%	35%	32%	0%
My responsibilities under the Data Protection Act have been explained to me.	83%	13%	4%	0%
I have been informed that the misuse of personal data will be treated as a disciplinary offence by my organisation.	79%	14%	6%	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.	30%	62%	8%	0%

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

- *The Computer Misuse Act* 27%
- *The Freedom of Information Act* 92%
- *The Human Rights Act* 51%
- *The Public Interest Disclosure Act* 29%
- *The Data Protection Act* 96%

Q6 **Loss of public or user confidence**

	Yes	No	Don't know	Not Applicable
My organisation has an Information Security policy	33%	3%	64%	0%
I have been provided with a copy of the policy.	10%	46%	37%	6%
I have been informed about the policy and what I must and must not do.	25%	37%	33%	6%
Senior management in my organisation is committed to the policy and its observance.	28%	5%	65%	2%
I know where to find written procedures for reporting a security incident.	24%	44%	30%	1%
Someone in my organisation is specifically responsible for IT security	59%	1%	39%	1%

Thank you for taking the time to complete this survey.

Please press the 'Submit' button below.

Your.Business@Risk

ICT Staff Survey

Q1 **Which ICT Department do you work in?**

Corporate ICT	100.0%
Departmental ICT	0.0%

Q2 **The risk of business disruption**

	Yes	*No*	*Don't know*	*Not Applicable*
My organisation takes the threat of a virus infection very seriously	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	85.7%	14.3%	0.0%	0.0%
Staff have been given clear instructions about dealing with emailed files from external sources	42.9%	28.6%	28.6%	0.0%
Staff are alerted when new viruses are discovered and are advised as to what they must do	83.3%	16.7%	0.0%	0.0%
We have clear procedures in place for reporting a virus incident	71.4%	14.3%	14.3%	0.0%
Our procedures for recovering from a virus infection have been documented	57.1%	28.6%	14.3%	0.0%
Our virus software is automatically updated by the software vendor	100.0%	0.0%	0.0%	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	57.1%	28.6%	14.3%	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.	28.6%	28.6%	42.9%	0.0%
Our user registration and sign-on procedures prevent unauthorised access to our networks	100.0%	0.0%	0.0%	0.0%
Proper password management is enforced by the system on all users	42.9%	42.9%	14.3%	0.0%
Our dial-up connections are secure	85.7%	0.0%	14.3%	0.0%
Network management staff have been appointed	100.0%	0.0%	0.0%	0.0%
We have appointed an IT security officer	42.9%	28.6%	28.6%	0.0%

	Yes	No	Don't know	Not Applicable
A detailed daily log of network activity is maintained.	28.6%	28.6%	42.9%	0.0%
Network logs are inspected periodically by network staff	42.9%	14.3%	42.9%	0.0%
Sensitive programs and information are given additional protection.	71.4%	28.6%	0.0%	0.0%
Security violations are reported to IT security staff immediately by our security systems	57.1%	0.0%	42.9%	0.0%
Our web site vulnerability is checked every month	42.9%	14.3%	42.9%	0.0%
Physical entry controls prevent unauthorised access to our IT facilities	85.7%	14.3%	0.0%	0.0%
Our servers & network equipment are sited securely and adequate protection is offered.	85.7%	14.3%	0.0%	0.0%
Our internal procedures minimise the risk of deliberate damage by employees leaving the organisation	57.1%	28.6%	14.3%	0.0%
Any amendment to a program or system must go through our change control process	28.6%	57.1%	14.3%	0.0%
Our change control processes are well documented	28.6%	57.1%	14.3%	0.0%
All IT staff are trained in our change control requirements	14.3%	57.1%	28.6%	0.0%
Backups of data on all servers are taken frequently.	85.7%	14.3%	0.0%	0.0%
Backup arrangements are properly documented.	85.7%	14.3%	0.0%	0.0%
User and IT staff have been trained in how to conduct backups of servers.	100.0%	0.0%	0.0%	0.0%
Monitoring of backups ensures that management is alerted when backups of remote servers do not take place	71.4%	28.6%	0.0%	0.0%
My organisation has a clear business continuity plan.	42.9%	28.6%	28.6%	0.0%
All staff named in the business continuity plan know of its existence and their role in it.	28.6%	28.6%	28.6%	14.3%
Our continuity plan is based upon a robust risk analysis process	42.9%	14.3%	28.6%	14.3%

Q3 **The risk of financial loss**

	Yes	No	Don't know	Not Applicable
The systems most at risk from fraud have been identified.	40.0%	0.0%	60.0%	0.0%
The systems most at risk are afforded additional protection.	28.6%	28.6%	42.9%	0.0%
We have a documented access control policy	71.4%	28.6%	0.0%	0.0%
Access to systems is only provided to those who need it.	85.7%	0.0%	14.3%	0.0%
We have controls to prevent the copying or removal of software.	42.9%	14.3%	42.9%	0.0%
Hardware is clearly security-marked.	85.7%	0.0%	14.3%	0.0%
My organisation has clear rules covering private use of IT facilities and in particular what is and what isn't acceptable	85.7%	14.3%	0.0%	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	100.0%	0.0%	0.0%	0.0%
Internet activity logs are reviewed by managers.	57.1%	0.0%	42.9%	0.0%
We bar access to internet sites we deem to be unsuitable	100.0%	0.0%	0.0%	0.0%
Our policies make it clear to all staff that the downloading or storage of unsuitable material is a disciplinary matter	100.0%	0.0%	0.0%	0.0%
Protocols for internet and e-mail use have been developed and are available to all users.	85.7%	0.0%	14.3%	0.0%
My organisation has made it clear to all staff that use of unlicensed software is prohibited.	100.0%	0.0%	0.0%	0.0%
Security software that prevents the installation of any program except by authorised IT staff is installed on all PCs and laptops.	14.3%	71.4%	14.3%	0.0%
Our Internal Auditors undertake reviews of software on users' PCs.	28.6%	28.6%	42.9%	0.0%
Users in my organisation are prevented from gaining access to system utilities.	71.4%	14.3%	14.3%	0.0%
Our asset register is up to date, as are all enterprise / site license numbers	71.4%	14.3%	14.3%	0.0%
My organisation has a documented Data Protection Policy.	100.0%	0.0%	0.0%	0.0%

	Yes	No	Don't know	Not Applicable
My organisation has appointed a data protection officer.	100.0%	0.0%	0.0%	0.0%
All users are required to sign a confidentiality undertaking as part of their conditions of service	42.9%	28.6%	28.6%	0.0%
My responsibilities under the Data Protection Act have been explained to me.	71.4%	28.6%	0.0%	0.0%
Misuse of personal data is treated as a disciplinary offence.	100.0%	0.0%	0.0%	0.0%
PC's are timed out after a period of inactivity	42.9%	42.9%	14.3%	0.0%
My computer has a lock out facility to be used when left unattended.	83.3%	16.7%	0.0%	0.0%
Systems containing personal data are registered with the Information Commissioner.	85.7%	0.0%	14.3%	0.0%

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

- *The Computer Misuse Act* 100.0%
- *The Freedom of Information Act* 83.3%
- *The Human Rights Act* 33.3%
- *The Public Interest Disclosure Act* 33.3%
- *The Data Protection Act* 100.0%

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	42.9%	14.3%	42.9%	0.0%
Staff are informed about the policy and what they must and must not do.	42.9%	14.3%	42.9%	0.0%
Senior management is committed to the policy and its observance.	28.6%	14.3%	57.1%	0.0%
An officer group manages the implementation of information security.	42.9%	14.3%	42.9%	0.0%
Regular independent reviews of information security are undertaken.	33.3%	16.7%	50.0%	0.0%
We comply with BS7799 standards.	28.6%	14.3%	57.1%	0.0%
There are clear written procedures for reporting and following up all security incidents.	28.6%	28.6%	42.9%	0.0%

Thank you for taking the time to complete this survey.

Please press the 'Submit' button below.