

# online quality controls

■ **Computers have become the 'tools of the trade' for most accountancy firms. They provide the platform for word processing and spreadsheets, accounts preparation packages, tax compliance work and practice management. Add to this e-mail and the internet for communication and research and it is a rare firm that does not rely on electronic systems for some aspects of its business.**

Greater use of technology has many potential benefits for businesses, but it also has many potential risks. A firm's computer data represents an investment in time and money and is therefore an asset to the business and needs to be protected. Protecting the integrity and security of computer data will also help to ensure the continuity of the business.

The Quality Checked Seal (QCS), ACCA's quality assurance programme, covers these important areas of a firm's systems and regards some basic quality controls as best practice.

## organisation of a firm's data files

As with any filing system computer data files need to be organised to facilitate easy retrieval of information by all authorised users. Firms should have policies to cover two things:

- how individual documents are named
- where they are filed.

This is no different from a manual filing system. Storing all documents within a folder such as 'my documents' with no systematic naming convention is the electronic equivalent of filing all correspondence in a single file in no particular order.

This is not efficient, even for a very small business. Some file management system will be needed but its structure will depend on a number of factors including the volume of documents, the number of clients, what software the firm uses and the firm's own preferences.

Accounts preparation and tax packages often include some file management functions and there are a number of document management systems that will allow firms to store, retrieve and collate data. However, for many firms setting up a folder structure within MS Word may be all they need. Whatever structure is used, the file organisation should be understood by all members of staff and consistently applied across the whole firm.

If a firm's computers are not networked, or if files are created outside the network (e.g. when staff take laptops to clients' premises), there should be a policy on what data is stored on individual machines. How this is done will depend on how the firm operates but it should ensure that data can be located easily. If there are several copies of a document on different machines then it must be clear which is the final or latest version.

## security

To avoid unauthorised access to the firm's data, computers should be password protected. A firm can also use passwords to protect sections of data, for example to make the client database read-only except to designated individuals or to restrict access to confidential data to the partners or senior staff.

Any system that transfers data from one machine to another, or has access to the internet, is vulnerable to computer viruses which are capable of destroying all your electronic data. Once a virus is contracted it could then be passed on through e-mail to clients or anyone in your address book. This would damage your firm's reputation as well as your data.

There are many anti-virus software products available on the market to protect your electronic data and these should be used and updated on a regular basis to take account of any new viruses identified.



## Liz Kirkham explains how making effective use of your computer system can help you get the Quality Checked Seal.

Some anti-virus products are only intended for home use so you should check that any software you install is licensed for business use.

If you use external e-mail or the internet you should also have a reliable firewall installed. Some software companies bundle their anti-virus and firewall software together. Some firms restrict external e-mail and internet access to one stand-alone machine to minimise any risk. This will not be practical for many firms but if it is you should ensure that you do not send e-mail or copy data from this machine to others in the office.

### disaster recovery

There are advantages to having data saved electronically. If paper files are lost or destroyed it may not be possible to re-create the information in them and a firm would risk not being able to deal with its clients' affairs effectively for some time.

Electronic data is capable of being saved and restored very quickly provided that a firm has an effective disaster recovery plan. The risks facing paper files such as fire, theft and flood also affect electronic ones. And there are additional risks peculiar to electronic files such as accidental or deliberate deletion or data corruption.

Therefore a regular backup of all of a firm's computer data is an essential safeguard for all firms that use computers. It will depend on the level of usage and reliance a firm places on the data as to how often backups should be taken. This may vary from daily to weekly or even monthly backups.

A backup copy should be kept off-site so that it is not lost in the same fire or theft as the original data. In addition, backups should be tested to ensure that data retrieval is possible as it is not a good time to find out that the backup is corrupted when you have just experienced a system failure.

A firm's disaster recovery plan should also consider how hardware could be replaced if required. Backed up data is no use without hardware to run it on. If a firm is using specialist systems or hardware it should have a maintenance agreement in place and procedures for recovery or replacement of software and hardware.

Even if a firm's hardware and software can be purchased off the shelf from a high street computer store it should have a disaster recovery plan to consider how it would replace these items, e.g. will everything it needs be in stock?; is its insurance cover adequate and up to date?; how will it fund essential purchases while an insurance claim is being processed?

### data protection act

Firms holding detailed information about their clients need to be registered under the Data Protection Act. Information about notification exemptions can be found on [www.dpr.gov.uk](http://www.dpr.gov.uk). This contains a self-assessment guide which you are recommended to follow to confirm that you do not hold the sort of data that would require notification.

Electronic data offers many benefits to accountancy practices but also has many potential risks. These risks can be reduced by following best practice procedures. ■

Liz Kirkham – Compliance Officer, ACCA

Further information about ACCA's quality assurance programme and the Quality Checked Seal kitemark is available from [www.accaglobal.com/professionalstandards](http://www.accaglobal.com/professionalstandards).