Navigating the expanding landscape of information security standards can be a challenge. So if you don’t know your PCI DSS from your ISO 27001, Lesley Meall’s at-a-glance guide can help.

As computing and communication devices, software, data and networks have become more accessible and prolific, their security has become more complex. So has the landscape of information security frameworks, schemes and standards. The occupants now include (but are not restricted to) COBIT, Cyber Essentials, PCI DSS and the ISO/IEC 27000 series. It’s almost enough to make you hanker for the mainframe or desktop computing eras, when you could draw a bright line around your IT assets and their security.

Well, almost. A more connected and ubiquitous computing ecosystem is not without benefits. But technologies and trends such as cloud computing, growing (personal and professional) use of mobile devices and social media, and the emergence of ‘big data’ have created new and significant security challenges. Very few organisations are now immune to vulnerabilities, such as leaky employee endpoints, as well as threats and risks, such as disruption to business, fines and reputational damage.

“The threat from IT security breaches is too significant for accountants with IT roles to overlook the information security frameworks, schemes and standards that can help to identify, assess and address the key risks and threats,” says Omer Tariq, manager for risk and advisory at BDO. Marc Vael, international vice president at the Information Systems Audit and Control Association (ISACA), a professional association focused on IT governance adds: “Understanding them can help you to save valuable time building proper information security in your organisation and when validating and confirming where you are with this.”

Figuring out how much you need to understand in order to do this is almost as complex as some of the standards. Among the many potential influences are:
- where your responsibilities for IT security begin and end;
- the size, type and structure of your department or organisation;
- ownership and use of IT assets, products and services;
- IT management and governance frameworks in use;
- existing IT security policies and procedures;
- compliance with statutory, sector and supplier requirements; and
- access to technical expertise and financial resources.

So your need to know (as an individual, department or organisation) will sit somewhere on a very broad spectrum - not unlike the information security responsibilities and technical expertise of the members of the IT Faculty. But everyone has to start somewhere, and if you don’t already know your COBIT from your PCI DSS, or your ISO 27001 from your BS7799-2, a basic grasp of some of the most widely used frameworks, schemes and standards relating to IT security is an important step on the road to enlightenment – or certification.

Let’s begin with the latest and greatest UK government initiatives in this area, and see where this leads.
This started life as a 1980s government initiative by the Commercial Computer Security Centre of the now defunct Department of Trade and Industry; then, after a long and circuitous international journey, the 27000 series of information standards was launched in 2005 (learn more at 27000.org/thepast.htm), to help organisations improve their information security management.

The members of this fledgling family of standards you are most likely to encounter are 27001 and 27002. 27001 provides the requirements for establishing, implementing, maintaining and continuously improving an information security management system (ISMS); it replaced the BS7799-2 standard. 27002 outlines the hundreds of potential controls and control mechanisms, which may be implemented subject to the guidance in 27001. 27002 superseded ISO 17799 (a code of practice for information security).

You can learn more about the development of other standards in the 27000 series at 27000.org/contact.htm and other ISO standards related to the 27000 series at 27000.org/other.htm.

Numbers in the ISO 27000 series (also known as the ISMS family of standards) are allocated by the International Organisation for Standardisation (ISO, iso.org) which has developed and published more than 19,500 voluntary ‘best practice’ standards. ISO is a membership network of national standard setters, such as the UK British Standards Institution (BSI) – a private company incorporated by Royal Charter.

No law says you have to comply with 27001, but compliance with 27001 is required of product and service providers to an increasing number of businesses provide ‘independent’ ISO 27001 certification is as simple as Googling ‘iso 27001 accredited certification providers’, which brings up possibilities ranging from the Big Four accounting firms to specialists such as BSI (and yes, that is the same BSI that acts as the UK’s national standard setter).

The IASME Consortium Ltd is one of two bodies currently accredited to appoint Cyber Essentials certification providers (the other is CREST, a non-profit organisation). IASME evolved from another government initiative, and took forward a project of the Technology Strategy Board, a non-departmental public body, established by the government in 2004, and funded by the Department for Business, Innovation & Skills.

You can learn about approaches to certification, including companies that are licensed to deliver IASME assessments and routes to becoming an assessor, at iasme.co.uk/index.php/companiesdeliver.
**PCI DSS**

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organisations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. PCI DSS is different to Cyber Essentials, the ISO 27000 series, the IASME standard and COBIT in one very significant way: compliance is not optional; though it’s not a statutory requirement.

Merchants who do not comply with PCI DSS can find themselves held responsible for any losses incurred through fraud and face fines from the acquiring bank or financial institution that they use to process card payments – and almost all merchants who take card payments are expected to meet one of the four levels of PCI DSS compliance.

You can learn more about why and how to become compliant at [pcisecuritystandards.org](http://pcisecuritystandards.org) and find companies and providers that are qualified to provide PCI DSS-related products and services at [pcisecuritystandards.org/approved_companies_providers/index.php](http://pcisecuritystandards.org/approved_companies_providers/index.php).

A jargon-free version of the site for small merchants is available at [pcisecuritystandards.org/smb/](http://pcisecuritystandards.org/smb/).

**COBIT**

Control Objectives for Information and Related Technology (COBIT) is an IT governance framework, with a supporting toolset. It defines a set of generic processes that can be used by business managers, IT professionals and assurance professionals to enable good practice and policy development for IT governance and control throughout an organisation.

The global non-profit organisation ISACA first released COBIT in 1996. It's a high-level business oriented framework, so it is not focused solely on IT security or internet-based cyber security, though many organisations use COBIT as the framework for their governance and control systems. In 2013, ISACA released the guidance Transforming Cybersecurity Using COBIT 5 (the latest version, which incorporates the ISACA risk IT framework and the ISACA Business Model for Information Security).

In 2013 ISACA also launched the COBIT 5 Certified Assessor Program to recognise professionals with the skills to perform COBIT-based IT process assessments and the necessary experience in planning, building, running and/or monitoring IT processes, and provide them with a credential.

You can learn more at [isaca.org](http://isaca.org).

Lesley Meall is a freelance writer and ex-software engineer. She is author of the Chartech guides to online accounting software, using dashboard software, and payroll software and services.

**SPOILED FOR CHOICE?**

The schemes, standards and frameworks covered here are just some of the many out there. Different countries have their own equivalent to the UK Cyber Essentials scheme (such as the National Institute of Standards and Technology Cybersecurity Framework in the US); even a single organisation such as the ISO has many standards relating to information security (not just the 27000 series). It can be hard to see beyond the hyperbole of service providers with vested interests and there is no consensus on which individual or combined approach is superior.

A user of COBIT may also need to demonstrate compliance with the Cyber Essentials scheme, PCI DSS and ISO 27001, despite overlaps; another organisation may need to comply with PCI DSS and Cyber Essentials, while compliance with 27001 or COBIT could be overkill.

As ISACA’s Vael says, “all of the frameworks, schemes and standards should be considered as good inspiration sources. But all of them require intelligent interpretation”. So although this Chartech article may be enough to help some accountants with IT roles or responsibilities to assess their options, identify the standards and certifications that might best meet their needs, and form the basis of any necessary action, for others it may be one small step on a long and winding road through a landscape - and where some of you find a lot more investigatory work lies head.