

## **Auditing a data centre – but to what standard?**

**Barry Elliott**

[belliot@capitoline.co.uk](mailto:belliot@capitoline.co.uk)

Most people would agree that auditing a data centre is a good idea to demonstrate compliance with various standards and operating practices. However there is a great deal of confusion as to what data centres are being audited against. There are about forty different standards in circulation that claim some applicability to data centres, either very closely, e.g. TIA 942, or more generally, where a data centre is treated as just another place of work.

So when a data centre operator, or customer of a data centre, calls for an audit then the issue becomes one of what is the subject area, or areas, of most interest to that operator or user? One answer may be to audit against all of them but this would take a long time, cost over a quarter million Euros and need a full time manager just to keep up with the paperwork and ongoing maintenance of these qualifications.

Users and operators must therefore be specific as to what they really need to achieve and this may be linked to customer expectations or some legislative or regulatory requirement.

We have identified six main areas that address the design, operation and working practices of a data centre. These are;

**Business continuity and operating practices.** These may be general quality practices such as ISO 9000, environmental practices such as ISO 14000 or business continuity standards such as BS 25777:2008 *Information and Communications Technology – Continuity management, Code of Practice*. These standards call for good work practices, risk assessments, correct documentation and procedures in place and a business continuity and disaster recovery plan in case things do go badly wrong.

**Information security.** This is a very wide area that looks at data security, firewalls etc. all the way to the requirements of physical security for the site itself, computer rooms, cages and racks. ISO 27002 is a popular approach *Information technology. Security techniques. Code of practice for information security management*. The whole ISO 27000 series of documents gives a detailed and often complex approach to the whole area of Information Security Management Systems but although it is good at asking questions it is not too forthcoming with many answers. Many countries impose their own security requirements such as the British Government's Security Policy Framework, the European ITSEC, Information Technology Security Evaluation Criteria and the American Trusted Computer System Evaluation Criteria (TCSEC) and we also see requirements from statutes and agreements such as the Sarbanes-Oxley Act in the USA and Basel II accord in Europe. The Payment Card Industry

Council has its own physical data security standard initiated by American Express, Mastercard and Visa.

**Data Centre design and resilience.** To work properly the data centre must be designed and built to the most appropriate standards. The owner of the data centre must also decide how much redundancy and resilience to build into the model. The common format is to use the N, 2N etc. terminology where N means you have enough items to do the job, but no more, N+1 means one more item than you really need (so any one can fail and your system still operates) and 2N means two distinct systems and 2N+1 would mean two distinct systems with each system having an extra layer of component redundancy. The more layers of redundancy then the more resilient the data centre will be but of course the more it will also cost. There is also an issue of efficiency as well. Many items, such as Uninterruptible Power Supply Systems, UPS, do not run efficiently if lightly loaded. The American Up Time Institute and the American standard TIA 942 have given us the Tier model, whereby Tier 1 is the least resilient and would normally offer an N design, Tier 4 would be the highest level and would generally offer a 2N design and Tiers 2 and 3 are somewhere in the middle. The TIA 942 standard goes into some detail about the Tier models whereas the original work from the Up Time Institute is more of a design philosophy and hence opens to some interpretation. The new BICSI standard on data centres takes a different view on some items and as all these standards are American, with their references to the US National Electrical Code, and 110V 60 Hz electrical systems, none of them are directly applicable to the rest of the world.

**Energy efficiency.** The 'green agenda' is one of the fastest areas of growth in many areas of human activity and information technology is no exception. IT is now believed to have overtaken the aviation industry in terms of CO<sub>2</sub> output and hence has started to receive much more political attention. In America the US government passed the Server and Data Center Energy Efficiency, Public Law 109-431, April 2007. In Europe we have the 2001 European Directive on Energy performance in Buildings and the 2008 EU Code of Practice for data centre efficiency management. Many other organisations have come to the front offering their own classification systems for buildings in general (LEED, BREEAM) and data centres in particular (the Green Grid, Energy Star, EPA, the US Department of Energy etc.). A whole host of competing metrics to measure energy consumption and efficiency have been introduced from Energy Star rating for individual servers to efficiency ratings for whole buildings.

**Health and safety at work.** This approach is to treat a data centre just like any other place of work, which it is. There is more solid legislation applicable here than to any other area of data centre design or operation. From the EU we have directives that call for the safe use of electricity, correct safety signage, the use of emergency lighting, control of noise levels and safe access for the disabled. All these Directives have found their way into national laws and outside the EU most countries have a similar set up to control the work environment.

**Building regulations.** Most countries have sets of regulations that describe the safe and efficient construction and use of a building and once again a data centre is no exception. Regulations cover the construction and use of a building to minimise the risk of a fire, e.g. fire rating of walls and doors, number and location of emergency exits etc. Also covered are items such as the correct levels of ventilation for buildings where people live or work. Also appearing nowadays are legal requirements

to construct a new building to be as energy efficient as possible. Some parts of the world need to enforce seismic regulations to minimise the effect of earthquakes.

So to return to our main theme; to what standard should a data centre be audited to? And the answer is: respond to the main interest or concern of the owner or user? All the areas discussed will be of interest at some stage and indeed some are legal requirements but every user and owner will have a different set of requirements and driving forces. The Amsterdam Internet Exchange (AMS-IX) and Capitoline LLP have pioneered the technique of an asymmetric approach to auditing whereby the areas of most interest are focussed on, the relevant standards are identified and the required outcomes are defined. An audit should ask specific questions and set a benchmark to judge the answers by. Areas of concern should lead to an action plan to address any shortcomings and a re-audit plan implemented to follow them up.

The Amsterdam Internet Exchange, AMS-IX, is the largest internet exchange in the world and works by organising peer-to-peer connections via a set of strategically placed data centres located in or near Amsterdam.

In the interest of the members and customers of the AMS-IX the management decided to apply a common set of technical and operational requirements across all the data centres used by AMS-IX. Capitoline worked with AMS-IX to develop such an asymmetric auditing strategy as no single standard exists, or is likely to exist, that asks the right questions for all customers. AMS-IX is most interested in the correct technical set up and ongoing operation of a data centre that leads to the most reliable provision of the services that AMS-IX requires. Adherence to the AMS-IX standard is proven by an audit by a suitably qualified organisation.

There is no one standard that asks all the right questions of, and provides the right answers to, the correct and reliable operation of a data centre. By focussing on the business needs of an enterprise and picking from the 40 or so relevant national and international standards in circulation, then the correct standard and audit can be derived for your organisation.

The Capitoline  
view of Data  
Centre Design  
and Auditing

