

Business continuity – the new hot topic in data centre management

B J Elliott

belliot@capitoline.co.uk

www.capitoline.eu

The successful and reliable provision of any service depends upon the following attributes;

- A well designed and constructed plant that takes into account appropriate Standards and best practice to achieve efficient and reliable operation
- Management techniques that put in to place operating procedures and protocols that ensure the continuing efficient and reliable operation of the enterprise
- Disaster recovery plans that have an established and rehearsed procedure for dealing with any incident that impairs the operation of the enterprise and puts in to place a recovery programme

This approach could lend itself to the management of an oil refinery just as well as a data centre. But let us focus on the particular requirements of a data centre because this is one area where the different backgrounds of the management teams involved (IT, facilities management etc) cause them to often focus on their own areas and fail to address the bigger picture.

The hierarchy of Standards, codes, regulations etc, that give us the basic engineering principals and legal operating requirements should be drawn in the following order;

National laws, regulations and Statutory Instruments

EU Directives

CENELEC standards

IEC/ISO standards

National standards (although these take priority when referred to by national laws)

Other international standards e.g. ANSI, ASHRAE, TIA, VDI, BSI etc

Manufacturers' instructions

Industry best practice

Technical Standards

Technical Standards give the best practice methods for designing and implementing the data centre from a physical, electrical and mechanical viewpoint. Some requirements covering health and safety and energy management are covered by European Directives and national standards. Many technical standards exist that cover the myriad of engineering disciplines encountered in a data centre but two documents in particular address the engineering aspects of data centre design and subsequent resilience and redundancy of that design; these are:

ANSI/TIA-942:2005 *Telecommunications Infrastructure Standards for Data Centers*

and

Tier Classifications define site infrastructure performance. The Up Time Institute, 2008

The Up Time Institute's (TUI) document defines four 'Tiers' of operation that describe the expected downtime per year from a data centre when certain design routes are taken. The TIA 942 standard draws heavily upon the philosophy offered in the TUI document and offers more detail in engineering terms about what is required to achieve these levels.

One central plank of the philosophy is the adoption of the N, N+1 and 2N methodology. Briefly, N means enough items to do the job at hand, N+1 means that each system has one redundant component and 2N means that systems are completely replicated. Other variants may be 2N+1 for example, meaning two independent systems where each system also has redundant components. Ultimately it is a risk versus cost strategy as more levels of redundancy and resilience will invariably cost more. Organisations are invited to consider the costs of downtime to their own business before they decide upon the strategy most appropriate to their business.

Both of the above standards are American. There are no directly equivalent European (CENELEC) or international standards (ISO/IEC). The methods described in the two American documents are mostly universal but for use in Europe the technical references contained in TIA 942 need to be substituted for EU Directives and CENELEC standards wherever necessary.

The TUI model is not the only resilience model around; in Germany BEKOM has published an availability methodology and in the USA Syska Hennesy has produced its own availability system. However the TUI model remains the mostly widely accepted approach.

Other standards are being written, such as in Holland at the moment, but the only European standard that mentions data centres at the moment is EN 50173-5 which is a cabling standard for data centres.

Business Continuity standards

Building a data centre to the latest standards and incorporating the requisite availability/redundancy techniques is only the first step to successful long term operation. The next stage is managing the data centre and being prepared for technical failures or any other event that impinges upon the data centre operation. This area generally comes under the heading of Business Continuity Management, BCM. BCM standards can be generally aimed at all businesses and enterprises whereas some are more focussed on Information and Communications Technology, ICT.

The following Standards have been identified which cover this area.

- **BS 7799-3:2006** *Information security management systems. Guidelines for information security risk management*
- **BS ISO/IEC 20000-1:2005** *Information technology. Service management. Specification*
- **BS ISO/IEC 27001:2005** *Information technology. Security techniques. Information security management systems. Requirements*
- **BS ISO/IEC 27002:2005**, *Information technology. Security techniques. Code of practice for information security management*
- **BS 25999-1:2006** *Business continuity management, Part 1: Code of practice*

- **BS 25777:2008** *Information and Communications Technology – Continuity management, Code of Practice*
- **BS ISO/IEC 17799:2005** *Code of practice for information security management*
- **ISO/PAS 22399:2007** *Societal security - Guideline for incident preparedness and operational continuity management*
- **NFPA 1600;2007** *Standard on Disaster/Emergency Management and Business Continuity Programs*

In addition we have ITIL. ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT. ITIL has been developed in recognition of organisations' growing dependency on IT and embodies best practices for IT Service Management.

We also have PRINCE. PRINCE2 is a generic, simple to follow project management method. It covers how to organise, manage and control projects. It is aimed at enabling you to successfully deliver the right products, on time and within budget. A Project manager can apply the principles of PRINCE2 and the associated training to any type of project. It will help to manage risk, control quality and change effectively.

A PRINCE2 project has the following characteristics:

- A finite and defined life cycle
- Defined and measurable business products
- A corresponding set of activities to achieve the business products
- A defined amount of resources
- An organisation structure, with defined responsibilities, to manage the project.

In a survey by *Continuity Central* magazine of data centre managers in North America and Europe, BS 25999:2006 was quoted as being the most widely used. In 2008 a companion standard was published, *BS 25777:2008 Information and Communications Technology – Continuity management, Code of Practice*. BS 25777 appears to be a very appropriate document for use in Europe to describe best practice business continuity management in the ICT environment until a broader ISO/IEC standard is developed.

BS 25777 defines an ICT service as consisting of people, premises, technology, data, processes and suppliers. Under the "technology" heading is included the racking, cabling, servers and communications equipment.

The principles of ICT continuity management are based around six key concepts: Protect, Detect, React, Recover, Operate, and Return.

"For each critical ICT service the current continuity capability should be reviewed from a prevention perspective to assess risks of service interruption or degradation, e.g. single points of failure."

It seems clear that a number of strategies have to be put into place to ensure the successful and continued operation of a data centre. It starts off by defining what the very purpose of the data centre is. From that requisite software is defined and then the data processing hardware needed to

run the software and to enable communications and storage facilities can be defined. When that is known the correct size of building, power supplies and cooling can be derived. In parallel to this the amount of resilience and redundancy required by the customer must be designed in. Energy management and reduction methods must be also be applied.

When the basic site is designed then site security must be defined and implemented. As it is a place of work, like any other, then health and safety legislation must be followed. With the best possible infrastructure design in place it then comes time to implement the best working practices and of course associated with this comes the disaster recovery plan.

The diagram shows my interpretation of best practice design and management principles for a data centre based around the Business Continuity Concepts of BS 25777.

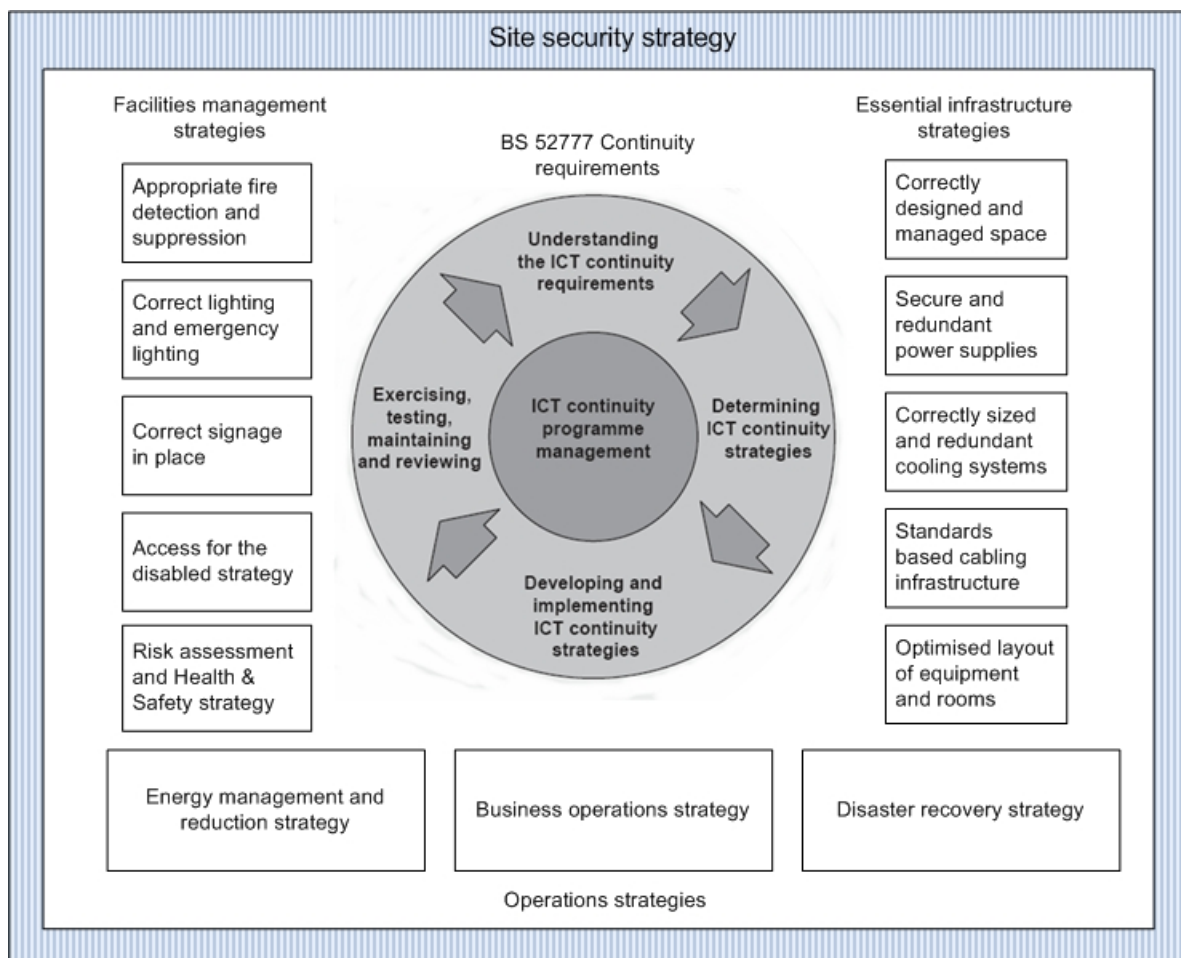


Figure 1: Design and management principles of a data centre