Chapter 1

Introduction

1.1 IT equipment

Data centre environments exists to house IT equipment. Broadly, this can be broken down into:

Servers providing compute capability. May be single-purpose servers, virtualisation hosts, modular multiple-unit blade server enclosures or larger mainframe equipment.

Storage systems providing aggregate storage to servers, such as dedicated NAS and SAN devices. May also include backup-centric storage such as tape storage systems.

Networking equipment including switches (unmanaged, L2/L3 managed), routers, hardware firewalls, hardware VPN, WAN termination and routing equipment.

Management equipment including local KVM, remote KVM, KVM-over-IP, serial console servers, smart power distribution units.

1.2 Infrastructural services

All data halls will vary. However, most will include some/all of the following:

Power distribution panels including circuit breakers, switches and meters. Also may include floor-standing UPS units.

Climate control equipment to maintain the room temperature and humidity in allowable ranges, often termed CRAC or CRAH.

Fire detection and suppression equipment.

Security equipment including access control devices, motion sensing and video cameras.

1.3 Regulation

Reliability standards govern to what degree a data centre can be described as fault-tolerent:

> **Uptime institute** has a number of "tiers" which summarise how reliable a particular data centre environment is.
>
> **TIA-942** has a number of similar tiers that are primarily dependent on reliability and redundancy

Efficiency standards aim to minimise the energy usage and environmental impact of data centres:

LEED

Data-related legislation has legal effect and may have ramifications in certain data centre environments:

GDPR governing personal data

FOI ensuring right of access to own personal data and to aggregate public data. Similar FOI laws exist in many countries.

HIPPA controlling how health data is stored and process

COPPA controlling how personal data of children is used and collected, including how consent from children/parents is taken for data processing.

Industry standards often are a requirement to do business in certain sectors and need to be followed:

PCI/DSS relating to handling and storage of payment card data. Compliance is normally a condition of being given merchant facilities.

ISO 27001 relating to storage/handling of general data in a secure fashion. Compliance is often a condition of being awarded business from certain public and private organisations.

1.3.1 Trends

There are a number of trends globally that are influencing data centre design and usage:

Virtualisation is becoming much more common where a hypervisor manages multiple operating systems on a single physical machine.

Cloud is a greater focus. Both in terms of replacement of certain on-site infrastructure with cloud services, integration in a hybrid onsite/cloud setup and provision of private cloud facilities.

Security is now a main focus area, and generally needs to be handled throughout all other activities as standard practice.

Environmental awareness both for energy saving, cost reduction and business reputation.

Automation to reduce the need for physical visits to the data centre environment.

1.4 People involved

Customer We will use customer to mean a customer of data centre services, as opposed to end user who utilises the services provided. The data centre customer has essentially got two options: on-site or co-located data centre.

End users People / systems who use the services provided by our data centre environment. They normally have expectations of availability, reliability but are not connected with the running of the data centre.

Estates / Facilities management personnel Depending on the facilty, a demarcation between the roles of data centre and facilites management will exist. This will become evident in things around power, cooling and fire alarm infrastructure. The relationship between data centre managers / technicians and facilities management professionals is a key asset to a well-run data centre environment.

1.5 On-site

Many organisations operate some on-site data centre provision:

- Some organisations may build and operate dedicated data centres for their own use.
- Many organisations will have a data centre that forms part of a larger facility, such as a hospital or college. It is often the case that non-IT personnel might have no idea that the facility has a data centre or where it is.
- Often, it's not even noticed or considered by the persons owning them. Even a NAS box stuffed in a corner that holds critical data needs to be considered as part of data centre provision!

1.5.1 Connectivity

An on-site data centre will need WAN connections to be ordered. These may take a number of forms such as standard DSL, GPON fibre, leased lines, microwave links. Carrier-owned equipment is often required and connects to customer owned equipment at the so-called demarcation point.

An on-site data centre located within a larger facility will also often form the central hub of the end-user-facing networking throughout the building or site, such as the office LAN.

1.5.2 Responsibilities

On-site data centres need careful co-ordination of different responsibilities:

IT personnel normally undertake network admin, system admin, patching and other IT-related duties.

Facilities management normally look after plant such as heating/cooling, parts of the electrical system and may have to facilitate copper/fibre installations.

Where exactly the demarcation between both sets of staff occurs is fluid and organisation-dependent. However, it is essential that the IT staff have a basic knowledge of certain mechanical and electrical concepts to facilitate productive interaction.

1.6 Business needs

Business needs must drive the choice of data centre provision. Some key questions include:

1. Is the workload better served by cloud or data-centre provision in the first place?

2. Are the users of the workload located in one particular site? Or are they distributed amongst multiple distinct sites or the wider internet?
3. How criticial is the workload to on-site business continuity?
4. What volume of data is likely to be exchanged between end-users and the data centre?
5. Can your on-site services match those a co-located provider can offer?

The solution chosen is often a compromise, and frequently a combination of multiple modes. For example:

- A supermarket chain might be best suited with a small on-site server room for in-store services, use a co-lo for central services and a cloud provision for its online store.