# CS25110 - Scenario Analysis Report

Tom Leaman (thl5)

March 15, 2013

# Contents

1 Introduction 3

2 Server Room 3
2.1 Physical Requirements 3
2.2 Service Provision Requirements 3
2.3 Other needs 3

3 Project Management 4
3.1 Risk Analysis 4
3.1.1 Incorrect provision of hardware 4
3.1.2 Overrunning of Budget 4
3.1.3 Late Delivery of Project Goals 4
3.1.4 Failure to Deliver by External Contractors 4
3.1.5 Incorrect / Late Delivery of Hardware 4

4 Hardware 4
4.1 Main Campus Server Room 4
4.2 Second Campus Hardware 5
4.3 User-facing Hardware 5

5 Software 6
5.1 IT & Services Software 6
5.1.1 Application Servers 6
5.1.2 Firewall 6
5.1.3 E-mail 6
5.1.4 Printing 6
5.1.5 File Storage 6
5.1.6 Naming & Directory 6
5.1.7 Webserver 6
5.2 User Software 6

6 Security 7
6.1 Network Security 7
6.2 Application Security 7
6.3 Physical Security 7

7 Naming & Directory Services 8

8 Business Continuity 8
8.1 Risk Analysis 8
8.1.1 Catastrophic Server Room Failure 8
8.1.2 Second Site Failure 8
8.1.3 Loss of Inter-Site Communications 8
8.1.4 Loss of Internet Communications 8
8.1.5 Network Security Breach 8

9 Ongoing Management 9
9.1 Disaster Recovery 9
9.2 Backups 9

10 Summary 10
10.1 Estimated Costs 10

# 1 Introduction

This document provides an overview of the ICT systems inteded to be provided for Mid Wales University. The University has around 2000 students and it is assumed to have around 50 academic staff, 50 post-graduate / research staff and 10 administrative staff.

Mid Wales University consists of two campuses in Newton and Caersws. One of these is assumed to provide office facilities for the majority of the administrative activities and shall be the location of the server room (henceforth considered to be the main campus). There will also be a second collection of servers on the second site providing redundancy for the main server room. The two sites will be connected by a fiber optic link discussed in section 2.2.

It is assumed that the University specialises in teaching Arts & Media subjects and, as such, has no subject-specific specialist ICT requirements.

# 2 Server Room

## 2.1 Physical Requirements

The room designated to be the server room will require enough space to house all of the equipment with around 3ft available above it for adequate ventilation and access to any cables which may be run along the ceiling.

There will be three 42U server racks in the centre of the room allowing full access to both the front and the back of the cabinet. It is imperative that these be grounded correctly so that any electrical anomalies do not present a threat to human health. These will provide adequate space for all the equipment specified in this document in addition to plenty of space for future requirements.

The server room should be located, as far as possible, out of the way of water and sewage services and should be accessible without climbing / descending any staircases (lift access is acceptable). It should also be noted that it is likely to be quite a noisy room and should be located away from areas that may suffer as a result of loud, continuous noise. If this is not possible, an alternative would be to sound-proof the room but it should be noted that this can be quite expensive.

There will also need to be one rack located on the second site (see 4.2).

## 2.2 Service Provision Requirements

It is recommended that a clean and separate power supply be provided both to the server room and, if possible, the second site's equipment rack. It is important that other building services' fluctuating power requirements do not affect the supply to either campus' equipment. Furthermore it is recommended that Uninterruptable Power Supplies be provided for each rack. Many of these also provide facilities to monitor the power consumption of individual devices (such as those provided by Geist).

Each site will require it's own internet connection. Since this will need to handle a lot of traffic at peak times of the day (particularly if students are to be resident on campus during their studies), fibre optic connections are recommended. The two sites should also be connected to each other directly by means of another fibre optic connection to allow services provided by the main campus to be accessed with minimal latency from the second campus.

## 2.3 Other needs

Server cooling will be provided by Airedale OnRak units (one per rack). These will dissipate the heat generated and will fit into the back of each of the server racks. It is recommended that a temperature monitor also be installed which is able to alert relevant personel if the temperature falls outside of normal operational ranges.

The server room must be fitted with a fire suppression system. This should use a gasseous suppression agent such as $CO_2$ which will not damage the sensitive equipment. This *will*, however require more space to be made available to store the suppression agent[1].

Physical access to the room must also be kept to only those staff members who require access to complete their tasks (and every effort should be made to enable them to work without access to the server room). Access will also be monitored either through a key card access system (see 6) or a physical visitor's log.

# 3 Project Management

The project will be overseen by a Steering Group chaired by a representative of the University (henceforth known as the Project Client). This Steering Group will contain a representative from all major departments of the University, a Project Manager and the head of ICT Services.

The group will be responsible for the specification of the services to be provided along with the smooth running and continuous day-to-day management of the project (as overseen by the Project Manager).

## 3.1 Risk Analysis

During the planning and development phase of the project, the following risks have been identified.

### 3.1.1 Incorrect provision of hardware

It is possible that the hardware outlined in this and future documents is incompatible or unfit for purpose. If this is the case, new devices will be specified and decided upon by the Steering Group.

### 3.1.2 Overrunning of Budget

While every effort has been and will continue to be made to ensure that all financial forecasts are accurate, unforseen expenses may be incurred. As such, it is recommended that a contingency of 10% of the overall project cost be included during planning which may be used to mitigate the risks of financial over-spend.

### 3.1.3 Late Delivery of Project Goals

Each phase of the project should have an established goal and time frame within which to be achieved. This should be closely monitored and regulated by the Steering Group by means of a weekly status report and *any* concerns should be raised as soon as possible so that mitigating action may be decided upon and undertaken by all relevant parties.

### 3.1.4 Failure to Deliver by External Contractors

Any phases of the project requiring external contractors are subject to further risks as a result of the work being undertaken (e.g. work not being finished on time or to correct specification). Therefore, any such phase should be given extra attention by the Steering Group and any specifically identifiable risks should be pre-emptively mitigated as far as is possible.

### 3.1.5 Incorrect / Late Delivery of Hardware

It is possible that hardware be delivered late or even damaged. Records of *all* purchases and deliveries must be kept so that any disputes / discontinuity may be dealt with as swiftly as possible.

# 4 Hardware

## 4.1 Main Campus Server Room

The main campus server room will contain one network switch to handle external traffic (internet and inter-site) and two further switches to distribute network connectivity inside the server room and to the rest of the building.

There will also be seven individual servers providing the following functions:

- Firewall server
- Application server
- Web server
- E-mail server
- Print server
- Primary DNS server
- Primary storage control server

It is recommended that the exact specification of these servers be decided upon after further requirements gathering and analysis by the Steering Group. Consideration should be made regarding how much processing power each requires. The most processor intensive services are likely to be provided by the application server, the storage controller and the web server. The print and e-mail servers are likely to need considerably less power.

In addition to this, there should be a workstation available in the server room for system administrators to use during maintenance and operation. It is assumed that any reasonable desktop computer will be acceptable and that some flavour of Linux will be installed (this is such a matter of taste that it should be decided upon by the staff who will be required to make use of it in their daily tasks). Furthermore, provision should be made for a monitor and keyboard to be attached to any of the servers in the racks for easy administration. Rack mountable KVM consoles are available and may be specified by the Steering Group.

The server room will also contain a RAID disk array with at least 6TB of useable space. This will be used to provide user's home directories and central backups of University documents, databases etc. Again, the exact make and model will be left to the Steering Group but it is recommended that these *not* be solid-state drives as these tend to fail with very little warning (even with proper backups in place, the author feels that people administering the system like to know when critical pieces of infrastructure are about to fail).

## 4.2 Second Campus Hardware

The second campus will house one further 42U rack. Attention should be paid to its placement with regard to cooling and fire safety. It should be located out of the way but not inaccessible. This rack will contain a backup application server, a secondary storage control server, a secondary DNS server and a backup / testing web server. In addition to these, it will require at least one network switch to connect to the internet and the main campus server room. There will also be a RAID disk array identical to that on the main campus.

## 4.3 User-facing Hardware

Users on either campus should be able to connect to the network wirelessly. This will require the provision of wireless access points through both sites. The specification and placement of these should be decided upon by the steering group after a comprehensive site survey.

Computer rooms, teaching rooms and offices will require workstations for the use of staff / students / visitors. Virtually any modern desktop hardware should suffice although it should be noted that the internal hard drive will only be required to hold the operating system as all data storage will be performed over the network.

It is possible that research students or other academic staff require particular pieces of hardware to be acquired. In this case, a request should be made to the ICT department for evaluation and processing but these requests are left entirely at the discretion of the Head of ICT.

It is expected that both campuses will require a number of peripheral devices (printers, scanners etc.) the location and specification of which will be decided upon by the Steering Group. Consideration should be made, however to ensure that they remain compatible with the rest of the system.

It is assumed that telephony requirements are being provided by a separate part of the design specification therefore no discussion of such systems will be made in this document.

# 5 Software

## 5.1 IT & Services Software

All of the servers (with the exception of the firewall and network storage covered below) will be installed with Debian Squeeze. This is an open-source Linux distribution used on production servers worldwide[2] and is very well supported by the community.

### 5.1.1 Application Servers

The application server will be used to provide software as a service to the users. The following list is expected to grow as a result of further requirements gathering activities outlined in section 3

Intacct Financial and Management Accounting software will be installed to provide payroll, PoS, budgeting and accounting services to administrative staff and public cafe / bar areas.

A Learning Management System will be provided by Blackboard. Blackboard has a large market share and industry backing [3] and although open-source alternatives were considered, none provide the range of features and support available from Blackboard.

### 5.1.2 Firewall

One of the servers will operate as a dedicated firewall and gateway. It will be installed with Smoothwall, a dedicated firewall distribution of Linux. It is open-source and is well documented through its online documentation and manuals [4].

### 5.1.3 E-mail

One of the servers will function as a dedicated e-mail server. It will be installed with Exim as the Mail Transfer Agent and RoundCube as the webmail front-end. Exim has been growing in popularity over recent years and is well supported on Debian platforms[5].

### 5.1.4 Printing

Print services will be handled by CUPS. It is likely that other utilities will be required to be installed as part of this system but this will depend on which printers are eventually selected and so the final decision will be in the hands of the Steering Group.

### 5.1.5 File Storage

The disks will be presented on the network using the CIFS protocol by means of Samba and cross-site backup policy will be enforced using rsync and cron jobs. Samba is very well established and well documented software which is frequently used to provide Windows and Linux home directories across the network.

### 5.1.6 Naming & Directory

See section 7

### 5.1.7 Webserver

One server will be given over to providing both the external website and an internal intranet. Nginx will be installed as the webserver. Nginx has been growing in popularity since its inception [6]. It is open-source and considerably less memory-intensive than Apache.

## 5.2 User Software

All student and staff workstations will be installed with Windows 7. I believe this to be a well understood platform for the average user and it may be possible to purchase a support contract from Microsoft.

Research students may require other versions of Windows or even Linux to be installed in order to run legacy applications critical to their work. In this case all software should pass through the audit procedures outlined below (see 6) before it is installed.

General office tools (word processor, spreadsheets, presentations etc.) will be provided by LibreOffice. This is not too dissimilar from commercial offerings and does not require licenses to be purchased.

# 6 Security

A policy of separation of concerns (that is, logically separate systems being kept as physically separate as possible) should be the first consideration toward security in virtually all areas of the ICT design.

The Steering Group should also put in place a regular check of the security systems as part of the regular maintenance schedule as mentioned below (see 9).

## 6.1 Network Security

Network services should, where possible, be limited to only those devices or users which require access. For example, the Point of Sale systems will only require access to particular applications provided by the application servers and as such should run on a separate VLAN. This means if any of the PoS machines are compromised, the scope for damage (at least theoretically) is limited to that sub-system of the overall network.

Furthermore, all devices wishing to access the network will be required to register a MAC address. While it is possible to spoof MAC addresses, this adds an extra hurdle for any potential attacker to jump.

## 6.2 Application Security

It is recommended that the Steering Group spend time putting together a document outlining what the University considers to be important factors in ensuring applications are safe, secure and stable enough to be deployed within the ICT infrastructure. This should include both Software as a Service (i.e. that which is installed on the application server and accessed remotely) *and* user software installed on individual work-stations. This document would then form the basis of a Software Security Audit procedure to be followed when procuring new software.

It is recommended that this procedure also be followed retro-actively for software outlined in this document. This is not just a point of sanity, it is intended that the results of the audits be kept on record for reference.

## 6.3 Physical Security

All workstations should be physically secured by means of a metal cable lock. It is important to ensure that the end of the lock not secured to the machine is attached to something large and heavy (all too often this step is skipped, entirely negating the purpose of the exercise!).

The server room itself must be kept locked at all times and it is recommended that some form of electronic access lock be provided which allows the monitoring of individual's movements. In the event of a problem, it is important to know who has accessed the room and when (see 2.3).

Any critical infrastructure located outside of the main server room should not be accessible to anyone who does not require access. To this end it is recommended that lockable (and preferable fire-proof) boxes be purchased and located out of sight (though not inaccessible).

The second site rack should be locked at all times and should be stored in a non-public area for increased security.

# 7 Naming & Directory Services

One of the servers at each site will be used exclusively as the authoritative name server for the University's domain(s), the primary controller being located in the server room and the secondary server on the second site. Debian will be installed as the Operating System (this is mostly for consistency with the other servers; if the Steering Group can justify a different OS, it should be possible to switch with little adjustment). BIND (v9) will be used to provide DNS services across the network and MySQL is recommended as the database controller for the records being stored.

In addition to this, LDAP will be used to provide directory services. This will also be used to store user data for all staff / student accounts (accounts which will be provided with a home directory on the main filestore). It should then be possible to use LDAP as the main authentication protocol across the network.

# 8 Business Continuity

The risks and mitigation strategies outlined below are intended to be a guide only. Further discussion and review should be carried out by the Steering Group (particularly with reference to specifying *exactly* which facilities and services are considered critical to the business continuity of the University).

## 8.1 Risk Analysis

### 8.1.1 Catastrophic Server Room Failure

In the event of all (or most) systems becoming unavailable in the server room (for example as the result of fire), critical applications (identified by the Steering Group) will be provided by the backup application server on the second site. Network storage will be provided by the backup storage devices on the second site although this will be considered a degraded service and only users with business critical needs (as identified by the Steering Group) will be allowed access. Naming and directory services will be provided by the secondary DNS server which will also be required to handle the activities once performed by the dedicated firewall. This too will be considered a degraded service. It is assumed that the public website of the University is considered business critical and as such will be served by the secondary web server in this eventuality.

### 8.1.2 Second Site Failure

In the event of the second site's ICT facilities being compromised, services provided by equipment on the second site should fall-back to using the primary systems available from the main server room. Directory and naming services will be considered a degraded service until such time as the secondary DNS server can be reinstated. Similarly, the ability to backup data to the second site will be unavailable. Efforts should be made to duplicate the backups available from the server room as a precautionary measure.

### 8.1.3 Loss of Inter-Site Communications

If the connection between sites is lost, any business critical tasks which depend heavily on services provided by the ICT department should be temporarily re-located to the main campus and repairative action be taken immediately.

### 8.1.4 Loss of Internet Communications

If either site experiences a loss of connectivity, it should route all external bound traffic through the other site. Based on the location of the University and the author's own personal experience, this situation is considered likely and adequate attention should be paid by the ICT group to ensure that this situation is dealt with as automatically and seamlessly as possible.

### 8.1.5 Network Security Breach

In the event of a possible network security breach, the affected machines should be brought offline as soon as possible whilst maintaining business continuity. For services which are duplicated (in whole or in part) on the second site, the secondary hardware and systems may be used with little to no interruption to business continuity. If there is no backup / duplicate service available, other hardware should be provisioned at the discretion of the Head of ICT and brought online from backups as soon as possible. Care should be taken to ensure that any backups used to restore offline systems be absolutely free from the errors / concerns which caused the system to be taken offline originally.

It is possible (or even likely) that such a security breach may affect many if not all of the systems on a single campus or even both of them. If this is the case, web services should be moved to an external provider temporarily whilst a full examination and rebuild of the system takes place. Planning for this sort of eventuality is no trivial undertaking and should be discussed at length by the Steering Group and reviewed regularly by the ICT group to ensure that business critical services are (as far as possible) unaffected whilst still ensuring that any concerns about the security of the failed system are not carried over to replacement systems.

# 9 Ongoing Management

It is recommended that in addition to a general ICT manager, the University also employ one or two system administrators and one ICT strategy adviser. These should meet on a regular basis with key staff in each department (that is people who understand what is required of the ICT systems within their own department). This regular meeting will allow current and future aspects of the system to be analysed and maintained without losing focus on the deliverable goals of day-to-day operations.

In addition to this, a maintenance schedule should be drawn up consisting of the task to be accomplished, the time it should take place and the member of staff responsible. Regular maintenance tasks may include (but are not limited to) updating system software, checking hard disk integrity and replacing batteries in UPSs.

Logs of all changes / additions to the critical infrastructure should be produced and kept up to date. These should be stored (along with other critical documents) in the server room (preferably in a fire-proof container). This ensures, should problems occur, that they can be traced back to their origin and fixed much quicker and with less risk to service.

## 9.1 Disaster Recovery

Furthermore, the Steering Group should compile a disaster recovery strategy to be maintained by the ICT committee. This will include strategies for recovery in the event of critical system infrastructure failure. For example, if the application server crashes, what is the procedure for switching to the back-up server, identifying the problem and reaching a solution. These operational procedures should be well understood by those members of the team who will be required to act upon it and as such it is recommended that these procedures be rehearsed at regular intervals (much the same way that a fire evacuation plan may be rehearsed).

## 9.2 Backups

Regular backups should be made of all critical data. The following strategy is presented as a guideline which should be revised by the Steering Group and ICT staff.

User's home directories will be backed up incrementally overnight to the second site. Rsync contains adequate options to ensure that this is done using minimal network bandwidth while maintaining correct meta-data.

Critical configuration files, logs, departmental documentation and other electronic documents identified by the University will also be backed up to the second site; preferably more often than once per day especially for documents which are likely to change on a regular basis (e.g. system log files). Provision should also be made for these to be backed up in a third location entirely off-site. Many companies are now offering cloud solutions for exactly this situation although I believe we may be able to arrange a mutually beneficial exchange of backups with another University / institution.

## 10 Summary

In conclusion, the University will require a secure server room on the main campus which will provide the primary hardware for all systems across both sites. It will also be necessary to house some secondary / backup hardware securely on the second campus.

Project Management will be overseen by a Steering Group responsible for the final specification and delivery of the services required. Control will then be handed to the ICT department for continuous management.

Business continuity objectives will be defined and documented clearly with well-rehearsed operational procedures for dealing with critical issues.

I believe that the infrastructure and strategies outlined in this document will provide a comprehensive and resilient solution to the business ICT requirements of the University at a reasonable level of cost.

### 10.1 Estimated Costs

- **Server Room Infrastructure** - £3,600
- **Server Room Services** - £4,000
- **Server Room Hardware** - £6,500
- **Second Campus Infrastructure** - £1,200
- **Second Campus Hardware** - £4,500
- **Network Provisioning** (e.g. site-wide ethernet) - £1,500
- **User Workstations** - £100,000
- **Software Licenses** - £75,000

**Total: 196,300**

## References

[1] *http://www.techrepublic.com/blog/security/the-mystical-world-of-data-center-fire-suppression/4113*

[2] *http://www.debian.org/users/*

[3] *http://en.wikipedia.org/wiki/Learning_management_system*

[4] *http://www.smoothwall.org/*

[5] *http://www.securityspace.com/s_survey/data/man.201007/mxsurvey.html*

[6] *http://trends.builtwith.com/Web-Server/nginx*

[7] *http://en.wikipedia.org/wiki/BIND*

[8] *http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol*