Scenario Analysis Report University of Mid Wales - CS25110 Assessed Assignmnet 2010-11

Peter Maynard

10 January 2011

1 Executive Summary

This report contains my recommendations regarding the ICT services for a new building at the University of Mid Wales, with support for teaching laboratories, academic staff offices, administration and support offices, research laboratories, coffee shops and other semi-public spaces. My recommendations were drawn mostly from the lectures and practicals of CS25110 and my knowledge from taking the Cisco Certified Network Associate course.

Here is an brief extract of my recommendations for the eight topics:

- **Custom Designed Server Room** – Secure location for the room, providing it with enough power.
- **Project Management** – Using the PRINCE2 protocols allow for international standard of management.
- **Computer Hardware** – Dedicated servers for each essential service and optimization using virtualization with standard hardware for all users.
- **Computer Software** – Mostly UNIX and Open source variants for servers and essential software with user specific software depending on its uses.
- **Security** – Hardware, data and users be kept safe from theft, damage or misuse.
- **Name and Directory Services** – Cover basic naming standards using DNS and LDAP
- **Business Continuity** – Repercussions of ICT failure and what can happen to the rest of the University.
- **Ongoing Management** – ISO 9000

Contents

2 Introduction

This is a scenario analysis report for Mid Wales University. It contains my recommendations of what should be done for the following eight topics.

- **Custom Designed Server Room** – Making sure that it is built in a secure location with the necessary facilitate to maintain secure and happy servers
- **Project Management** – Making sure that the whole project keeps running smoothly with out any problems
- **Computer Hardware** – Covers what kind of hardware may be required for the specifications of the University
- **Computer Software** – Covers what software may be required for the specifications of the University
- **Security** – Makes sure that the hardware and software is safe from harm
- **Name and Directory Services** – My recommendations for naming and directory services thought the network.
- **Business Continuity** – Making sure that you know what the consequences of failure is
- **Ongoing Management** – Helping to keep track of ongoing management of the system and what can be done to improve it

These are not set in stone and can be improved on, but they will help in the initial setting up of the ICT system in the new buildings.

3 Recommendations

The following eight sections show my recommendations. They are broken up into two main parts, these are my actual recommendation and various reasons why I have chosen them. Recomendations

3.1 Custom Designed Server Room

There are a few points that need to be considers before placing a server room. The first is the location. I would recommend a room that is not on the ground floor or at the top of a building. The main reasons for this is that if it where to be on the ground floor, it is vulnerable from people driving though the walls and damaging or stealing equipment for example. If it where to be placed at the top of the building, it runs the risk of water leak from the roof damaging equipment. It is also a good idea to think about other threats from the surrounding area, such as fuel storage.

It must also be placed in a location that will be able to provide it with enough dedicated electrical power to run the basic requirements as well have room for expansion. All server rooms should have an emergency power supple that will be automatically activated when there is a power cut. This will then allow the servers to be shut down safely or continue to run until the power is restored. I also recommend that it be located in a central location to its users. The room should also be able to support the masses of networking cables that may be needed to run though the walls for systems to run correctly. Which means that there should be no electrical or other type of interference. I also believe that the room should not have any outside facing windows, as this is a vulnerability to the security of the equipment. I would recommenced that there be an inside window where authorized users can check on the equipment, with out having to enter the room. I would recommend that the entrance to the server room be a secure plain door with no description to what is in side, this will prevent users that don't need to know from finding out about the servers physical location.

The floors of the room should have extra support for all of the systems that will be placed in the room to make sure that it is able to handle all the weight that it will be holding up. Also the entrances to the room must be wide enough to enable new or old equipment to be transported though them with out too much trouble. I would also recommend a room that can be used to build or repair systems that need to be taken apart. This room should be relatively close to the server room if not next door to allow for easy access to the systems. This room or the server room should have a table, chair, electrical sockets and few network interfaces to allow for easy testing.

There should also be emergency alarm and prevention systems such as fire, theft and power cuts. If there is a fire the system should active and attempt to suppress the fire as well as alerting the fire department. It is a good idea to use a system that will not asphyxiate any personal in the room. It is also a good idea to make sure that the system can not be activated by accident, and to make sure that the system is contained in the room. So as not to flood the rest of the building with the any sort of suppression gases.

The room should have air conditioning which should be kept at around $20 - 21$C. There should also be a humidifier to keep the humidity constant. It is very important to keep these systems running at all times, and they should each have redundancy systems which will be activated if one of the systems were to fail. It is recommended that you get dedicated systems installed, rather than using a few portable air/humidity conditioning systems. As the portable systems are loud and inefficient and you will still have too place a duct in the wall to remove the hot air. It is also a good idea to raise the floor to allow for better cooling of systems that will be running in the room.

3.2 Project Management

The management of this project needs to have a scope, which will be used to verify that the project is on track and when it is completed. I will recommend that you have the project split up into the following task lists:

- Server Room
- Hardware Delivered
- Hardware Configured
- Installation of Network
- Testing Network
- Testing Hardware
- Final Check

These are some examples of the scope which could be used as the projects goals. I recommend that each of these gaol are to be split up into smaller parts and each of these goals have there own manager, which all report to the main manager which is in charge of the hole project.

There are other factors to manage such as the length of time for each of the tasks. These can be managed using gantt charts. If a task overruns for a reason beyond its control it should be noted and the task manager should be notified. When this happens they should talk to the project manager who will decide if it is still feasible to continue with the project.

To help with the management of these tasks I will recommend that you follow some of the principles that is provided by PRINCE2[1]. PRINCE2 give this project a controlled start, middle and end. It makes sure that there are regular review against the main goals, see list above. It also makes sure that there is good communication and agreement of the final outcome.

By following the PRINCE2 procedures will make sure that if the project is changed along the way money and time is not wasted by continuing with the tasks and also makes sure that they keep up with change.

There are eight processes that define a project management activities under PRICE. These are as followed:

1. **Start up** – This is where a project team gets designed and appointed, gathers information on the project and sets up a risk log. This is a log of all the risks that can happened to the project and is used to make sure that the project does not fall into it.
2. **Directing a project** – Defining what is required from the project, authorising the funds for the project and committing the resources. This process also communicates with any external interested parties.

[1] PRINCE2 Stands for **PR**ojects **IN** **C**ontrolled **E**nvironments - http://www.prince2.com/what-is-prince2.asp

3. **Initiating a project** – When initiating a project it needs to be made clear that they are finite, have a defined start and end. It must also be clear what needs to be achieved and why, how the outcome it go to be achieved.

4. **Controlling a Stage** – When controlling a stage the manager needs to deliver products within tolerances. These are keeping risks under control, checking with the business case and makes sure that the project is going in the agreed direction.

5. **Managing product Delivery** – This is where agreements are made in relation to what will be completed and what needs to be done.

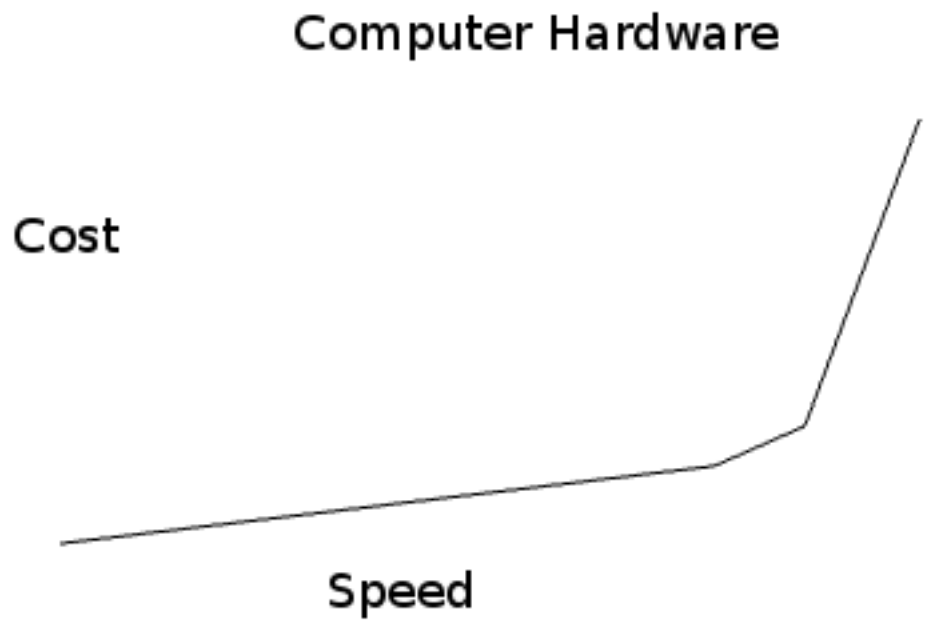
6. **Managing Stage Boundaries** – These are the points that are defined where if a project reaches, it may be better to cancel it rather than continue. The boundaries get confirmed at each of the major stages.

7. **Closing a Project** – makes sure that it is a controlled end to the project, and check that everything has been delivered to specification. It is also a good idea to document and later actions that need to be taken. Also a good idea to report the projects performance.

8. **Planning** – This happens thought the projects lifetime. It concentrates on the plan, stage, exception and team plan.

3.3 Computer Hardware

When buying new hardware it is best not to buy brand new hardware as soon as it is released. The reason for this is that the price will be a lot higher than if you where to buy something that was released two months before hand, and the difference in performance is minimal. See illustration, it shows the difference in cost and speed.



Computer Hardware - showing the rise in cost compared to speed

To insure that the system will be able to handle all that is required from it, when buying hardware all ways keep in mind what is required of it. You should also make sure that when designing the system you have redundancy or backup systems that will be able to take over from any malfunctioning hardware with out interruption to the users as much as possible.

I believe that you will require the following services:

- Storage Server
- Firewall
- Proxy/Web Cache Server
- Database Server
- Lightweight Directory Access Protocol Server
- Dynamic Host Configuration Protocol
- Domain Name System

- Mail Server
- Web Server
- Print Server
- Virtual Private Network
- Simple Network Time Protocol Server

From this list of requirements, I recommend for reliable operations you purchase a dedicated server and use virtualization to help save money on the cost of hardware. I think it would be best to make sure that each of the services in the list above have their own servers, and use virtualazation to help with managing back up and redundancy systems. This will save on money, although this may require more configuration, this is a cheap alternative to extra hardware. I will also recommend that you have a tape drive to store your back up on. For more information on the type of software used for file storage see the Software section of this report.

For the file server I will recommend that you have two servers to activity back each other up. Each server should have the following specification. 25TB storage with 16GB of RAM and dual-core AMD Opteron processor or similar. That should be able to cope with the requirements of the University with out much difficulties. For the other servers I will recommend a server with about 8/16GB of RAM and 0.5/1TB hard drive, with a single or double Dual/Quad-core Intel Xeon processors or similar. And then each service should have a load balancing or redundancy system. Which should have the same hardware as the master. This means that you will need to buy two servers for each service.

For power users I will recommend a system that is above the standard specifications of basic desktops. In today's standards I would recommend an Intel I3/7 with 4 to 8GB of DDR3 RAM and a 2TB hard drive, or equivalent. This will enable to user to happily run whatever they may need with out too many problems. My reason for this is that high end users may require to use lots of system resource intensive software such as 3D modelling.

For secretarial and administrative staff we recommenced that the system hardware be a basic desktop computer, or laptop. All though if it is a laptop make sure not to store any important data on the laptop its self and to make sure that all passwords and user names be cleared from the system when it is shut down. A basic desktop computer at the moment is something like an Intel Dual Core 2.5Ghz and 2GB of RAM with a 250GB hard drive. This will be able to run all of the requirements of a admin of secretarial staff, this will cover word processing and data entry.

For visitors I recommend that you have a WiFi network set up so that they will be able to connect to the network and use the provided services. I will also recommend an option for the visitors if they need it, that you provide laptops or temporary logins where they will be able to use services. I will recommend that the specification of the laptops will be the same as the basic secretarial and admin staff, as I wouldn't have though that visitors will require much more than email and web access.

For the coffee shop I will recommend having a stand alone system that is unable to connect to the internet or the local network. This will prevent malicious users from intercepting or stealing important account details. For the hardware its self it will only need to be a low end computer,

with optional touch screen. A computer that is based on the Intel i3 or Intel Atom with about 3/1GB of RAM, and a 250GB hard drive.

All hardware should come with ergonomic keyboards and mouse. With a standard 17" TFT monitor.

As a CISCO certified engineer I feel obligated to recommend that you use CISCO networking hardware as they provide you with secure and highly reliable performance. I recommend that you have a router to provide OSI layer 3 support and switches to allow layer 2 packet management. I will also recommend that you have fibre optics connecting all the backbone services together. Each room has its one dedicated transmit and receive fibre connection, you should brake it down to 1000mbps connections to all computers in the room. Or if they do not require such speeds you could use 100mbps to save on money. All cables should be category six, this will increase performance has it has better insulation. In the server room, it is a good idea to make sure that all the cables are colour coded to help with management. An estimate of the cost of hardware may follow the following trend:

Hardware	**Estimate Cost**
2x File Storage Server	£15,200 @ £7,600 each
22x Other Servers	£12,100 @ £550 each
10,000x Varius Other computers	£180,0000 @ £180 each
Total	**£1,827,300**

3.4 Computer Software

For servers that need to be secure from the outside world such as firewalls or proxy servers. I will recommend that the operating system they run be based on a UNIX variant. One of the most secure UNIX operating systems that currently available is *BSD. This is a good operating system to run on servers as it provides the users with security and access to all leading software. The only draw back is that the administrators needs to know how to use a UNIX based operating system, which in some cases the system administrator is only able to use a Windows based system. The advantages of using a UNIX operating system over Windows is that there is no licensing fees compared to Microsoft Windows or Apple.

The software that I will recommend for the servers is going to all be open source. This means that if you do not require support/training, it will all be free to use. I will recommend Apache for web hosting, PostgreSQL for databases, Squid Proxy, Postfix for email and IP Tables for the firewall. This software is relatively easy to set up and get working. I will also recommend that you keep track of all the stats of the servers, to help notice abnormal activities quicker. For stats monitoring I shall recommend you install Munin, as this is an industrial standard networked resource monitoring tool. There is also a lot of support available on the internet, using sites like google you can find answers in no time.

For the file storage I will recommend that you use ZFS as the file system as this will provide much greater data integrity and supports the ability to have very large filesystems. It also makes backing up data to another server easy and can be accomplished with one simple command line. It supports the ability to send incremental changes between a snapshot of the system to another server else where.

For the system to run correctly with minimal management from administrators it is necessary to install and configure Domain Name Service (DNS) and directory services. For more information about these, please see the Naming and Directory Services section of this report. For Domain Name Services I will recommend that you use BIND, as it is one of the leading open source software that allows configuring of domain names. For user authorization and directory services I will recommend for the same reasons as BIND that you use OpenLDAP. All though it is possible to use Network Information Service, NIS. I will not recommend this as it is becoming obsolete. All though it is very capable of handling the same as LDAP, its just it lacks some features that LDAP have or will have implemented.

The operating system that I recommend for the teaching and research labs is going to depend on what is being taught in them. If it is something that does not require much more than taking notes and running some programs. It might be a good idea to install and use Microsoft Windows. Because most users that do no study computer science rarely need or use anything other than Windows. If on the other hand computer science is being taught in the labs, then I will suggest that you install a variation of UNIX as it will be able to support more of the software required for the users than Windows. Other software to be installed on these systems will be software like word processing, spreadsheet and web browsing.

For academic, administration and support offices, I would recommend allowing them to chose what they prefer to work on. For example if they are used to using Apple then allow them to purchase one using the University funds or bring in their own and connect it up to the network for them. This will allow for better work performance as they will be more happy to work for you. But if

they do not have any preference the best system to give them is a computer that runs the latest Microsoft Windows and Office Suite. As they are more likely to know how to use a Microsoft machine than UNIX or Apple. But I will recommend that you remind them they will be more secure if they where to work with UNIX. As if they do this will create less problems with keeping licences and viruses protect up to date. Make sure to install the basic office suite, mail reading and web browsing software on all of these machines, so they will be able to complete all given tasks with out any problems.

For public areas I will suggest that you install a secure variation of Linux. Make sure to lock it down so the public users will only be able to access restricted and monitored services. It might also be a good idea to allow staff and student to log in and provide them will full access to the system so they will be able to continue with there authorized activities. I will recommend a web browser and word processing software to be install for the public, and full teaching and research software be installed for authorized users.

It may be necessary to install operating system specific software for thing like 3D Modelling, Computer Aided Design and financial management. Make sure that these software works and runs as the user expects as to maximize performance of the users and user satisfaction. An estimate of the cost of software may follow the following trend:

Software	**Estimate Cost**
Microsoft Windows Block Licence	£Unavailable
Microsoft Office Block Licence	£Unavailable
Open Source Support Services	£8,600 pa
Virus Definition Updates	£2,000 pa
Total	£10,600pa with extra

3.5 Security

I assume that the University will have top priorities that the hardware, data and users be kept safe from theft, damage or misuse. As this will create a bad image and will cost the University if any of this where to happen.

To ensure that the server room all ways be secure and safe from damage. You need to make sure that the space around the room be maintained as a danger free zone. This means making sure that if there is improvements to the building, that nothing will interfere with communications or draw much needed power from the servers to other new hardware being placed in the building.

To prevent hardware from being stolen. I recommend that all hardware be securely locked to the building. It is also a good idea to psychically and virtually tag the hardware and take note of the serial number, which will assist in recovering the hardware if stolen, and to help prevent the selling of stolen goods. I recommend that all labs and public areas have CCTV recording and clear notices that users are being recorded or monitored. To make sure that none of the hardware has been stolen or damaged I would recommend that someone from the building maintenance staff be allocated in checking all rooms that the hardware is present and undamaged, as well as constant monitoring of CCTV recordings.

For the security of the server room I will recommend that there be only one entrance, which is unmarked and have a numeric key pad to allow authorized access. All so make sure that when employees or contractors enter the room they are never alone, and accompanied by personnel which have enough knowledge to know if the contractor or employee is not misusing the system. This makes sure that nothing can be stolen, copied or accidentally damage the system. As well as making sure that any injuries are reported. To make sure that the security of the server room be maintained there will be a log book and computer record of who and why they have entered the server room. It is also recommended that only a select few can enter the room, who will have to be authorized by the top system manager.

To help in the protection of users and user data, it is recommended that there be a system in place that will prevent the users from accidentally entering their account passwords on an unencrypted connection. Make sure that all uses change their password at a set interval.

Misuse of the system such as playing games or messing around with other hardware such as the projector can be monitored by covering staff and building maintenance staff. This will ensure that only users who actually need the system be allowed access. It is also a good idea to keep all networking equipment behind locked doors and to not allow users access to these systems, as this is the main for a communication thought the network. Therefore it is a great data and user security risk, as a malicious user may be able to tap into the flow of data and store or tamper with the data packets. But to make sure that the computer system is not being misused in a software context, then it is recommended that the system administrator install and monitor software that keeps track of logs, network traffic and users statistics.

3.6 Naming and Directory Services

Naming of hardware is required, as it helps too identify each node on the network. It is best too give names that are descriptive and help in the overall management of the network. When naming, it is good practice to give the machine a network global unique name. I would recommend that you split you the name depending on its location in the building and what it does. For example if it is on the first floor, is a staff computer and is the third computer in the room. I would name it <building-name>-1-<staff-group>-3. 1 means that its on the first floor and 3 means that it is computer three.

When naming servers or desktops it is helpful to give them descriptive names, but this could pose a security risk, as the name will show up in data packets that are send inside the network. So any malicious users will be able to work out what server runs which services and can help them in determining there target.

DNS – Domain Name System, is used to configure the network allowing hosts to be called by their domain names. DNS takes the domain name, which is the name of the host, and converts it to an Internet Packet (IP) address which can then be used to communicate with the machine. The same can happen the other way around, this is called Reverse DNS lookup. DNS is useful because if the machine is configured to use your DNS server, you will be able to type in the name of the machine you would like to connect with and it will translate to the IP address a name is easier to remember than an IPv4/6 address.

Having just DNS configured will not help in locating, users, resources or services. This is why we need a directory service. These services will help in the configuring of user names and passwords, groups and their memberships, net groups and mail aliases. Having a directory service running on your network, will enable all machines that are configured correctly to allow users to log into their system with a single user name and password. It will also allow them access to their files that are stored on the network from any machine.

To help locate such things, this is where Lightweight Directory Access Protocol - LDAP comes in. The data that is contained in LDAP can be globally or locally unique to the network. But it will normally contain the following data. Name of the company, in this case “Mid Wales University”, the user ID for example it could be a three character string with a single digit at the end, it will also contain their name and email address. It will more than likely be stored in a hierarchical tree with the root at the top followed be location, organisation then people, printers and services. For more information about directory naming please see the Software section of this report.

3.7 Business Continuity

As the University is a business, I will expect that it wants all of the systems to be running at 100% at all times. But there will be times when software crashes and hardware fail. This will not doubt cause problems for students and staff. This is where a risk analysis will help in working out what needs to be maintained and find out what is the most important.

If a part of the ICT system is to fail then there can be huge setbacks in the rest of the business. Such things can give the business bad publicity and even lose customers. It can also mean angry employees. This can be prevented by ensuring a back up plan be in place for all possibilities. You need to make sure that there will be a member of staff that knows what needs to be done in the event of an emergency and what procedures to do. I will cover the risks of what some could happen if some of the systems services where to fail. There are three levels of risks, high, medium and low.

Below is a table shows the outcome and probability of a system service failure. It shows that the ICT system effects more than just its self. You need to be aware of how much damage there can been to the business from miss configured software.

System Service	Likelihood	Damage Level
LDAP failure/error	Low	High
Mail Server Failure	Medium	Medium
Compromised System	High	Very High

These can effect the entire business, because if users are unable to log in they will not be able to conduct business and this will effect the performance of the University. For example if they mail server goes down, users will be unable to respond to potential customers as known as students. If the system was to be compromised customers will lose trust in using the University's services.

3.8 Ongoing Management

I will recommend that the ongoing management of the ICT systems be maintained using the ISO 9000 standard. This will make sure that the system be transparent and easy to see mistakes and stop them from happening. ISO 9000 is built on a set of internationally acknowledged standards contained in eight principles. These are:

1. **Customer Focus** – Makes sure that what ever is needed by the customer is flexible and responds to market opportunities. It also makes sure that the system works better for customers and helps to understand what they want.
2. **Leadership** – It makes sure that all staff have their own purpose and know what direction they should be heading in. it also makes sure that people know what the University's main goals are and how they can help advance and make it a better place. It makes sure that people are free and responsible for what they do.
3. **Involvement of people** – This makes sure that each and every member of staff is involved and have ownership of what they do. They are more likely to share knowledge and experience with other staff, which will make sure that all systems are running at 100%.
4. **Process approach** – This makes sure that all activities and resources are managed as a process, this means that everything gets done to within the requirements of the University. It also attempts to improve the process as it goes along.
5. **Systems approach to management** – This manages the inter-related processes to help give the best result. It makes sure that all the processes are consistent and efficient.
6. **Continual improvement** – makes sure that all the processes are flexible and able to react quickly to opportunities. It recommends that it be a permanent objective to improve the current processes.
7. **Factual approach to decision making** – Makes sure that all decisions are informed and has the ability to review and challenge decisions that have been made or will be made. It is based on reliable and accurate information.
8. **Supplier relationships** – Makes a mutually beneficial relationship by pooling expertise and developing and improving to change to the market. It helps in a clear and open communication.

I recommend that the University have this as the ongoing management structure, as it provides a well proven way in which to manage a project.

I also recommend that all administrators be trained to handle every other persons responsibilities, in the event on an emergency if the normal admin is not available someone else will be able to pick up where the other left off. Even if they cannot complete the task as quick as the other person, so long as they can do it. This makes sure that there will all ways be someone who can fix any problem.

You should also have a protocol of having stickers and signs that let people know what is going on in case they accidentally shut down the wrong system. For example a sign that says "Only shut down after phoning this number", this will mean that the person in charge will know weather or not it is safe to disable the machine.

4 Conclusion

In conclusion I believe that overall my recommendations focus on the security of the system and making sure that hardware, data and users are kept safe from danger and damage. As I believe that these are important and should be reflected in the security of the system that is to be created. I also believe that the system should be managed with efficiency, this is also reflected in my recommendations as a lot of the software chosen is from the open source community, as you know open source means that the source is available and is constantly being updated and improved. This in my opinion is the best way to create an efficient system.

The main limitations of my recommendations is the fact that over time the systems will be coming increasing less powerful in relation to new hardware. This can count as an advantage or a limitation, as most of the system is based on a UNIX variant, this means that you have to make sure that you hire staff that know how to use these systems.