Topic 1 - Networks

What you need to know:

- ***Choosing a network for a company***
  - *cost of network*
  - *size of organisation*
  - *how the system will be used*
  - *existing systems*
  - *performance required*
  - *security issues*
- ***Types of networks available and the use of associated hardware***
  - *Client server networks*
  - *Peer to peer networks*
  - *Bus/Ethernet*
  - *Ring*
  - *Star*
  - *Suitable topologies for LAN and WAN*
  - *Wireless networks*
- ***Software components***
  - *User accounts and logs*
  - *Security strategies*
  - *Configuration management*
  - *Remote management*
  - *Disaster planning (backup and restoration)*
  - *Auditing (keeping logs).*

Factors that influence the choice of a network

- Cost of a network
- Existing systems
- Performance required
- Security issues
- Size of organisation
- How the system will be used

Factors influencing the choice of a network

- **Cost of a network**

  Includes the cost of the server, cabling, software and third party communications. Not usually an issue in bigger organisations.

- **Size of an organisation**

  Determines the complexity of the network as larger organisations may have users in sites around the world; therefore costs of communications could be high, this will also determine whether they need a LAN or a WAN.

Factors influencing the choice of a network

- **How the system will be used**

  Affect the scale of the network as large organisations will need LANs set up in each store with one being connected to a WAN, which allows all stores to communicate with the head office.

- **Existing Systems**

  Networks usually have to work with existing systems, therefore consideration has to be taken as to whether the new network will be compatible with the current software/hardware.

Factors influencing the choice of a network

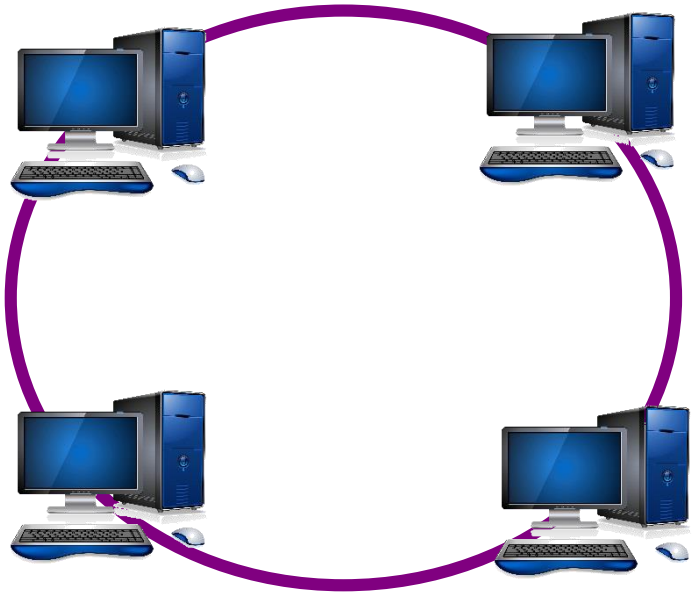
- **Performance required**

  Determine the way the computers and hardware will be connected together. It will also determine the type of server needed, i.e. some departments will need real-time processing.

- **Security issues**

  Determine whether internet access is needed and how the company can protect the network for hackers and viruses.

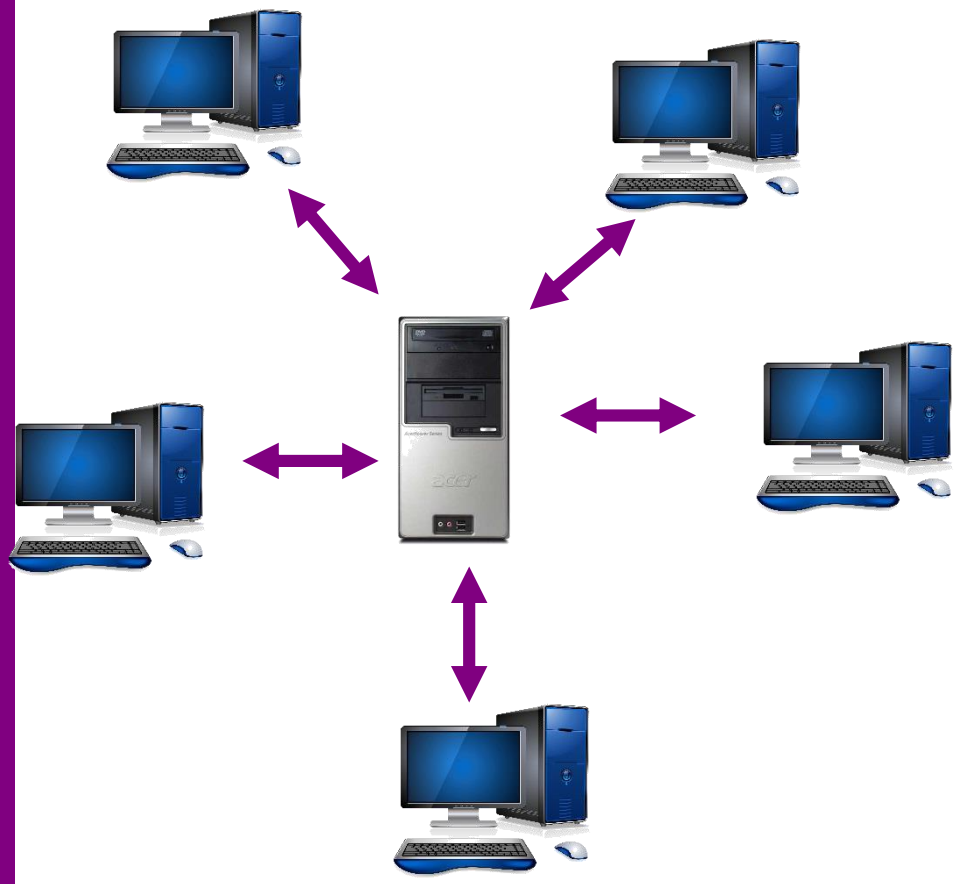
Types of networks available and the use of their associated hardware



Peer to Peer

A network where each computer has the same status and they are able to communicate with each other on an equal footing.

Types of networks available



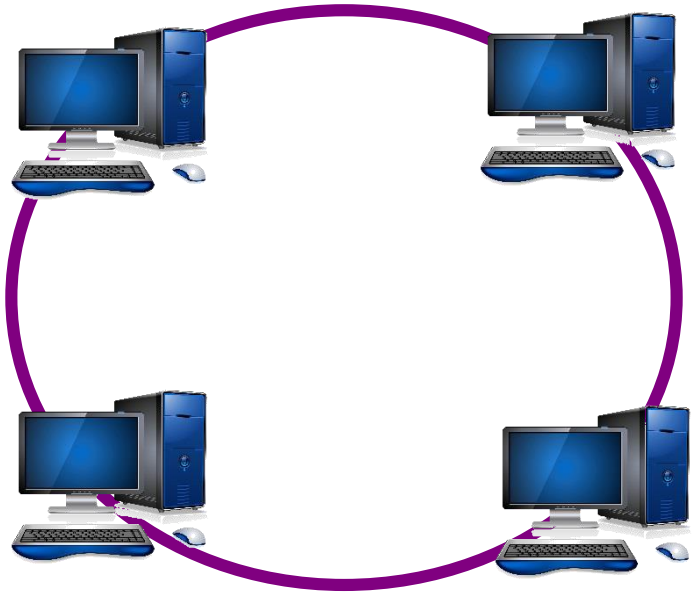
Client server

A preferred network for larger networks. Computers do not have the same status. A more powerful computer is used as a central computer where all the files and programs are stored.

Types of networks

Peer to Peer		Client server	
Advantage	**Disadvantage**	**Advantage**	**Disadvantage**
•Cost saving as no server is needed. •No network manager is needed. •Easy to set up •No reliance on a server. •Lower operational costs. •Peer responsibility.	•Backups cannot be made centrally. •Users need more IT knowledge. •Poor security. •Some computers may run slowly. •Only suitable for small networks. •Files not held centrally.	•Security is better. •Centralised data, •Backups are taken centrally. •Faster access to programs and files. •Centralised administration.	•More expensive. •Need specialist knowledge. •Software is sophisticated and expensive. •If the server breaks down it renders the network unusable.

Network topologies

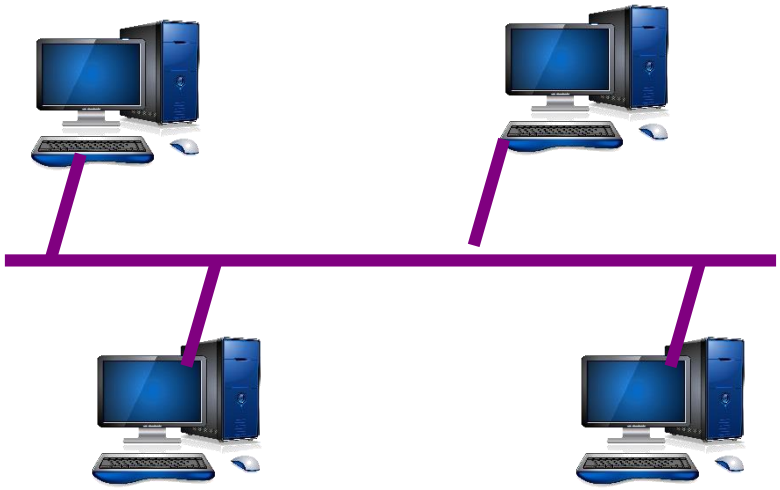


- **Ring Topology**

  No sever is involved therefore it is a peer to peer network.
  - Computers are arranged in a circle.
  - Data sent by one computer passes around the ring until it reaches the correct computer.

Advantages	Disadvantages
•The network is not dependant on a central computer. •Each computer has the same access as the others.	•If there is a break in the connection the whole network fails. •Faults are difficult to locate. •Impossible to keep the network running whilst adding equipment.

Network topologies

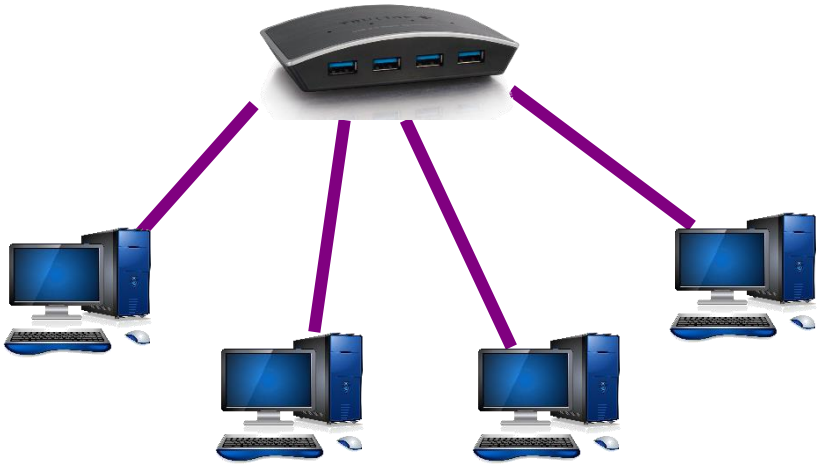


- **Bus Topology**

  All devices are connected to the network to a command shared cable called the backbone. Signals are passed in either direction along the backbone.

Advantages	Disadvantages
•Cost effective because of the small amount of cable needed. •Simple cable runs makes it easy to install. •Easy to add extra devices.	•If more than 12 devices are connected to the network, the performance of the network is degraded. •If there is a break in the backbone, the network cannot be used.

Network topologies



- **Star Topology**

  Uses a central connection point to connect all the devices on the network together. Central point can be a hub, switch or router.

Advantages	Disadvantages
•Fault tolerant. •Load tolerant. •Easy to add extra devices.	•Higher cost – cabling. •Dependant on the central hub, switch or router. If this fails, the network fails.

Wireless networking

Many computers are now able to connect to the Internet or communicate with other computers in a LAN wirelessly. With wireless communication the data transfer medium is the air through which the radio waves travel.

- Can work anywhere that they get signal from their network.
- Many hotspots – public places that offer wireless connection.

To set up a small Wi-Fi network you would need:

- A broadband connection to the Internet
- A router
- Wi-Fi enabled computers

How Wi-Fi works

- Router is connected to the Internet by a high speed broadband connection.
- The router receives data from the Internet
- It transmits the data as a radio signal using an antenna.
- The computer's wireless adapter picks up the signal and turns the radio signal into data that the computer can understand.

Wireless networking

Advantages	Disadvantages
•Allows inexpensive LANS to be set up without cables. •Allows people the freedom of working anywhere a signal can be received. •Ideal for networks in old listed buildings where cables would not be allowed to be installed. •Global set of standards – can use Wi-Fi all over the world.	•Power consumption is high – this means laptops soon exhaust their rechargeable batter. •There may be health problems in using Wi-Fi. •Security problems •Home users - Very limited range •Interference if wireless network signals start to overlap.

Software Components

- Networks need software to tell the connected devices how to communicate with each other.
  - User accounts and logs
  - Security strategies
  - Configuration management
  - Remote management
  - Disaster planning (backup and restoration)
  - Auditing (keeping logs).

Software Components

- User accounts and logs

  User accounts and logs are an important part of network software and prevent misuse of the network by users. With this software it is very easy to find the culprit if there is a misuse.

  - Everyone is given a username and password
  - Will have certain rights depending on the access needed.
  - A user logs in and out when necessary.

Software Components

- Security Strategies

  The use of networks exposes organisations to a range of security threats, so strategies regarding the use of networks need to be developed to minimise threats. There are a range of methods available:

  - Use of a password and user ID
  - Virus checkers
  - Firewalls
  - Encryption

Software Components

- Configuration Management

  Necessary to configure the network to maximise its performance. Organises and maintains all the information on a network.
  - The network manager will refer to this when the network needs upgrading or expanding.
- Advantages are:
  - Much easier to repair, expand or upgrade the network.
  - Network will be optimised.
  - Less network downtime.
  - Security will be optimised.
  - Roll back changes.
  - Keeps records of all changes.

Software Components

- Remote Management

  A network manager can perform many tasks from their terminal:
  - See which users are using the network
  - Check on e-mails being sent in company time
  - Check on the Internet sites visited
  - Check on hardware
  - Check licenses for software are not being exceeded
  - Guide users through problems
  - Check users do not have any unauthorised software downloaded
  - Log a user off
  - Shut down stations.

Software Components

- Disaster Planning

  Companies will have to cope with a situation that will cause the loss of hardware, software or data. The loss can be cause by:

  - Hardware failure
  - Software bugs
  - Natural disasters
  - Deliberate damage
  - Accidental damage

  Disaster planning is needed:

  - To minimise disruption
  - Get systems working quickly
  - Ensure all staff know what to do to recover data.

Software Components

- Backup and restoration

  Backups should be taken:

  – On a regular basis
  – Kept away from the computer in a fireproof safe
  – Use grandfather, father, son approach.
  – Use with a RAID.

  Files need to be restored using the backups. It is important staff know how to do this.

Topic 2 - Database Systems

What you need to know:

- Databases
  - *Explain the terms data consistency, data redundancy, data integrity and data independence.*
  - *Explain the terms relational database organisation and data normalisation.*
  - *Restructure data into normalised form.*
  - *Describe the use of primary keys, foreign keys and links.*
  - *Describe the advantages of different users having different views of data.*
  - *Database security. Recognise that the individual user of a database may be prevented from accessing particular elements of the information.*
  - *Data warehousing and data mining.*
  - *The purpose of a database management system (DBMS), query languages and data dictionaries.*
- **Distributed databases**
  - Candidates should be able to define a distributed database and discuss their advantages and disadvantages with reference to suitable examples.

Flat Files

Flat files store all the data in a single file. This causes many potential problems.

What problems could arise from the use of this file?

Customer	Forename	Surname	Address 1	Postcode	Tel No	Tool ID	Tool	Hire Price	Date Rented	Date Due Back
1200	Steve	Smith	1 Dacre Street	L91 6TY	243 6782	2	Steam stripper	£9.50	14/08/2008	15/08/2008
1200	Steve	Smith	1 Dacre Steet	L91 6TY	243 6782	2	Steam stripper	£9.50	19/08/2008	21/08/2008
1201	Jenny	Chung	12 Morris Street	L43 1WW	782 8722	3	Carpet cleaner	£43.00	14/08/2008	19/08/2008
1202	Raymond	Chandler	8 Fell Street	L21 L44	920 1111	1	Pressure washer	£15.00	13/08/2008	14/08/2008
1203	John	Jacobs	99 Teesdale Rd	L44 7TU	976 6121	4	Floor Sander	£67.00	13/08/2008	17/08/2008
1203	John	Jacobs	99 Teesd le Rd	L44 7TU	976 6121	1	Pressure washer	£15.00	17/08/2008	20/08/2008

Flat File

- More storage space is required, and more data entry time (***data redundancy***)

Customer	Forename	Surname	Address 1	Postcode	Tel No	Tool ID	Tool	Hire Price	Date Rented	Date Due Back
1200	Steve	Smith	1 Dacre Street	L91 6TY	243 6782	2	Steam stripper	£9.50	14/08/2008	15/08/2008
1200	Steve	Smith	1 Dacre Street	L91 6TY	243 6782	2	Steam stripper	£9.50	19/08/2008	21/08/2008
1201	Jenny	Chung	12 Morris Street	L43 1WW	782 8722	3	Carpet cleaner	£43.00	14/08/2008	19/08/2008
1202	Raymond	Chandler	8 Fell Street	L21 L44	920 1111	1	Pressure washer	£15.00	13/08/2008	14/08/2008
1203	John	Jacobs	99 Teesdale Rd	L44 7TU	976 6121	4	Floor Sander	£67.00	13/08/2008	17/08/2008
1203	John	Jacobs	99 Teesdale Rd	L44 7TU	976 6121	1	Pressure washer	£15.00	17/08/2008	20/08/2008

- Data that should be identical is different (***inconsistencies***, causing ***data integrity*** issues)
- Incomplete data (are these the only tools the business rents? Are these their only customers?)

Relational Databases

To resolve problems with inconsistencies and data redundancy, we use ***relational databases***.

Relational database– A large collection of data items and links between them structured in such a way that it allows it to be accessed by a number of different applications programs

Data redundancy – where an item of data is stored more than once in a database. This means that data entry/amending time is longer (as multiple copies need to be added/amended), and disk space is wasted.

Data inconsistencies - data that should be identical, but isn't. Data types, or the data itself could differ. If you have several similar pieces of data, how would the user know which one to trust?

Relational Databases

Using relational links and shared fields, the data can be more efficiently

Customer	Forename	Surname	Address 1	Postcode	Tel No
1200	Steve	Smith	1 Dacre Street	L91 6TY	243 6782
1201	Jenny	Chung	12 Morris Street	L43 1WW	782 8722
1202	Raymond	Chandler	8 Fell Street	L21 L44	920 1111
1203	John	Jacobs	99 Teesdale Rd	L44 7TU	976 6121

Customers

Tool ID	Customer	Date Rented	Date Due Back
2	1200	14/08/2008	15/08/2008
2	1200	19/08/2008	21/08/2008
3	1201	14/08/2008	19/08/2008
1	1202	13/08/2008	14/08/2008
4	1203	13/08/2008	17/08/2008
1	1203	17/08/2008	20/08/2008

Rentals

Tool ID	Tool	Hire Price
2	Steam stripper	£9.50
3	Carpet cleaner	£43.00
1	Pressure washer	£15.00
4	Floor Sander	£67.00
1	Pressure washer	£15.00

Tools

This avoids redundancy, removes inconsistencies and will improve data integrity.

Primary Keys , Foreign Keys and Links

- **Primary Key** – *a unique identifier for each record in a table.*
- **Foreign Key** – *a field in one table that is also the primary key in another table. Foreign keys establish links between tables.*
- **Composite primary key** – *a primary key made up of a combination of two or more fields*
- **Links** – *the relationship between tables.*

Primary Keys

Customer	Forename	Surname	Address 1	Postcode	Tel No
1200	Steve	Smith	1 Dacre Street	L91 6TY	243 6782
1201	Jenny	Chung	12 Morris Street	L43 1WW	782 8722
1202	Raymond	Chandler	8 Fell Street	L21 L44	920 1111
1203	John	Jacobs	99 Teesdale Rd	L44 7TU	976 6121

Link

Link

Tool ID	Customer	Date Rented	Date Due Back
2	1200	14/08/2008	15/08/2008
2	1200	19/08/2008	21/08/2008
3	1201	14/08/2008	19/08/2008
1	1202	13/08/2008	14/08/2008
4	1203	13/08/2008	17/08/2008
1	1203	17/08/2008	20/08/2008

Foreign Keys

Tool ID	Tool	Hire Price
2	Steam stripper	£9.50
3	Carpet cleaner	£43.00
1	Pressure washer	£15.00
4	Floor Sander	£67.00
1	Pressure washer	£15.00

Composite primary key

Ensuring Data Integrity

Data Integrity – *the correctness of data*

- **Removing transcription errors** - using automatic input devices, verification checks, validation checks.
- **Regular maintenance** - if employee or pupil leaves, changes address, etc.
- **Data Independence** – the separation of the data from the applications that use it. This ensures the data is more secure.
- **Data consistency** is using one file to hold a central pool of data. A company may hold all its customer data in one file. This avoids the need to input data twice so that if data is changed in one file it won't need to be changed in another and remains consistent.

Security

Relational databases are more secure than flat files because of:

- ***Data independence – the data and the programs used to access it are independent/separate***. New applications can be developed to access the data without changing the data. New systems can still use existing data.
- ***Hierarchy of access prevent access to data unless required, or restricts access to parts of the program that uses the data.***

Data Warehousing

- ***A data warehouse is a large database used to store an organization's historical data which is used by a MIS to extract information to help managers make decisions.***
- It allows the company to store all the details of what it has sold to every customer.
- The company can see who uses a loyalty card and exactly what they have bought and what
- method they used to pay for it.
- Can compare information like the sickness data from different stores.
- Storing all this historical data better equips managers to make their decisions.

Data Mining

Data Mining is the process looking for the idea of trends, patterns or generating new information

- is the analysis of a large amount of data in a data warehouse to provide new information.
- Is interrogating large amounts of data
- is a speculative process investigating potential patterns
- involves the presumption that dormant within the data are undiscovered patterns /groupings / sequences / associations.
- software uses complex algorithms to search for patterns.
- is drilling down into the mass of data so users can understand it more / discover meaningful patterns.
- Is looking for meaningful patterns in a large mass of data and presenting results in tables and graphs.

Database Systems

Examples of the use of data mining (the first 2 are worth more marks):

- **Fighting shoplifting in clothing stores** – e.g. Jaeger used DM to look at transactions and position of item in store, and discovered that most stolen items were near a door, even items with security tags. This led to increased CCTV in these areas, more prosecutions and recovery of goods.
- **Identification of customer needs** – e.g. Virgin Media use DM to target customers most likely to buy new services or upgrades.
- Companies with a list of customers likely to buy a certain product, can then target them with a mail shot.
- Comparisons with competitors to see how their own business could be improved
- Useful 'what if' results from modelling exercises
- Predictions for future sales
- Analysis of best sites for shops
- Analysis of sales patterns

DBMS

Database Management Systems are applications to hold a centralised collection of structured data.

They keep the data separate from the applications, and are completely independent.

DBMS allow:

- databases to be defined or modified
- databases to be queried
- Data amendments
- Adequate security
- Import/export of data

DBMS

- ✓ Data independence
- ✓ Avoids redundancy
- ✓ Data is shared
- ✓ Data integrity is maintained (all programs share the up-to-date data)
- ✓ Better security
- ✓ Standardised data definitions (via a data dictionary)
- ✘ Difficult to create and maintain
- ✘ Expensive
- ✘ Data is more vulnerable than distributed databases.

DBMS

Components of a DBMS:

Queries/Query Languages:

Queries are ***requests for specific information from a database*** (written in a special language)**.**

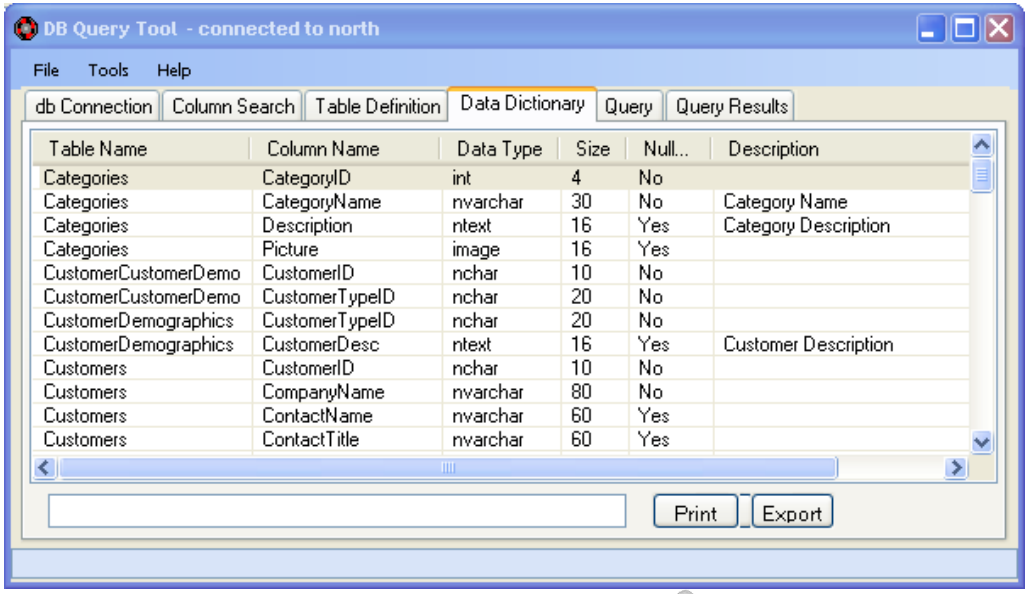
SQL (Structured Query Language) is the most common query language, and this allows not only the retrieval of data, but also sorting and updating of data in a database.

DBMS

Data Dictionaries

A data dictionary defines all data items in a database. This includes:

- Table name (entity)
- Field names (attributes)
- Field types
- Field lengths
- Validation
- Relational links and keys



Distributed Databases

A distributed database has data stored on a number of computers at different locations but appears as one logical database.

Advantages:

- Faster response to user queries of the database
- Non-dependence on one central huge store of data
- Easy to backup and copy data from one server to another
- If one server fails then the other servers can be used
- Reduces network traffic as local queries can be performed using local servers.

Disadvantages:

- Heavy reliance on networks and communications which may not always be reliable
- Security issues particularly if sensitive personal data is being transferred
- If one of the links to a server failed then the data could not be obtained from that server
- Increased costs owing to the use of expensive communication lines
- Greater chance of data inconsistency
- Harder to control the security of data spread in many different locations.

Normalisation

- ***Normalisation – a staged (mathematical) process which removes repeated groups of data and inconsistencies.***

- Normalisation is done to many different levels, but levels 1-3 is all we will be studying in this course.

Normalisation

- **1NF**
- A table is in **First Normal Form** (1NF) if there are **no repeating groups or data.**

- **2NF**
- A table is in Second Normal Form if it is in 1NF and it has **no partial dependencies (***also called functional dependencies)*.

- **3NF**
- For a table to be in 3NF it must be in 2NF and have **no transitive dependencies**.

Example - University Database

Pupil Num	Pupil Name	DOB	Subject Num	Subject	Lecturer Number	Lecturer Name
P99010	Jane Grey	12.03.86	CP101	Computing	UH	Glover, T
P99205 P99205 P99205	Tom Jones Tom Jones Tom Jones	05.11.86 05.11.86 05.11.86	CP101 MA110 PH190	Computing Music Physics	UH UG 58	Glover, T Reader, B Day, S
P99311 P99311	Sam Hill Sam Hill	16.08.86 16.08.86	BS101 EN004	Business Music	UH UG	Newman, P Reader, B

1NF

A table is in **First Normal Form** (1NF) if there are **no repeating groups or data.**

What data is being repeated in this flat file table?

This data is repeated, so inconsistencies could arise. This must be removed.

Pupil Num	Pupil Name	DOB	Subject Num	Subject	Lecturer Number	Lecturer Name
P99010	Jane Grey	12.03.86	CP101	Computing	UH	Glover, T
P99205 P99205 P99205	Tom Jones Tom Jones Tom Jones	05.11.86 05.11.86 05.11.86	CP101 MA110 PH190	Computing Music Physics	UH UG 58	Glover, T Reader, B Day, S
P99311 P99311	Sam Hill Sam Hill	16.08.86 05.11.86	BS101 EN004	Business Music	UH UG	Newman, P Reader, B

These are **repeating attributes**, since they could have different values, or no values at all, for each pupil. These items belong in a new table. One way of storing this data would be to use attributes such as Subject1, Subject2, Subject3. This is inefficient, and shouldn't be done.

Pupil Num	Subject Num	Pupil Name	DOB
P99010	CP101	Jane Grey	12.03.86
P99205 P99205 P99205	CP101 MA110 PH190	Tom Jones Tom Jones Tom Jones	05.11.86 05.11.86 05.11.86
P99311P99311	CP1019 EN004	Sam Hill Sam Hill	16.08.86 16.08.86

Pupil

Subject Num	Subject	Lecturer Number	Lecturer Name
CP101	Computing	UH	Glover, T
MA110	Music	UG	Reader, B
PH190	Physics	58	Day, S
BS101	Business	UH	Newman, P

Subject

Subject(Subject_num, Subject, Lecturer Number, Lecturer Name)
Pupil (Pupil num, Subject_num, Pupil Name, DOB)

To ensure the tables remain linked, the key field of **Subject** is placed into **Pupils**, and becomes part of its primary key.
Why is a composite primary needed?

Pupil Num	Subject Num	Pupil Name	DOB
P99010	CP101	Jane Grey	12.03.86
P99205 P99205 P99205	CP101 MA110 PH190	Tom Jones Tom Jones Tom Jones	05.11.86 05.11.86 05.11.86
P99311P99311	CP1019 EN004	Sam Hill Sam Hill	16.08.86 16.08.86

A composite primary key is needed to ensure that each record is unique – records wouldn't be unique if just Pupil_num was used.

These tables are now in **1NF**.

2NF - ***A table is in 2NF if it is in 1NF, and it has no partial dependencies, only functional dependencies.***

<u>This process only applies to tables that have a composite primary key.</u>

Functional Dependency - Each field in a table must depend <u>entirely</u> on the primary key.

In other words, if a value in the primary key changes, any values which would have to change don't belong in that table.

Pupil Num	Subject Num	Pupil Name	DOB
P99010	CP101	Jane Grey	12.03.86
P99205 P99205 P99205	CP101 MA110 PH190	Tom Jones Tom Jones Tom Jones	05.11.86 05.11.86 05.11.86
P99311P99311	CP1019 EN004	Sam Hill Sam Hill	16.08.86 16.08.86

Pupil

Subject Num	Subject	Lecturer Number	Lecturer Name
CP101	Computing	UH	Glover, T
MA110	Music	UG	Reader, B
PH190	Physics	58	Day, S
BS101	Business	UH	Newman, P

Subject

Subject(Subject_num, Subject, Lecturer Number, Lecturer Name)
Pupil (Pupil num, Subject_num, Pupil Name, DOB)

As **Pupil** is the only table with a composite primary key, we can ignore **Subject** for the moment.
What fields do not depend entirely on ***both*** parts of the primary key, and have created a lot of duplication?

Pupil Num	Subject Num	Pupil Name	DOB
P99010	CP101	Jane Grey	12.03.86
P99205 P99205 P99205	CP101 MA110 PH190	Tom Jones Tom Jones Tom Jones	05.11.86 05.11.86 05.11.86
P99311P99311	CP1019 EN004	Sam Hill Sam Hill	16.08.86 16.08.86

Pupil

Subject Num	Subject	Lecturer Number	Lecturer Name
CP101	Computing	UH	Glover, T
MA110	Music	UG	Reader, B
PH190	Physics	58	Day, S
BS101	Business	UH	Newman, P

Subject

These items do not depend on **both** parts of the primary key only **Pupil Num**, not **Subject Num**. We remove this data (apart from the primay key, which must remain), and place it into a new and sensibly named table.

2NF Tables

Pupil Num	Pupil Name	DOB
P99010	Jane Grey	12.03.86
P99205	Tom Jones	05.11.86
P99311	Sam Hill	16.08.86

Pupil

Subject Num	Subject	Lecturer Number	Lecturer Name
CP101	Computing	UH	Glover, T
MA110	Music	UG	Reader, B
PH190	Physics	58	Day, S
BS101	Business	UH	Newman, P

Pupil Num	Subject Num
P99010	CP101
P99205 P99205 P99205	CP101 MA110 PH190
P99311 P99311	CP1019 EN004

Options

Subject

Pupil (Pupil num, Pupil Name, DOB)
Subject(Subject_num, Subject, Lecturer Number, Lecturer Name)
Options(subject_num, pupil_num)

The tables are now in 2NF, and are already more sensibly organised, as there is much less duplication and likelihood of inconsistencies.

3NF

For a table to be in 3NF it must be in 2NF and have **no non-key dependencies**.

Non-key dependencies – any fields that are related and dependent on each other, and not the key field.

Pupil Num	Pupil Name	DOB
P99010	Jane Grey	12.03.86
P99205	Tom Jones	05.11.86
P99311	Sam Hill	16.08.86

Pupil

Subject Num	Subject	Lecturer Number	Lecturer Name
CP101	Computing	UH	Glover, T
MA110	Music	UG	Reader, B
PH190	Physics	58	Day, S
BS101	Business	UH	Newman, P

Subject

Pupil Num	Subject Num
P99010	CP101
P99205 P99205 P99205	CP101 MA110 PH190
P99311 P99311	CP1019 EN004

Options

Subject(Subject_num, Subject, Lecturer Number, Lecturer Name)
Options(subject_num, pupil_num)
Pupil (Pupil num, Pupil Name, DOB)

Which of these tables contain non-key dependencies?

Pupil Num	Pupil Name	DOB
P99010	Jane Grey	12.03.86
P99205	Tom Jones	05.11.86
P99311	Sam Hill	16.08.86

Pupil

Subject Num	Subject	Lecturer Number	Lecturer Name
CP101	Computing	UH	Glover, T
MA110	Music	UG	Reader, B
PH190	Physics	58	Day, S
BS101	Business	UH	Newman, P

Subject

Pupil Num	Subject Num
P99010	CP101
P99205 P99205 P99205	CP101 MA110 PH190
P99311 P99311	CP1019 EN004

Options

Subject(Subject_num, Subject, Lecturer Number, Lecturer Name)
Options(subject_num, pupil_num)
Pupil (Pupil num, Pupil Name, DOB)

Lecturer Name is a non-key dependency, as this is dependent on the **Lecturer Number – that is, if the lecturer number changes so will the lecturer name**. We remove **Lecturer** details to a different table., and we leave a copy of **Lecturer Num** so that a link between the tables is maintained.

3NF Tables

Subject

Subject Num	Subject	Lecturer Number
CP101	Computing	UH
MA110	Music	UG
PH190	Physics	58
BS101	Business	UH

Pupil Num	Pupil Name	DOB
P99010	Jane Grey	12.03.86
P99205	Tom Jones	05.11.86
P99311	Sam Hill	16.08.86

Pupil

Option

Pupil Num	Subject Num
P99010	CP101
P99205 P99205 P99205	CP101 MA110 PH190
P99311 P99311	CP1019 EN004

Lecturer Number	Lecturer Name
UH	Glover, T
UG	Reader B
58	Day, S
UH	Newman, P

Lecturer

Subject(Subject_num, Subject, Lecturer Number#)
Options(subject_num, pupil_num)
Pupil (Pupil num, Pupil Name, DOB)
Lecturer(Lecturer_number, Lecturer name)

The tables are now in 3NF

Topic 3 - HCI

What you need to know:

- **4.3.3 Human Computer Interface (HCI)**
  - The factors to be taken into account when designing a good user interface
    - *consistency of signposting and pop up information*
    - *on screen help*
    - *layout appropriate to task*
    - *differentiation between user expertise*
    - *clear navigational structure*
    - *use by disabled people*

Designing a good HCI

These factors must be taken into account when creating a HCI:

- consistency of signposting and pop-up information
- on-screen help
- House style/ethos
- Layout appropriate to task
- differentiation in user expertise
- clear navigational structure
- location of where machine is to be used
- customisable to suit the needs of the user
- use by disabled people.

HCI

Consistency of signposting and pop-up information

Users must always be clear on what to do next when using software. To help achieve this, HCI designers can ensure consistent use of **signposting** and **pop-up** information.

E.g. aids to navigation such as the **Next** and **Previous** buttons, pop-up menus, icons, etc., all look the same from screen to screen and all appear in the same position on the screen.

Navigation around the program should be clear, consistent and easy to follow – this will make the software more intuitive, so you can learn how to use it faster

HCI

On-screen help

An on-screen help facility helps users as they are using the software, instead of them having to look through printed manuals or user guides.

Help screens should explain things simply and use easy-to-follow examples .

The software should recognise and anticipate the users' goals and offer assistance to make the task easier. Microsoft Office uses Wizards that help you through some of the more complex tasks. This allows the users to accomplish their tasks in as short a period as possible.

HCI

Layout appropriate to task

You would not have the same layout for a piece of software for young children learning how to spell as you would have with a piece of CAD software used to design complex buildings. As these totally different tasks, they need a more appropriate screen layout.

For example, the interface to teach children spelling should:

- have a minimum amount of text on the screen
- use bright colours to attract young children to the package
- have an uncluttered appearance
- involve minimal use of the keyboard
- use speech synthesis so they can hear words.

HCI

The interface for CAD should:

- allow the user to customise the screen (e.g., include items they use and get rid of any items they don't)
- minimise mouse movements
- keep the working area of the screen as big as possible by:
  - Using pull-down menus
  - Using a large screen for complex interfaces , so more of the diagram can be seen on the screen at one time
  - Use input devices such as graphics pads/tablets so that selections can be made from the tablet rather than on on-screen menu
  - Design menus so that the most popular selections are at the top of the menu, to avoid the need to move down through the menu more than is necessary.

HCI

Differentiation in user expertise

A good HCI will cater for different levels of expertise at the same time. Customisable HCIs make allows the users to change the way their user interface works/looks to suit their work preference.

Provide short cuts for experts - experts often type very quickly and will be able to memorise commands using a combination of keys. This will be quicker than using the mouse to click on icons and menus.

More ways of performing the same operation – a beginner may prefer to use a drop down menu or click on an icon in order to print out a file whereas the experienced user may find it faster to issue a command using a sequence of keys such as Ctrl+P.

A beginner will also need easily accessible help utilities.

HCI

Where the PC is going to be used has an impact on the suitability of an HCI.

e.g. The HCI should avoid placing importance on the use of sound, if it is to be used in a noisy area.

- Touch screens may be suitable for use in museums, where an easy-to-use and reliable input method is needed

House Style/Ethos

A HCI for a piece of software used in a particular company must convey the house style and ethos of that company.

HCI

Clear navigational structure

- It speeds things up if there is a familiar route through the programs as users will not have to keep learning new layouts
- It must be clear to the users how to accomplish certain tasks, so for a complex task the user can be guided through using a series of small steps. E.g. the mail merge wizard in Word
- Forward and back buttons should always be in the same place on different screens. If a user wants to flick quickly through a series of pages, it is annoying to have to position the mouse before clicking.

HCI

Use by disabled people

- Sensory impaired users may not be able to read the letters on the screen properly, so the HCI should use a font that is easy to read and ensure that its size is large enough to read. The user should be given the option to customise their screen colour, contrast, font size.
- The blind can use a 'talking' computer where the words are spoken as they are input or output.
- Blind users can also use Braille keyboards to input data and Braille printers to produce output in Braille.
- Disabled people who are unable to write can use voice-recognition systems to input data.

Example 1: Teaching a child to read

- Have a minimum amount of text on screen
- Use child friendly font/size of font
- Use bright colours to attract the child's attention
- Have an uncluttered appearance
- Involve minimal use of the keyboard / alternative input devices
- Use speech synthesis / sound so that they can hear the words (sounds must relate to what's on-screen
- Animation/videos to keep their interest
- Instant feedback on their responses
- Interactivity e.g. quizzes, educational games
- Visual prompts e.g. *pictures of a cat if that is what they are being asked to read*

Example 2 - CAD

- Minimum amount of icons, leaving most of screen clear for diagrams
- Use a lot of keyboard shortcuts
- Options/tools can be selected from a graphics tablet rather than clicking on-screen
- Should allow tasks to be done as quickly as possible
- Keep mouse clicks to a minimum
- Allow interface to be customised, to choose a better colour scheme and turn off sounds

Topic 4 - The Internet

What you need to know:

- *Candidates should recognise the Internet as a network of networks.*
  - **The Impact of the Internet upon Business -** Candidates should understand the use of associated hardware and the advantages and disadvantages of:
    - (i) FTP
      - *Distribution of information between business and other organisations.*
    - (ii) E-commerce
      - *The requirements of interactive shopping, for example maintaining a company website, catalogue of stock, methods of secure payment, database of customer orders.*
      - *Advantages and disadvantages to both the customer and business.*
    - (iii) Online databases *How to access online information.*
      - *How a search engine works, how web pages are added to search engine lists.*
      - *Define and explain how the following can be used to access information:*
      - *URL's*
      - *Web crawlers*
      - *Boolean searches*
      - *Hyperlinks*
    - (iv) Distributed computing using the Internet
      - *Shared processing across the Internet and its advantages and disadvantages e.g. WHO's 'Popular Power' influenza research; music distribution; SETI research into radio signals.*
  - **Connecting to the Internet** *Candidates should be able to:*
    - Cable access to the Internet
      - *describe the use of and the advantages and disadvantages of Dialup and Broadband;*
    - Mobile access to Internet
      - *describe the use of and the advantages and disadvantages of mobile access to the Internet.*
  - **Moral, Social and Ethical Issues associated with the Internet**
    - *Candidates should show an awareness and understanding of:*
      - *censorship*
      - *accuracy of information*
      - *privacy*
      - *effects upon communities*
      - *ownership and control*

The impact upon businesses

The Internet is a huge group of networks joined together. Each of these networks consists of lots of smaller networks.

What is the difference between the Internet and the World Wide Web?

The Internet is a massive network of computers, the World Wide Web is a method of accessing and sharing resources using the Internet.

The impact upon businesses

FTP is a standard set of rules that have been established to allow the exchange of large files over the internet

Files can be transferred by using email attachments, but this method is slow and as transfer limit imposed by email providers is small, transfer of large files could be prevented. With FTP, you are not limited by file size, so extremely large files of any type can be transmitted.

- You are not limited to file size unlike with email attachments
- allows reliable transfer of files between platforms
- greater security in transfer of information

Examples:

- Used for uploading a database of sales from one branch of the organisation to the head office.
- Used to distribute information between the company and their customers and suppliers
- Used for down/uploading a website from/onto the internet/server .
- Transfer files from mac to pc.

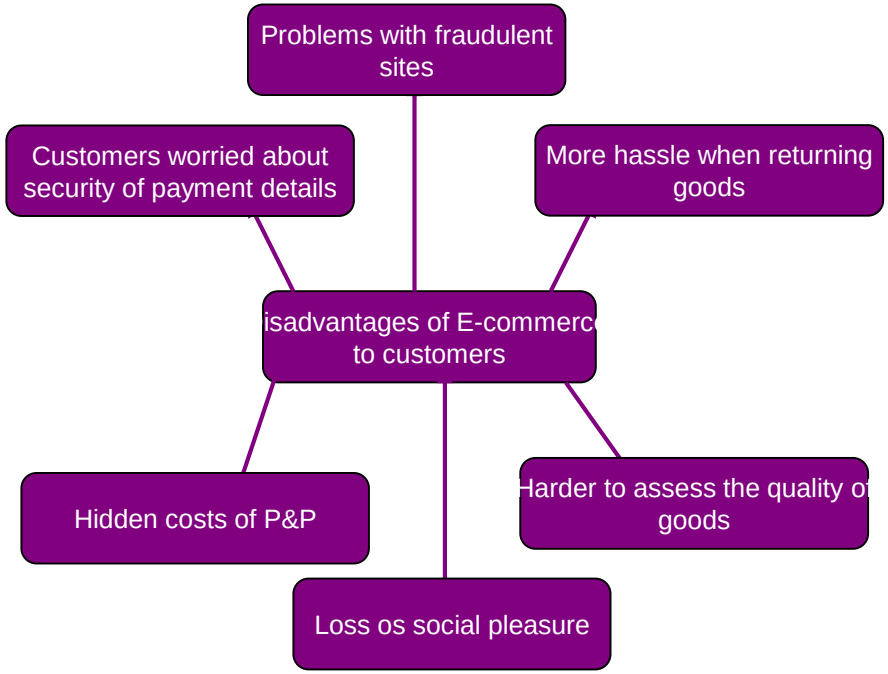
The impact upon businesses

E-commerce is the electronic activities needed for the successful running of a business:

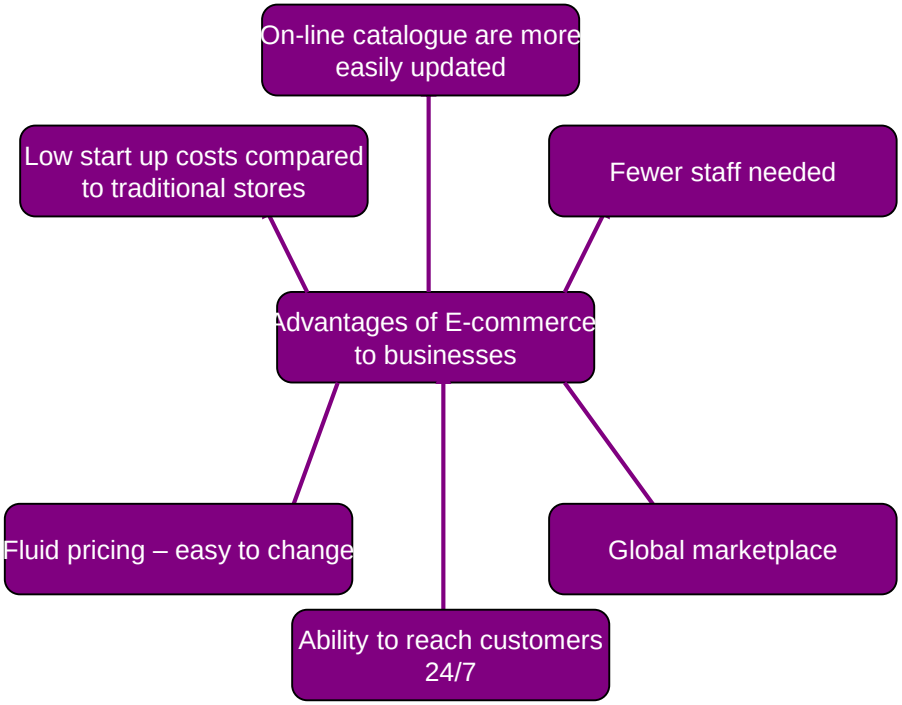
- Online marketing
- EFT (Electronic Fund Transfer)
- Just in time control systems/supply chain management
- EDI (Electronic Data Interchange)
- Automatic Stock Control
- Automated Data Entry

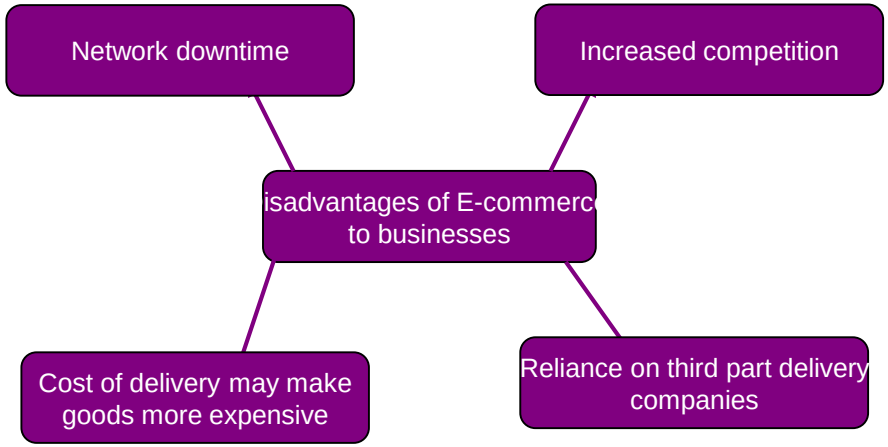
- <u>Requirements for an on-line shopping service</u>
  - On-line catalogue of products and a search facility, and all linked to the stock control system
  - Shopping basket to store items for purchase
  - Checkout
  - Secure payment methods
  - Trained staff to create and maintain the web-site
  - Database of customer orders (used for marketing, repeat orders or in case of returns)

The impact upon businesses



The impact upon businesses





The impact upon businesses

On-line Databases

When using networked computers, users can share a the same database, thus avoiding data duplication and redundancy. E-commerce use databases in this way, using **Electronic Data Interchange** (EDI). EDI is where companies automatically transfer data without requiring any paperwork.

For example, the ordering , checking and payment for goods automatically.

The impact upon businesses

Accessing Information On-line

Information can be accessed on the Internet by:

1. **Typing in the URL** (Universal Resource Locator) is the web address of a site, or the unique address for a file that is accessible on the Internet. ***If you know the website address, you simply type it in to go directly to the website you want.***
2. ***Surfing the Internet by following hyperlinks, clicking on a link to move from one area of interest to another.***
3. ***Using a search engine by entering key words and pressing enter,*** and the program searches for any matches.
4. ***The use of a web crawler which browses the web and keeps an index of what it finds***

The impact upon businesses

Search engines

A search engine uses an index of hundreds of millions of web-sites; this is done automatically using a **web crawler to *browse all web pages in a systematic manner, following every hyperlink and keeps an index of what it finds***. This data is then added to the search engine's main index.

When a search is performed, the index is checked and any relevant sites, along with a some brief details, are retrieved in order of relevance.

- Can be used for automating maintenance tasks on a Web site, such as checking links or validating HTML code.
- Can be used to gather specific types of information from Web pages, such as harvesting e-mail addresses (for spam purposes)

The impact upon businesses

Using Search Engines

Boolean searches – ***the use of AND, OR and NOT to include or exclude information.***

- Using **AND** narrows a search by combining terms; it will retrieve documents that use both the
- search terms you specify, (e.g. Portland **AND** Oregon)
- Using **OR** broadens a search to include results that contain either of the words you type in, (e.g. liberal **OR** democrat)
- Using **NOT** will narrow a search by excluding certain search terms, (e.g. France **NOT** Canada)
- It helps save time searching for information as it helps you narrow down a search.

The impact upon businesses

Distributed Computing

Distributed Computing – a series of computers are networked together and they each work on solving the same problem by sharing data processing, storage and bandwidth

Some problems generate so much data, that processing it requires a huge amount of resources and time. One solution would be to use an expensive supercomputer, another option is to use distributed computing. More, less powerful computers are networked via the Internet, and work together on the same problem. In many cases, users are donating the use of their idle computers to work on tasks that have a common good.

DO NOT CONFUSE THIS TOPIC WITH DISTRIBUTED DATABASES

The impact upon businesses

Examples of Distributed Computing applications:

- **The SETI** (Search for Extraterrestrial Intelligence) **Project -** The purpose of the SETI project is to search for intelligent life outside the Earth and to do this a radio telescope is used. Supercomputers were used in order to process the vast amount of data. Then someone came up with the idea of using a virtual supercomputer consisting of a huge number of Internet-connected home computers.
- **Developing Flu Vaccines**
- **Folding@home** – cancer, Alzheimer's, Parkinson's, etc.
- Climate research

The impact upon businesses

Advantages of distributed computing

- reduces cost because an expensive powerful computer such as a supercomputer is not needed
- can pass work to computers anywhere in the world using the Internet
- improved performance as each computer can work on part of the data.

Disadvantage of distributed computing

- issues with the security of data spread out on so many different computers.
- Heavy reliance on networks and communications which may not always be reliable
- Increased costs owing to the use of expensive communication lines

Connecting to the Internet

Connecting to the Internet

The Internet can be accessed using ***Dialup***, ***Broadband*** and ***mobile broadband***

Dialup uses a telephone line and a **modem** to connect to the Internet. A modem converts digital signals into sounds which are passed along a telephone line. The receiving PC converts the sound back to a digital signal so it can be understood.

- ✓ Relatively cheap, as you only pay for when you are connected to the internet.
- ✘ Very low ***bandwidth*** (the speed of data transmission) and this limits its use.
- ✘ You cannot use the telephone for conversations whilst connected to the Internet.

Connecting to the Internet

Broadband

Broadband is an always-on, high bandwidth data connection.

It gives much faster access and transfer speeds to the Internet, allowing you to watch video on demand (VOD), download files quickly, listen to radio, watch TV programmes and so on. None of these would be possible without a fast broadband connection.

Connecting to the Internet

Advantages of broadband

- ✓ Files can be downloaded quickly.
- ✓ Allows you can to use the phone while you are on-line.
- ✓ Can listen to radio, watch video (VOD) and play on-line games.
- ✓ No time is wasted connecting to the Internet, as it is always on (this allows virus checkers to automatically update their files.)
- ✓ Web-cams and videoconferencing can be used.
- ✓ Cheap phone calls can be made using the Internet (VOIP).
- ✗ Relatively expensive monthly subscriptions.
- ✗ High bandwidth allows illegal downloading of films or music.
- ✗ Broadband may not be available where you live.

Connecting to the Internet

Mobile Broadband

Accessing the Internet via mobile phones or usb 'dongles'.

- ✓ Allows for fast Internet access on the go.
- ✓ Allows for more productivity – i.e. tasks can be done as soon as you think of them
- ✘ Can be very expensive and have a small download limit.
- ✘ Connection and speed is dependent on signal
- ✘ Security

Moral, Social and Ethical Issues associated with the Internet

Moral, Ethical and Social Issues Associated with the Internet

Moral – issues of right and wrong, and how people should behave.

Ethical - matters that are not strictly illegal, but could be considered wrong.

Social – factors that are affecting society

In the exam, you will be asked to give your own opinions on how the Internet has affected society. This unit is less about being right or wrong, but more about being able to justify your opinions.

Moral, Social and Ethical Issues associated with the Internet

Moral Issues

Lack of control over the internet

- Unless filtering software is used, children can **easily gain access to pornographic or violent images**.
- **Lack of policing** of the internet means that information is not checked to ensure that it is correct, very hard for children to be able to check the accuracy of the information.
- Laws cover the production or distribution of pornographic material but as much of the material comes from other countries, where it might be legal, not much can be done to stop it.
- Concern that paedophiles may use the Internet for distributing pornographic pictures of young children and they also can use it to lure children into meetings with them after they have spoken to them in chat rooms.
- **Inappropriate web-sites** - people are able to view inappropriate material such as pornography, racism, violent videos, how to make explosives, etc.

Moral, Social and Ethical Issues associated with the Internet

- **Creating deliberately misleading web-sites** - people may rely on and use this information thinking it is correct. Websites can be biased and give misleading information.
- **Bullying** – in chat rooms, by e-mail, in blogs, by text message is a problem especially for the young.
- **it is easy to spread rumours using the Internet**. You only have to tell a few people in a chat room and the rumour will soon spread. Normally, if someone started a rumour that was untrue and it caused another person distress, then the person starting the rumour could be sued. When rumours are started over the Internet it is difficult to identify the person responsible.
- **Using e-mail to give bad news** (e.g. redundancy, demotion, firing, etc.) when explaining face-to-face would have been better.
- **Illegal sharing** of movies, music, etc., denies copyright owners of profit.

Moral, Social and Ethical Issues associated with the Internet

Ethical issues

- **Plagiarism/essay banks** - copying material without attributing or referencing the source of the information. This could also involve using websites which sell essays or coursework. This could devalue qualifications, and is also cheating. This could result in being disqualified for exams or expelled from university.
- **Spam** – (i.e. the same advertising e-mail to millions of people) – people waste time deleting spam if the spam filter allows it through.
- **Stealing wireless Internet bandwidth** - Using someone's wireless Internet connection without permission. Sometimes it is possible to connect to the Internet using an open network. The net result of using the network is to slow the network down for legitimate users, or use it for illegal purposes.
- **Manipulating images** - by using photo/video editing software you can distort reality and you can no longer believe what you see in video, TV, newspapers, magazines and on websites.
- **Companies monitoring staff use of email or internet** - Some organisations will even read personal e-mails.

Moral, Social and Ethical Issues associated with the Internet

Social issues

- **Privacy** - social networking sites, e-commerce sites, Internet service provider records, e-mail monitoring at work, etc., all erode a user's privacy.
- It is relatively easy to capture internet traffic. In the light of the increase in Internet crime, security scares and increased terrorist activity should the security services be allowed to monitor all Internet traffic?
- **Gambling addiction** - gambling can cause many social problems and it is on the rise with the ease with which bets can be made using the Internet.
- **Gaming addiction/Obesity** - many children spend hours playing computer games and their social skills and schoolwork can suffer as a result.
- Outsourcing call centres
- **Widens social gap** - Have and have nots – Digital divide
- **Impact of e-commerce on traditional sellers** – businesses closing because they cannot compete.

Moral, Social and Ethical Issues associated with the Internet

Control and censorship of the internet

- **Ownership of the Internet** - no-one owns the Internet. People have the right to say what they want. The internet is international. Material which would be illegal if published in hard copy form is freely available on the Internet e.g. racist propaganda, bomb making instructions, pornography.
- Some say the Internet should be censored but who will do the censoring and how can control be implemented? Will governments start censoring information that shows them in a bad light?
- If you ban sites will they become more appealing so people will search for them more avidly.
- **The availability of offensive material**
- **Censorship** Invasion of privacy by governments. (e.g. China)
- **Freedom of speech**. Do we have the right to the privacy of our emails and data files? Do we have the right to encrypt our data?
- **Effects on communities** – people are interacting less in real-life, and more on social networks/mobile phones.
- **The internet can negatively influence vulnerable people** e.g. inciting people to become terrorists, suicide, etc.

Topic 5 - ICT Policies

What you need to know:

- Candidates should understand:
  - the potential threats and consequences for data misuse and understand the need for backup procedures
  - *Threats*
    - *Terrorism*
    - *Natural disasters*
    - *Sabotage*
    - *Fire*
    - *Theft*
  - *Consequences*
    - *Loss of business and income*
    - *Loss of reputation*
    - *Legal action*
- The factors to take into account when designing security policies
  - *Physical security*
  - *Prevention of misuse*
  - *Audit trails for detection*
  - *Continuous investigation of irregularities*
  - *System Access - establishing procedures for accessing data such as log on procedures, firewalls*
  - *Personnel administration*
  - *Operational procedures including disaster recovery planning and dealing with threats from viruses*
  - *Staff code of conduct and responsibilities*
  - *Disciplinary procedures.*
- Operational procedures for preventing misuse
  - *Screening potential employees*
  - *Routines for distributing updated virus information and virus scanning procedures*
  - *Define procedures for downloading from the Internet, use of floppy discs, personal backup procedures*
  - *Establish security rights for updating web pages*
  - *Establish a disaster recovery programme*
  - *Set up auditing procedures (Audit trails) to detect misuse.*

What you need to know:

- Prevention of accidental misuse
  - *Backup and recovery procedures*
  - *Standard backups to floppy disc*
  - *RAID systems – mirror discs (Redundant Array of Inexpensive Disc)*
  - *Grandfather, Father, Son systems*
  - *Backing up program files.*
- Prevention of deliberate crimes or misuse
  - *Methods for controlling access to computer rooms*
  - *Methods of securing integrity of transmitted data e.g. encryption methods including private and public keys. Call back procedures for remote access*
  - *Establish firewalls*
  - *Proxy servers*
  - *Methods to define security status and access rights for users*
  - *Methods for physical protection of hardware and software*
  - *Security of document filing systems.*
- **Factors determining how much a company spends to develop control, minimising risk**
  - Risk Analysis
  - *Identify potential risks*
  - *Likelihood of risk occurring*
  - *Short and long term consequences of threat*
  - *How well equipped is the company to deal with threat*

Security policies

Risk Analysis - ***assessing the likelihood of threats occurring, estimating the cost of the damage they could cause and what can be done at reasonable cost to eliminate or minimise the risk.***

- **Identify potential risks or threats**
- **Likelihood of risk occurring** - power cuts are inevitable but explosions much less likely - senior managers have to assess the likelihood of each risk occurring and put in the necessary security to prevent it happening (if possible).
- **Short and long term consequences of threat** - resources (staff equipment, etc.) need to be allocated to recover the data or hardware; the business may have to pay compensation; financial loss due to loss of business through not being able to take orders; loss of public trust can cause embarrassment or loss of business; prosecution under Data Protection Act; bankruptcy; cost of replacing equipment
- **How well equipped is the company to deal with the threat?** – What procedures are in place to cope with the threat? Does the company have the resources to cope with threats? This is reviewed periodically because of changing needs and circumstances.

Threats to ICT systems

Threats to ICT systems can cause the business to lose money because of:

- Legal action – *keeping data secure is a part of the data protection act. Failure to do so will lead to prosecution*
- Lost business
- Consumer confidence
- Lost computer time
- Staff time sorting out the problems.

Threats to ICT systems

Short term consequences of losing data

The main consequences of losing data are:

- **Loss of business and income** – losing details of customers and their orders will mean the company will not know that a customer has placed an order and they will not know whether an order has been paid for.

Long-term consequences of losing data

- **Loss of reputation** – organisations will not look good if they cannot look after data properly. There have been many recent news stories about government departments losing personal data.
- **Legal action** - there is a requirement under the Data Protection Act 1998 for organisations to keep personal data safe. Organisations who fail to do this will face prosecution.
- **Going out of business**

Sources of threats

- **Viruses**
- **Adware**
- **Spyware**
- **Hacking**
- **Deliberate abuse/sabotage**
- **Accidental abuse**
- **Natural disaster**
- **Fire**
- **Terrorism**
- **Theft**
- **Faulty hardware or software**

Natural Disasters

Whilst seldom an issue in Britain, natural disasters have to be considered and prepared for:

Earthquakes, floods, volcanoes, tidal waves, gales, etc. – loss of power and communication systems, damaged ICT equipment

Lightning strikes – momentary power loss can cause data loss or damage equipment

Best ways of safeguarding against these are proper backup procedures and a detailed disaster plan.

Faulty Hardware/software

- **Faulty hardware -** computer hardware is usually reliable but can and does break down, so you have to be prepared for this. The main problem would be caused by the hard drive becoming damaged, rendering the data and the programs unusable.
- **Faulty software -** software, especially bespoke software and sometimes packaged software, can contain errors (or bugs as they are called) and these can cause damage or loss of data.

Best way of safeguarding against this is proper backup procedures, regular hardware checks and use reliable software bought from a reputable retailer.

Threats from fire

Some precautions that need to be taken:

- no smoking in any computer rooms
- power sockets should not be overloaded
- wiring should be checked regularly for safety
- bins should be emptied regularly
- do not leave large quantities of paper lying around
- fire alarms/smoke detectors in all rooms
- install a sprinkler system
- Store backup media in fireproof safes
- remove backup copies off-site.

Theft

If a computer is stolen then the hardware, software and data will be lost. A firm may be in contravention of the Data Protection Act 1998 if it can be proved that they did not have adequate security to prevent the loss of any personal data stored.

Computer theft is common, particularly with laptops. Laptops are particularly vulnerable to theft because they are:

- small, light and easily concealed
- often used in public places (cafes, on a train, at an airport, etc.)
- put into car boots
- very desirable and easy to sell by thieves.

Best way of safeguarding against this is avoid the use of laptops, use encryption and physical security methods.

Hacking

Hacking involves attempting to or actually breaking into a secure computer system. Hacking is usually done remotely, using the Internet. Usually a hacker is a proficient programmer and has the technical knowledge to be able to exploit the weaknesses in a security system. Once a hacker has gained access to an ICT system they may:

- do nothing and be content that they have managed to gain access
- gain access to sensitive or personal data
- use personal data to commit blackmail
- cause damage to data, viruses, DOS attacks
- deliberately alter data to commit fraud.

Best way of safeguarding against this is to use firewalls which are kept up-to-date

Viruses

Viruses – a software program designed to disrupt the operation of a computer system, by attaching itself to files that are distributed (often via email)

Connecting to the Internet increases the risk of viruses being spread to the internal network. The latest virus scanning and removal software should be installed on all computers. **Best way of safeguarding against this is to use anti-virus software which is kept up-to-date**

- ***Denial of service attacks (DOS)* -** an attack on a secure system of an organisation so that the organisation is deprived of some of their resources. E.g., a DOS attack on an on-line bookshop could mean that the bookshop's network is so overwhelmed with requests that there is a temporary loss of network connectivity. Orders cannot now be placed, costing the business money.

Can be prevented by blocking repeated access attempts from a particular IP address.

Problems with power loss

- A standby power system keeps the power running until the mains power is restored. Standby power will usually consist of either stored power (for short losses of power) or a combination of stored power and a generator. Stored power consists of banks of batteries. Generator power is generated using diesel or petrol.
- Because there is a slight delay between losing the power and starting the generator, batteries are also needed to provide power during this interval.

Best way of safeguarding against this is to use battery-powered UPS (uninterruptible power supply), which will immediately provide power to the file-server, so work can be saved properly.

Problems with power loss

Changes in the power supply

Power fluctuations, sometimes called spikes and surges, occur more often than complete power loss. You notice these when your lights start to flicker. Power fluctuations can cause problems with computers and can be a cause of data loss

Best way of safeguarding against this is to use surge-protectors

Worms (*a self-replicating program that disrupts a PC by consuming increasing amounts of system resources*)

Adware (a software package which automatically displays or downloads advertisements to a computer)

Spyware a software package that can be unknowingly installed on computers, and which collects small pieces of information about users without their knowledge, and transmits this over to the internet, where it can be abused.

Best way of safeguarding against this is to use anti-virus software which is kept up-to-date

Security Policy

What is a security policy?

A security policy is a programme of actions to follow in order to protect an ICT system or its data.

Why is a security policy needed?

The Data Protection Act puts a responsibility on businesses to keep information secure because of its potential for misuse.

Security Policy

What would you find in a security policy?

1. **Prevention of misuse**
2. **Continuous investigation of irregularities**
3. **System access procedures**
4. **Personnel administration**
5. **Operational procedures**
6. **Code of conduct/Disciplinary procedures (***See Working with ICT 2***)**
7. **Disaster recovery planning**

Security Policy

1. **Prevention of misuse – stopping people access the ICT system or data, so they can't damage it:**

A - Physical methods –

- Controlling access to the room by using keypads, swipe cards or biometric fingerprint or iris recognition.
- Controlling access to the building by the using security guards who will challenge visitors, log people in and out of the building and ensure access to rooms is controlled, etc.
- Locks on PCs to stop them from being switched on.
- Locking the computers away at night or securing them under steel covers prevents access or theft.
- Use security cameras in computer rooms
- Securing computers to desks using strong metal cables –
- evices that prevent CD/DVD drives or USB ports from being accessed
- Use a fireproof safe for the storage of data on portable storage media

Security Policy

B - Logical security (Software security)

Software security usually involves:

- **log-ins** and **passwords**
- **Hierarchy of access** for programs, files and data.
- **Audit logs/trails**
- **Encryption** – coding data before they are transmitted to prevent hackers from understanding the data.
- **Proxy servers** – prevents unauthorised access to blocked content on the internet (can also be hardware).

Security Policy

2. **Continuous investigation of irregularities –**identifying misuse of credit/debit cards by querying any transactions that are out of the ordinary for that customer.

- **Irregularities in places** -sometimes credit card payments for large amounts abroad are rejected by the credit card company. The credit card company ask the purchaser to contact them so they can ask them a series of questions to verify that they are the genuine card holder and that the transaction is genuine.
- **Irregularities in amounts** – for some expensive, out of character purchases, the bank will ask the customer to contact them so they can check that the transaction is genuine and that no-one is using their identity illegally.

Security Policy

3. System access procedures

Log-in procedures

- User accounts, passwords, audit logs, etc. See ***IT3.1 Networks 3***, slides 4 and 5 for more details.

Data access rights restrict a user's access to only those files they need in order to perform their job. Their rights are allocated by the network manager and enforced by the network software when they log on.

Users have different levels of access to files including:

- **Read only** - a user can only read data, not alter or delete it.
- **Read/write** - a user can and alter data
- **Append** - they can add new records but cannot alter or delete existing records.
- **No access** - they cannot even open the file.

Security Policy

4. Personnel administration

Staff should be managed properly to prevent them from misusing ICT facilities.

Personnel administration includes:

- **Training** - means staff are less likely to disobey the code of conduct, less likely to make mistakes with data, less likely to lose work, etc.
- **Fitting the employee to the task** - ensuring that the employee's knowledge and skills match the task they have to complete.
- **Ensuring that staff are controlled** - managers should ensure staff are working safely and are ensuring the privacy and security of the data they are using.
- **Ensuring all users follow a code of conduct**
- **Rotation of staff duties** to prevent fraud, since one group could discover the fraud committed by the other.
- **Disaster recovery training,** so everyone knows what to do if some or all of the ICT facilities are lost.

Security Policy

5 – Operational Procedures.

Managers can put these procedures into place to help prevent employees misusing ICT facilities:

A Virus procedures

B Downloading procedures

C Audit procedures

D Backup and recovery procedures

Security Policy

A - Virus Procedures

Preventing viruses

- Use regularly updated anti-virus checking software
- do not open e-mails or attachments from unknown sources
- train staff to be aware of the problems and how they can help
- do not allow programs such as games, video or movies to be downloaded onto the organisation's ICT systems
- Prevent users being able to use their own removable media floppy disks, removable magnetic drives).

Security Policy

B - Downloading Procedures

- Download files to a memory stick, not the main network. Scan this file and if clean, move it to the desired folder on your system.
- Do not install any software downloaded off the Internet onto company networks as these may contain viruses or be illegal.
- Do not use too much disk space by storing large downloaded files, or keep the files for longer than necessary.
- Users could store their own data on portable media or in a way that they can work on the files at home (e.g. cloud storage). Portable media should be scanned first, what data can be transferred, etc.).
- Do not allow personal data to be downloaded onto laptops, portable storage media or transferred as a file attachment .

Security Policy

C - Auditing procedures (audit trails) to detect misuse - See **Networks 3.1, slide 5**

D. Backup and recovery procedures

Backup procedures - the actions a person or organisation can take to ensure that regular backup copies are taken.

- ***keep backup copies*** off-site
- ***Keeping backup copies in a fireproof safe*** **-** However, they are only fireproof for a certain period of time - usually two hours.
- **make one person responsible** for the taking of backups
- **rehearse backup recovery procedures** - you need to be sure it is possible and you know how to recover data
- **Schedule back-ups to be taken at an off-peak time**, such as overnight.

Security Policy

Backup storage devices and media

- ***Magnetic tape* –** cheap, high storage capacity.
- ***Magnetic disk*** (e.g. hard disk) – copying the contents of one magnetic disk onto a different magnetic disk.
- ***Optical media* -** This includes media such as CD-R, CD-RW, DVD-RW, etc. Backup-rate is slow, but these are quite cheap.
- ***Pen/flash drives* -** These are very popular as they are small and portable and are ideal for backing up quite large amounts of work. They are also easily lost or stolen.
- **RAID systems (Redundant Array of Inexpensive Discs)- mirror discs -** Raid systems often have two hard disks. One is used as the main storage area, the second is an exact copy of the other hard disk. This way there is an immediate back-up source in place.

Security Policy

The grandfather, father, son system (the ancestral file system)

Large ICT systems use ***master*** files and ***transaction*** files. The master file is the most complete version of a file, and transaction files hold details of all the business transactions since the master file was last updated. The transaction file updates the master file.

Using the grandfather-father-son principle it is possible to recreate the master file if it is lost.

- Three generations of files are kept. The oldest master file is called the ***grandfather*** file and is kept with its transaction file. These two files are used to produce a new master file called the ***father*** file that, with its transaction file, is used to create the most up-to-date file, called the ***son*** file.
- The process is repeated and the son becomes the father and the father becomes the grandfather and so on. Only three generations are needed and the other files may be re-used.

Security Policy

Backing up program files

In many cases programs, if lost, can usually be recovered easily as the original disks can be used to load the files back onto the system. Increasing numbers of programs are downloaded from the Internet, so if the originals are damaged or lost, then the software producers will allow them to be downloaded again.

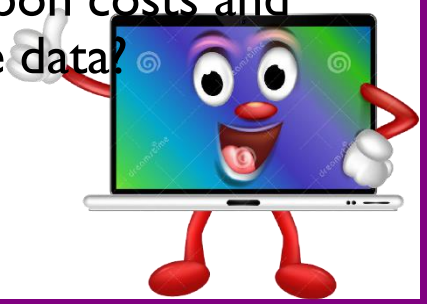
Many companies develop their own software or spend a considerable time customising existing programs so they work better for their organisation. In this case the programs need to be backed up originally and at any time new changes are made

Security Policy

- **7 – Disaster Recovery Planning - *Ensuring the availability of key services should a disaster occur.***
- Parts of a disaster recovery programme:
- **Cost**
- **Risk**
- **Data**
- **Hardware/software/communications**
- **Personnel, responsibilities and training**
- **Procedures**

Security Policy

- **Cost**
- Set up a budget for it
- What backup medium should be used, as this will affect the cost (e.g. Tape or disc/ Raid systems vary in efficiency and cost)
- Is hardware insured or will it need to be replaced
- Software can be re-installed. (or de-bugged by the programming department).
- **Risk**
- What problems could occur?
- What is the likelihood of them occurring e.g. are we going to get an earthquake in UK?
- Will data need to be stored on site or off site depending upon costs and the likelihood of the risk occurring and the criticality of the data?



Security Policy

Data

- Backups of all data should be regularly made. This means that the worst case scenario is that the business has to go back to the situation of the last backup and carry on from there. Backups may take a long time – often carried out overnight.

Hardware/Software/Communications

The total or partial loss of

  - computing equipment or software
  - telecommunications equipment or services
  - premises housing the IT equipment.
  - essential services such as electricity, heating or air conditioning
- Alternative communication /computer systems may be arranged in case a network goes down or alternative power supply.

Security Policy

Personnel, Responsibilities and Training

- The loss of certain key employees (illness, death, alternative employment)
- The loss of maintenance or support
- Make one person responsible for backups so people don't think others are doing it and it does not get done or do they use online backup companies or both
- Screening potential employees
- Virus information and virus scanning procedures
- Downloading from the Internet, use of floppy discs, personal backup procedures
- Staff code of conduct for using computer systems
- What response should staff make when the disaster occurs

Security Policy

Procedures

- Produce procedures for minimising the risks
- Test the plan on a regular basis to make sure it still sufficient
- Establish physical protection system (firewalls etc.)
- Establish security rights for file access and updating web pages
- Establish a disaster recovery programme. This starts with a backup policy to secure the data so it can be recovered later e.g. backup procedures required.
- How often should backups be taken?
- Restoration policy backup every day/hour and rotate tapes to ensure there is always a copy to restore files
- What type of backup? Where the backup is to be stored?
- Decide upon types of backup full, incremental or differential depending upon how many items of data are changed
- Set up auditing procedures (Audit trails) to detect misuse
- Premises relocation

Topic 6 - Working With ICT

What you need to know:

- **Telecommuting**
  - Teleworking
    - *'Working from home using computer networks'.*
    - *Use and associated hardware.*
    - *Advantages and disadvantages for the organisation and individual.*
  - Video-conferencing
    - *Use and associated hardware.*
    - *Advantages and disadvantages for the organisation and individual.*
- **Codes of Conduct**
  - Definition
    - *An agreement made by an employee to obey the rules of the organisation and work within specified guidelines as regards use of ICT and the Internet.*
  - Potential problems
    - *Introduction of viruses. Misuse of ICT such as using an organisation's printers for personal work. Using the Internet and running up telephone bills for own purposes, using company time for personal email.*
    - *Distribution of material that is racially or sexually offensive.*
    - *Misuse of data for illicit purposes.*
    - *Inappropriate use of mobiles phones – in restaurants, schools, public transport.*
    - *Blackmail, computer fraud or selling to other organisations.*
    - *Violating terms of copyright or software agreements.*
  - Contents of a code of conduct
    - *Responsibilities*
    - *Respecting rights of others*
    - *Abiding by current legislation*
    - *Protecting hardware and software from malicious damage*

What you need to know:

- *Complying with licensing agreements*
- *Authorisation*
- *Permissions on data access*
- *Security defining rules about password disclosure, personal use of emails and the Internet and data transfer rules*
- *Penalties for misuse*
  - *informal warnings*
  - *written warnings*
  - *dismissal*
  - *prosecution*

– Difference between Legal and Moral issues with respect to codes of conduct
  - ***Disinformation***
    - *Not fully informing potential customers or clients of all available facts concerning products or services e.g. imminent introduction of new models.*
  - ***Privacy***
    - *Informing data subjects of their legal rights and processes for complying with those rights.*
    - *Monitoring company emails.*
  - ***Employment patterns***
    - *Effects upon the workforce.*
    - *Personal empowerment.*
  - ***Equity***
    - *Information poor and information rich societies and the consequences of such.*
  - ***Intellectual property rights***
    - *Ownership rights to data.*

Teleworking/Telecommuting

Teleworking – using ICT communications systems to save a journey (e.g. videoconferencing)

Telecommuting – performing job-related tasks by using ICT communications systems to send and receive data to/from a central office, without having to be present at the office.

Whilst these are two separate terms, in the exam they will be considered synonymous.

Telecommuting Requirements

- e-mail access
- mobile computing
- mobile phones
- data warehouses (where all the organisation's data is kept in a huge, single database)
- computer
- Fast broadband and Internet connection (wireless router, cable router, etc.)
- microphone (used for videoconferencing)
- webcam (used for videoconferencing)
- internet phone (for making phone calls over the Internet)
- printer.

Jobs/People suiting telecommuting

Some jobs are ideally suited for working from home. Examples are:

- programmers, website designers, accountants, data entry clerks, etc.

The employee must be trusted. If personal or sensitive data needs to be sent, the employee must keep this data safe and private.

The employee must be self-motivated. There are plenty of distractions at home.

- he employee must have a place to work. They will need room in their house for the equipment needed

Benefits/Drawbacks of Telecommuting

To the employees

- ✓ No travelling expenses/time wasted
- ✓ Work more flexible hours
- ✓ Ideal for disabled/family commitments
- ✓ Less stressful
- ✓ makes it easier for people to live and work where they choose, as it is possible for some staff to work from home (less stressful).
- ✘ Home costs increase (furniture/lighting/heating)
- ✘ Less social contact
- ✘ Less pay
- ✘ More distractions

Benefits/Drawbacks of Telecommuting

To the business

- ✓ Smaller offices/less furniture/running costs
- ✓ Flexible staff hours
- ✓ Reduce
- ✓ Less staff illness?
- ✓ Less ancillary staff (cleaners, etc.)
- ✘ How hard are staff working?
- ✘ Harder to manage staff
- ✘ Meetings can be difficult
- ✘ Security risks of data transfer
- ✘ Health and safety checks needed on employee homes

Videoconferencing

Videoconferencing allows two or more people in different locations to see and talk to each other, exchange digital files, and enable users to share computer applications and even work concurrently on the same file.

Uses: Education, medicine (meetings about patients, exchange digital copies of x-rays, rural consultations, interpreting services, remote consultations with experts), and business meetings.

Videoconferencing Requirements

Hardware

- High specification multimedia PC
- Video cameras or webcams - sometimes the cameras can be operated remotely so it is possible to zoom in on a particular speaker
- Microphones
- A computer screen or display allowing many people to view the picture
- Loudspeakers
- A connection to a high speed digital network

Software

- Because of the high bandwidth requirements for the video and audio, it is necessary to compress and decompress the signals in real time and this is done using a device or software called a codec (coder/decoder). Sometimes the codec (to code/decode the signals) is hardware.

Benefits of Videoconferencing

Benefits to the employee

- Less stress as employees do not have to experience delays at airports, accidents, road works, etc.
- Improved family life as less time spent away from home staying in hotels.
- They do not have to put in long working hours travelling to and from meetings.

Benefits of Videoconferencing

Benefits to the organisation

- Less costs, as they do not have to spend money on travelling expenses, hotel rooms, meals, etc.
- Improved productivity of employees as they are not wasting time travelling.
- Meetings can be called at very short notice without too much planning.
- Short meetings can be conducted where it would not be feasible for people to travel long distances for such short meetings.

Benefits of Videoconferencing

Benefits to society

- Fewer people flying to meetings will cut down on the number of flights needed and hence reduce the amount of carbon dioxide emitted helping to reduce global warming.
- Roads will not be clogged up with traffic and this will cause less stress and cut down on pollution.

Limitations of Videoconferencing

Disadvantages/limitations of videoconferencing

- Specialist videoconferencing equipment is expensive.
- Poor image and sound quality owing to the compression/decompression of signals sent over the communication links.
- People can feel very self-conscious when using videoconferencing and may fail to come across well.
- Although documents and diagrams in digital form can be passed around, an actual product or component cannot be passed around.

Codes of Conduct

A code of conduct is a list of rules and expectations governing the use of ICT equipment within an organisation. An agreement to follow the code of conduct is written in to the terms of employment of all employees.

Without a code of conduct, employees can do whatever they want with ICT equipment. This can cause the organisation problems, some of which could result in them being fined.

Should an employee decide not to obey the code of conduct, then they will be subject to a series of disciplinary procedures which can eventually include dismissal.

Codes of Conduct

Problems when employees misuse ICT in the workplace include:

- Introduction of viruses by downloading games, not scanning portable media, not keeping virus scanners up-to-date, etc.
- Misuse of the ICT facilities (internet, e-mail, videoconferencing, printers, etc.) or use for personal reasons.
- Distribution of racially or sexually offensive material - e.g. sending offensive jokes by e-mail or text messages, circulating offensive images over the organisation's network.
- Misuse of data for illicit purposes - for example, using e-mails and text messaging to bully someone at work/school.
- Blackmail, computer fraud or selling to other organisations.
- Violating copyright or software agreements, causing the company to face legal action from affected organisations

What does a code of conduct contain?

- Responsibilities
- Respecting the rights of others
- Abiding by current legislation
- Complying with licensing agreements
- Authorisation
- Data access permissions
- Security policy
- Security

What does a code of conduct contain?

Responsibilities

All employees are responsible for the security and the integrity of the resources under their control.

- Users must respect the rights of other users, respect the integrity of the physical facilities and controls and comply with all software licences and contractual agreements.
- Users must act responsibly by ensuring that viruses are not introduced through failure to scan media, etc.
- They must ensure that they are not negligent by leaving their computer logged in so others can access the data, not leaving laptops where they are easily stolen and so on.

What does a code of conduct contain?

Respecting the rights of others

ICT systems such as e-mail, blogs and chat rooms can be misused. E.g., they may spread false rumours or bully a person. Employees need to feel safe in the workplace, so all employees must respect each other.

Abiding by current legislation

- Employees must act in accordance with the Data Protection Act 1998, The Computer Misuse Act 1990 and The Copyright, Designs and Patents Act 1988. Failure to do so is serious and could result in dismissal and a criminal prosecution.
- Adverts for goods on the Internet have to abide by legislation called the Trades Descriptions Act. Financial services such as loans, mortgages and insurance have to obey rules set out in the Financial Services Act.

What does a code of conduct contain?

Complying with licensing agreements

When you buy a piece of software, you are just buying a license to use it; you do not own it and are not free to do what you want with it.

When organisations purchase software to use over a network, they are purchasing a licence for a certain number of computers to use the software simultaneously. It is important that employees do not run more versions of the software than the software licence allows.

What does a code of conduct contain?

Authorisation

Access to the organisation's information resources, without the proper authorisation from the security manager, the unauthorised use of the organisation's facilities, and intentional corruption or misuse of information resources will usually be a violation of the code of conduct.

Data access permissions

Employees should not access data or files unless their permissions allow it. People should only access those files which are essential for the performance of their job.

What does a code of conduct contain?

Security policy

- non-disclosure of passwords
- non-disclosure of company data to any third party
- to ensure that printouts of company data are not left lying around
- to make sure that any unwanted documents are disposed of with care
- users and system administrators must guard against abuses that disrupt or threaten the viability of all systems.

What does a code of conduct contain?

Security

Some rules which can improve security:

- Rules about not revealing passwords to others and regular changing of passwords.
- Rules concerning the personal use of e-mail.
- Rules concerning the use of the Internet (e.g. employees may not access social networking sites/chat rooms/auction sites during working hours).
- Rules concerning data transfer. Many organisations will not allow the downloading of any material off the Internet onto the company's computers. Downloading of large files such as music files or videos uses bandwidth and make the Internet slower for others in the organisation.

Penalties for not following the Code of Conduct

For the code of conduct to be taken seriously, there must be penalties for misuse. Penalties will be applied according to the seriousness of the breach. Penalties for misuse involve:

- Informal warnings
- Written warnings
- Dismissal
- Prosecution

Alleged violations of the employee code of conduct will be investigated further and should there be any substance to the investigation, then further action will be taken.

Penalties for not following the Code of Conduct

Informal Warnings - Minor infringements of the policy could be unintentional. E.g. badly chosen passwords, excessive disk space consumption owing to bad file housekeeping. These unintentional breaches of the code of conduct are dealt with informally by the user's line manager

Written Warnings - More serious infringements are dealt with formally in case further action needs to be taken in the future. E.g.:

- sharing accounts or passwords,
- leaving documents laying around on your desk, etc.

Serious infringements are usually dealt with by issuing a formal written warning for the first instance, and possibly dismissal for the second.

Penalties for not following the Code of Conduct

Serious infringements include:

- unauthorised use of terminals
- attempts to steal data or passwords
- unauthorised use of or copying of software
- repeated minor infringements.

Dismissal

Very serious infringements may result in dismissal of an employee as a last resort or where employees have not taken notice of a number of written warnings. Actions of the employee which cause embarrassment to the organisation or could result in the company being prosecuted often lead to dismissal.

Penalties for not following the Code of Conduct

Prosecution

For very serious infringements there could be immediate dismissal, and a criminal prosecution could result. Whilst many organisations may shy away from the police being involved, from a publicity point of view, the seriousness of the offence may mean that there is no other choice.

Infringements of this kind would include theft of software or data, fraud, infringement of the Data Protection Act, downloading pornography, etc.

Legal/Moral Issues included on codes of Conduct

Legal issues are serious and against the law. If the issue is illegal then the police or other authority can bring about a prosecution which can lead to a fine or even imprisonment.

Moral issues, although most people would consider wrong, are not actually illegal.

Legal/Moral Issues included on codes of Conduct

Disinformation

Disinformation is false information intended to deceive or mislead. Disinformation can be a moral or a legal issue:

Moral – A salesperson advising a client to buy a certain make of computer with associated because the commission they will get is higher rather than it being the best computer to meet their needs.

Legal - A salesperson selling software claiming the software will do things it cannot do, which is against the Trades Descriptions Act.

Legal/Moral Issues included on codes of Conduct

Privacy - being able to keep information about your life private.

The law protects personal data being misused but things happen which are not illegal but against most people's morals.

Privacy as a moral issue: Companies buying lists of information off each other in order to cold call people to sell them goods or services.

- Companies monitoring their staff's use of e-mail or the Internet with a view to detecting misuse or just out of curiosity.

Privacy as a legal issue: Selling personal details of people without their permission, in contravention of the Data Protection Act.

- Not notifying the Information Commissioner that the organisation is processing personal data

Employment Patterns

Legal issues

- More likelihood of contracting illnesses such as RSI, back ache and stress. Organisations have a legal obligation to protect the employees against these risks by the use of the correct equipment (proper lighting, adjustable chairs, wrist rests, etc.) or correct working practices (changes in activity, regular breaks, etc.).
- Organisations will protect themselves from possible legal action by employees by training the employees to use ICT equipment safely and forcing them to adopt safe working practices by incorporating it into their code of conduct.

Employment Patterns

Moral Issues

- The use of computers to monitor performance, bosses looking at personal e-mails and time spent on the Internet mean that many employees feel threatened.
- Taking advantage of an employee's personal circumstances to offer them work at home using ICT for lower pay. E.g. mother with young children, carers, disabled, etc.
- Part-time work - with the use of ICT many more people work part-time. Part-time work offers employers more flexibility but the employees do not always have the same rights as full-time workers.

Employment Patterns

Equity (fairness)

E.g., rich countries can take advantage of the latest ICT developments, whereas poorer countries have to make do with older equipment/software.

Within countries, the population can be divided into **information poor** (lack of computer and Internet knowledge and access) and **information rich** (fast broadband access with good ICT knowledge). Information-rich people can take advantage of cheap loans, cheap holidays, etc., but information-poor people do not have access to this information.

Employment Patterns

Intellectual Property Rights

It is right that people who develop new software, hardware, communication methods, etc., should be rewarded for their work. It is not right that this work be copied by others.

Many organisations will state in their code of conduct that any work produced during working hours belongs to them.

Topic 7 - Managament of Change

What you need to know:

- Consequences of change
- *Candidates should be aware of the effects upon;*
  - *the skills required and not required*
  - *organisational structure*
  - *work patterns*
  - *internal procedures*
  - *the workforce (fears introduced by of change)*

Introduction

Organisations introduce new ICT systems to benefit themselves, not their employees, and many changes to a business can occur.

These changes could come in how the business operates, the jobs employees carry out, the skills the staff need, or changes to the management structure

Managements of Change

Changes in skills required -

ICT systems require different skills than manual systems, so staff may need to retrain.

The use of ICT has increased the number of skilled jobs available (network managers, programmers, computer engineers, etc.), but there has been a decrease in jobs such as typists, filing clerks, post clerks, etc.

Managements of Change

Changes to organisational structure

When a new system is introduced, some businesses take this as an opportunity to restructure, so it fits better with the new system.

This can lead to dissatisfaction among the employees, as working groups may be split up, or juniors being promoted over seniors, or can lead to some jobs being combined (e.g. A salesperson may now take orders, or deal with account queries, where previously these were two different job roles).

Managements of Change

Changes in work pattern

To meet the demand of a global 24/7 market, some businesses now operate around the clock.

This means more opportunities for shift work, part-time work and out-of-normal hours work.

This may inconvenience as many people as it might suit. Some may have family commitments, or it may not be compatible with a partner's work hours, etc.

Managements of Change

Changes to internal procedures

Since new ICT systems can be much more efficient than manual systems, staff may find themselves having to take on more, or different, responsibilities.

The new ICT system will be designed to be as efficient as possible, and not work around the existing system. As a result, Some employees may find that they perform the same job, but they now have to do it in a different way. Others still may find that their job frequently changes.

This amount of change can be very stressful to staff, particularly if they are not consulted about these changes.

Also, codes of conduct are required that outline what staff can and cannot do using the ICT system.

Managements of Change

Effects on the workforce

Fear of redundancy

Staff may fear redundancy as the new system is more efficient. Also, ICT systems can be expensive, so businesses will look to make savings by cutting staff.

Fear of reduced status/job satisfaction

Staff may worry that the restructuring due to the new ICT system may diminish their role in the business. Important tasks such as data management may now be performed by the system and available to all employees, so some middle-managers will lose some of their power.

Fear of ridicule

Staff may feel that their lack of skills will be embarrassing compared to more skilled employees (perhaps younger staff members).

Fear of relocation

Sometimes, business relocate to newer, smaller premises, or even to a completely new town/country, to reduce costs.

Overcoming resistance to new ICT systems

- Management should be full and frank about the reasons behind the new system's introduction, the effects of the new system, and its implications for all employees.
- Reassure staff that whilst redundancies may be needed, they will only occur when absolutely necessary.
- Staff should be involved in the introduction of the system, and can make suggestions about what they think the new system should do, or how. If they feel they have had an input to the new system, they may be more accepting of it.

Overcoming resistance to new ICT systems

- Comprehensive retraining programmes, either by training days, CBT or by having off-site training in a pleasant location, making the training more of a social event too.
- Listen to employees' criticisms of the new system, and act upon them if necessary.
- Encourage the employees that the new system will provide an opportunity to learn new skills, improving promotion prospects.

Topic 8 - Managament Information System

What you need to know:

- *Candidates should:*
  - *recognise Management Information Systems as organised collections of people procedures and resources designed to support the decisions of managers;*
  - Features of an effective Management Information System
    - *appreciate that Management Information Systems should:*
      - *include data that is relevant and accurate*
      - *give information when required*
      - *be accessible to wide range of users*
      - *present data in the most appropriate format*
      - *be flexible*
  - Understand the flow of information between external and internal components of an MIS
    - *be able to draw and interpret data flow diagrams.*
  - Features of good MIS
    - *accuracy of the data*
    - *flexibility of data analysis*
    - *providing data in an appropriate form*
    - *accessible to a wide range of users and support a wide range of skills and knowledge*
    - *improve interpersonal communications amongst management and employees*
    - *allow individual project planning*
    - *avoid information overload*
  - Factors which can lead to poor MIS
    - *complexity of the system*
    - *inadequate initial analysis*
    - *lack of management involvement in initial design*
    - *inappropriate hardware and software*
    - *lack of management knowledge about computer systems and their capabilities*
    - *poor communications between professionals*
    - *lack of professional standards*

Introduction

Management Information System – Systems that convert data from internal or external sources into information to be used by managers.

Management information systems:

- produce information beyond that normally needed for routine data processing
- produce information where the timing is critical
- are used to supply information to management in order to help make decisions
- are based around databases.

Most schools use SIMS (Schools Information Management System)

Features of a good/effective MIS

- Must include information that is ***relevant, accurate and fit for purpose***. Too much detail is almost as bad as too little. Validation and verification must take place to make sure that incorrect data is not processed.
- ***Must give the information when required***. Some information systems only produce certain output at a certain time. E.g. reports may be produced at the end of a monthly run for processing payments. Managers have to make decisions quickly and so should not have to wait for information. As MIS are used by the managers themselves, the information can be extracted whenever they need it.

Features of a good/effective MIS

- ***Be accessible to a wide range of users***. Managers in will need information relevant to their area of the business. The MIS must use all the data held by the corporate database and supply it to the full range of users. Managers must be trained in the MIS to use it effectively.
- ***Present the data in the most appropriate format***, or allow managers to choose how the information is presented. For example, in tables or the types of graphs used. They may choose to save the information in file formats that can be used for spreadsheets or presentations.
- ***Flexibility*** - A good MIS will therefore allow complete flexibility in the information it can produce and the way it is presented. The system should fit in with the managers and not the other way around

Internal/External Data in MIS

MIS use data that is both internal and external to the organisation.

Internal data was created within the organisation.

External data originated from outside of the business.

- Eg: To produce information about the effectiveness of a marketing campaign may include information about competitors as well as information about costs and sales from their internal ICT systems.
- Schools use MIS in various ways. For example, schools need to ensure they have the resources to cope with increases in the population. Internal information might include admission figures from previous years, details of brothers and sisters of existing pupils who will eventually start at the school, details of resources such as staff, rooms, desks, etc. External information sources could be figures from primary schools, census details (for indications of population), details of immigration, local authority data, etc.

Factors that can lead to a poor MIS

- ***Complexity of the system*** – systems must be able to deal with the detail managers require, but should not be too complex to use. MIS need to be simple to use so that all managers are capable of using them in their day-to-day work.
- ***Lack of formal methods when designing the MIS***– systems analysts may not following proper design methodologies and taking short cuts will result in a less than perfect system. Proper systems analysis takes time and effort but the resulting MIS is much better than MIS developed using less formal methods.
- ***Lack of management knowledge about ICT systems and their capabilities*** – Management should not rely upon the knowledge of the ICT development staff, and should try to keep up-to-date with new developments in ICT systems, to ensure that they use the best systems available to them.

Factors that can lead to a poor MIS

- ***Inadequate initial analysis*** - Inadequate analysis results in a system unable to perform a key task or that does not behave according to the original objectives. E.g. if the initial analysis is done by someone inexperienced, they might not fully analyse the information requirements of management.
- ***Inappropriate hardware and software*** - the hardware, (speed of the file server, speed of data transfer, etc.) all affect the speed at which management information can be extracted from all the data held. If the system is too slow then managers will only use the system when absolutely necessary. The MIS software should make it easy for managers to construct conditions for the extraction of the information they need and they should be able to choose how the information is presented.

Factors that can lead to a poor MIS

- **Lack of management involvement in the design** – If only ICT specialists take charge of the development of the information system, then the MIS may be less effective, as their business knowledge about the areas they are looking at is much weaker than the managers who are in charge of these areas. Managers should be part of the development team and consult with developers of the system.
- **Poor communications between professionals -** Poor communication between the business managers and MIS development staff may result in a system that does not meet the needs of the managers. Such systems may not extract the information needed, or may be cumbersome to use which puts off managers from using them.

Factors that can lead to a poor MIS

- **Lack of professional standards -** the British Computer Society (BCS) sets standards of practice to be observed by its members. Employing a member of the BCS ensures that the job should be performed in a professional manner. Not all computer professionals are members of the BCS, and don't conform to their standards. This could result in some professionals taking on jobs they are **not** experienced in in order to gain experience, but they may do a bad job of it. Alternatively, they may the try to persuade the organisation that they need a system that they **can** implement, which may not be what the organisation requires.

Topic 9 - Systems Development Life Cycle

What you need to know:

- System Investigation *Analysis of existing system and feasibility report*
  - *(a) Existing Hardware and Software*
  - *(b) Definition of the scope of the present system*
    - *Organisational chart*
    - *Define sources of data*
    - *Methods of data capture*
  - *(c) Major data processing functions and processes*
    - *High level (contextual view) data flow*
  - *(d) Identification of problems with the present system*
  - *(e) Identify user requirements for the new system*
  - *(f) Analysis of costs and benefits of the new system*
- System Analysis *Identify and understand tools and techniques used to analyse a system.*
- *Identify external and internal components to a system and the flow of data between them including Data Flow Diagrams (DFDs), including High level (contextual view) DFDs and low level (detailed view) DFDs, decision tables and systems diagrams.*
- *Candidates must be able to use all of the elements of a Data flow diagram correctly including:*
  - *flow direction line*
  - *process*
  - *entity*
  - *data store*
- *Data dictionaries.*
- *Entity Relationship diagrams.*
- *Candidates should understand that a 'Data Model' includes an*
  - ***Entity** Places, object or people represented by data in a spreadsheet or database*
  - ***Attribute** Information of facts about an entity*
- *Entity relationship modelling - candidates should be able to*
  - *draw and interpret ERM diagrams: one to one, one to many, many to many.*
- System Design *Design of hardware, software, data and file structures, information systems, network and data transmission issues, personnel issues and security processes and procedures.*

What you need to know:

- System Implementation *Acquisition and installation of hardware and software re-training.*
- *Appropriateness of different changeover strategies including 'direct' and 'parallel running'.*
- System Maintenance *Technical and User Documentation.*
- *Maintenance issues including identification of errors, security issues, changes in the business environment, dissatisfaction with hardware and software, updating the system*
- *Perfective, Adaptive, Corrective maintenance*
- System Evaluation *Criteria for evaluating a system.*
- *Understand the tools and their appropriateness for gathering information for the evaluation report including quantitative test, Error Logging Interviews, Questionnaires*
- *Methods of avoiding post implementation cost.*

SDLC

A system is a way of doing things

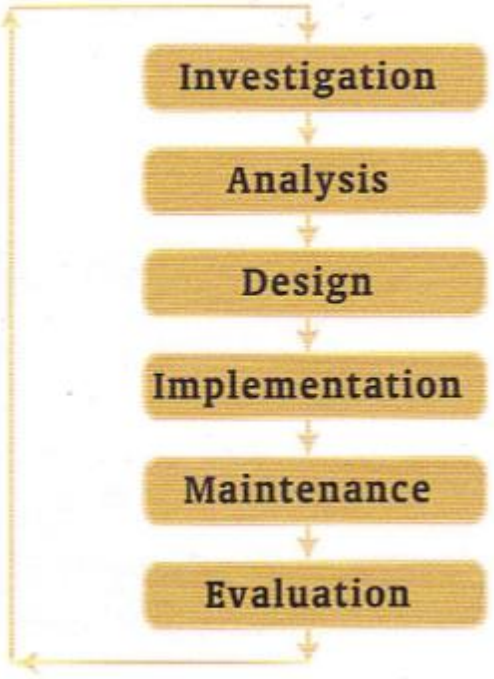
Organisations have various systems to deal with the different functional areas of the work they do. For example, there needs to be systems for paying staff, purchasing stock or raw materials, controlling how much stock is kept, keeping accounts, ensuring compliance with legislation, keeping records of staff employed and so on.

SDLC

The system development life cycle (SDLC)

The SDLC is a sequence of activities which are performed when a system is analysed, designed and implemented.

It is a cyclical process, as once the system has been successfully implemented, it is usual to periodically look at what improvements can be made to the system, and so the SDLC tasks are repeated.



SDLC

The tasks involved in system investigation

Before analysing the system, it is necessary to find out about the organisation and the tasks they want the new system to do. You need to investigate how the existing system works and what the requirements are for the new system. The existing system can be investigated by using:

- Interviews
- observation
- inspection of records
- questionnaires

SDLC

Interviews - interviews with managers should reveal how their particular department works and any problems they are having with the existing system. They can offer information about how they would like the new system to work and what information they would like the new system to provide.

Interviews should also be carried out with operational staff. These are the members of staff who perform the majority of the day-to-day work of the organisation and their knowledge of the organisation is usually restricted to their own area of work. As a result, they will be able to supply the fine detail about particular ways that jobs are done.

Collection of information using interviewing is time consuming.

SDLC

Observations - Observation involves sitting with a person and observing what they do in order to understand the information flows and processes they perform. This can be time-consuming and can cause reactivity (influencing how they perform because they are being observed).

Inspection of records - organisations still use and generate paper-based documents. By examining these documents you can understand what information is held and how it is communicated between different departments or between the organisation and suppliers and customers.

SDLC

Documents giving general information would include:

- organisation charts showing the showing the hierarchy in the organisation and who reports to whom
- staff CVs - to assess the skills or training needs of employees
- job descriptions - details of the responsibilities of employees
- policy/procedure manuals - to understand the way the organisation works
- previous systems documentation - paper documents when previous systems have been produced.

Documents giving specific information would include:

- product catalogues
- order forms
- Invoices and despatch notes
- picking lists (for warehouse staff).

SDLC

Questionnaires - questionnaires can be an ideal way of collecting information about a company. You do not have to spend time interviewing people and a questionnaire sticks to the important points without digressing, which can occur in an interview.

However, questionnaires have drawbacks.

Many people forget to fill them in, which can result in an incomplete picture of a system.

Respondents may misunderstand some of the questions, if the forms are simply posted to them and no personal help offered.

Some may be dis-honest or afraid to be honest in their responses.

SDLC

When compiling questionnaires, bear the following in mind:

- Ensure the questions are precisely worded so that the users do not have to interpret the questions.
- Make them anonymous, as answers may not be honest otherwise.
- Structure the questionnaire so that general questions are asked first, followed by more specific ones. It is also worth dividing the questionnaire into functional areas, so for example, one part could deal with sales order processing, another with stock control. Obviously this approach will vary depending on the type of organisation.
- Avoid leading questions (questions suggesting an answer).
- At the end, always add the question: 'Is there anything I have missed that you think I ought to know about?'.

SDLC

Feasibility and the feasibility report

Feasibility is an initial investigation to look at the likelihood of being able to create a new system with stated aims and objectives at reasonable cost. The results of this exercise are summarised in a document called a **feasibility report** and this document is used by senior managers/directors to assess the project's feasibility, and whether the project should go ahead or be abandoned.

Feasibility is an important activity because it makes sure that new systems are not developed that have little chance of success. There are many examples of new systems being abandoned after a significant amount of work has been done on them.

SDLC

Feasibility will normally involve the following:

- An initial fact find which will give information on what is required from the project.
- An investigation into the technical, legal, economic, operational and schedule implications.
- Identifying the costs and benefits of the new system and weighing them against each other.
- Making recommendations as to the feasibility of the project.
- A draft plan for the implementation of the project.

SDLC

What should be included in the feasibility report?

After the initial analysis of the existing system, a report, called a feasibility report, is produced on which a decision to go ahead with the project or whether to abandon it is made.

A feasibility report will normally contain some or all of the following:

- **User requirements -** the user requirements of the system should be identified, agreed with the analyst and written as a list. Any developed system will be judged on how closely it matches these requirements.

SDLC

- **Details of existing hardware and software -** it may be the case that existing hardware and software can be re-used or new or additional hardware or software is needed.
- **Definition of the scope of the present system -** The scope will determine the size and complexity of the proposed project. Included in the scope are details of organisation charts, sources of data and methods of data capture. This is so that everyone is clear what the system does and also what it doesn't do.

SDLC

- **Major data processing functions and processes -** this is illustrated as a *context diagram* which represents the whole system as a rectangle and shows how the information flows to and from the systems to the external organisations and systems. This diagram, and the topic of Data Flow Diagrams, will be covered later.
- **Identification of problems with the present system -** here you would list the problems with the existing system with a view to building a new system capable of solving them.

SDLC

- **Analysis of costs and benefits of the new system -** costs will be incurred such as staff, equipment, hardware, software, licences, communication systems, training, etc. These will have to be weighed up against the benefits of the new system such as fewer errors, more management information, ability to complete transactions in less time, increase in business owing to greater satisfaction among customers.

SDLC

Once the feasibility study is complete, further understanding of the system being developed is needed.

The process of finding out and documenting the existing system is called **systems analysis** and this is performed by a systems analyst. There is a variety of tools and techniques that produce diagrams and charts which are used to document a new or existing system.

SDLC

Analysis of the existing system

The systems analyst (or just analyst, for short) investigates the requirements for the new system.

Analysis will normally involve the following:

- understanding the existing system
- understanding the proposed system if there is no existing system
- gathering and analysing different user requirements
- setting out the solution in a logical way using tools and techniques such as data flow diagrams, data models, process specifications and systems diagrams
- producing a specification.

SDLC

Data flow diagrams (DFDs)

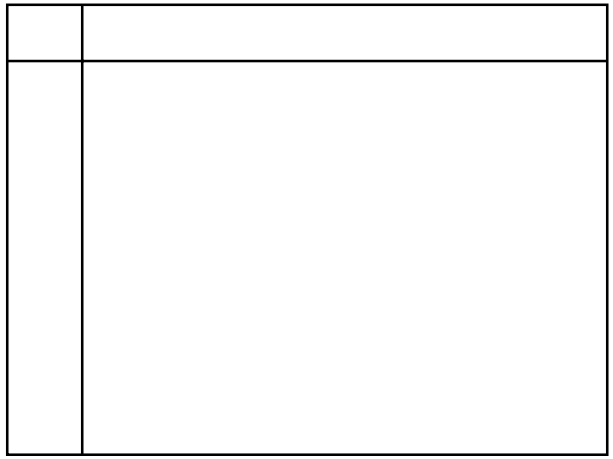
- It is important, when explaining an existing system, to look at the data/information flows (where information comes from, and where it goes to) within an organisation. This is best done diagrammatically using DFDs.
- These look at inputs, what processes are performed on the inputs and the outputs produced.

SDLC

Symbols used in DFDs

Process - a rectangular box is used to represent a process (***something being done with the data: manipulate it in some way or perform calculations on it, for example***).

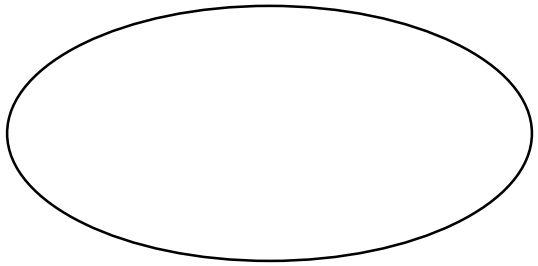
The box is divided into three parts, the top left box having a number in it which uniquely identifies the process. The main body of the box is used to record a brief description of the process and the top right of the box is used to record the person or area responsible for the process.



SDLC

External Entity - a source of data (where it comes from) or a sink of data (where it goes to)

This is an oval box which is used to describe where, outside the system, the data comes from and goes to. We are not concerned with what happens to the data before it reaches the box (if it is a source) or what happens to it when it goes past a sink.



SDLC

Data flow

- ***A data flow shows that data is being passed from one item to another on a DFD***
- A data flow is shown by an arrow pointing in the direction of the flow. Usually it is advisable to put a description of the data flow on the arrow to describe the data that is being passed
- By convention, we never use a verb on a data flow.

customer number

SDLC

Data store

A data store is anywhere data is stored; it could be a drawer where you keep letters, files, folders, books, a filing cabinet (or a certain drawer of a filing cabinet), magnetic disk, CD, etc. The main body of the data store symbol is used to label what information is being store, and it is prefixed by either an **M** for a manual store and **C** for a computer store.

C-Stock

SDLC

Levels of DFDs

When analysing systems it is usual to draw DFDs at different levels. The level used reflects the depth in which the DFD looks at the system being investigated.

- **Context diagram (or Level 0) -** a diagram which represents the ***overall system*** as a single DFD process
- **Level 1/2/3 Data flow diagram** (DFD) **-** shows the flow, storage and processing of data in a system in more specific detail than the context diagram

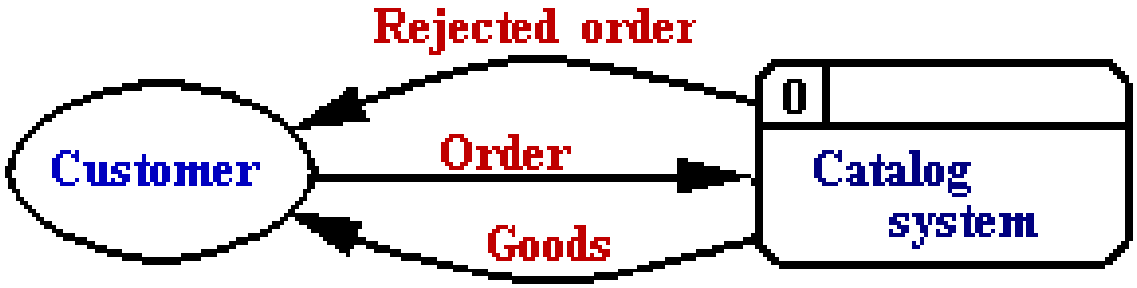
SDLC

The context diagram puts the system being investigated into context. It is a high-level DFD showing the entire system under investigation as a single box and the information flows between external entities such as suppliers and customers. The diagram might show the flow of orders from the customers (an external entity) to the sales department and goods being despatched from the warehouse to the customers.

- The aim of the context diagram is to show the scope of the system.

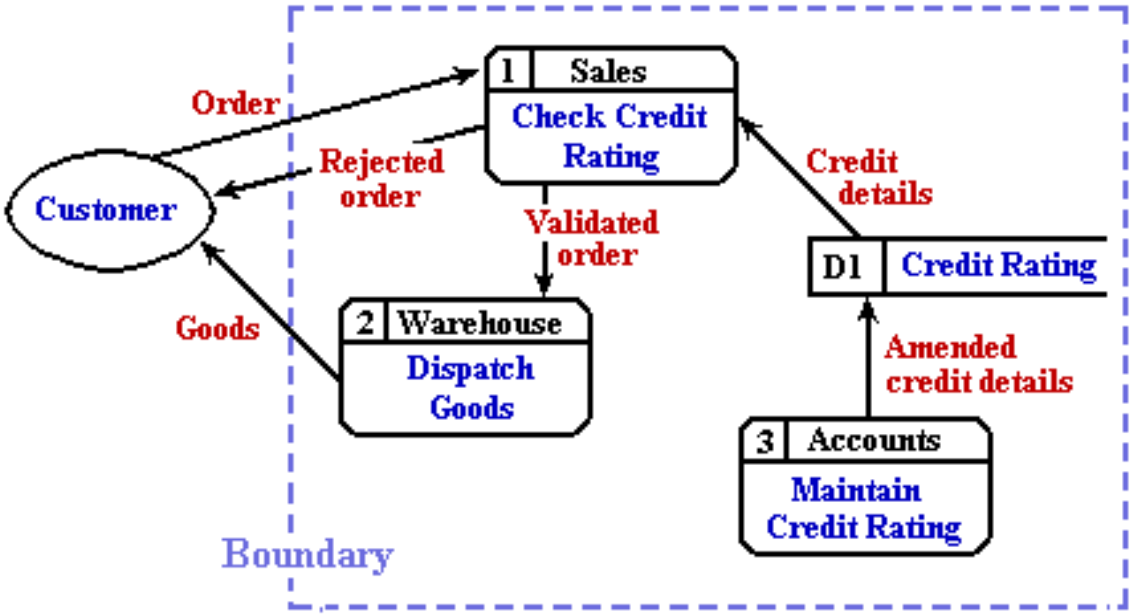
SDLC

The context diagram above, and the decomposition which follows, are a first attempt at describing part of a 'Home Catalogue' sales system. In the modeling process it is likely that diagrams will be reworked and amended many times - until all parties are satisfied with the resulting model.



SDLC

A level 1 DFD showing how the context diagram has been expanded.



SDLC

Entity relationship diagrams look at the components important to the system and the relationships between them. Usually, the e-r diagram informs how a relational database will be created and linked.

What is a relational database?

An entity can be anything about which data is recorded. It could include people, places, objects, customers, sales, payments or employees. Each entity has some associated **attributes** (further details about an entity).

SDLC

In the following table the attribute for the entity 'customer' contains further details

Entity	Attribute
Customer	Customer Number*
	Address
	Credit Limit*
	Amount Owing*

* Any attributes that cannot be broken down further are known as ***atomic***. Breaking down attributes to produce atomic attributes allows the flexibility to manipulate the data. For example, we could search for customers who have a certain postcode.

SDLC

Each entity is represented in an entity diagram by a rectangle with the name of the entity written inside. The relationship between the entities is shown as lines between these boxes.

The entity is always written inside the rectangle in capital letters and must always be *singular*.

Student

SDLC

Relationships

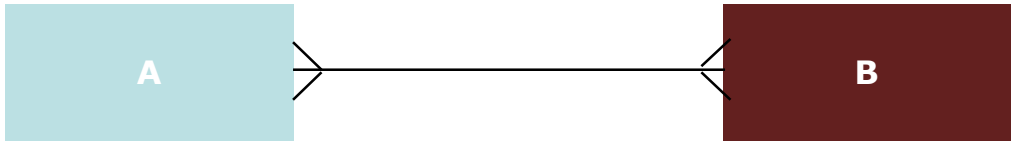
A relationship is the way in which entities in a system are related to one another. Relationships are shown using lines, 'crow's feet' withdescriptive text above them.

A relationship may be **one-to-one** (1:1), **one-to-many** (1:m), or **many-to-many** (m:n).

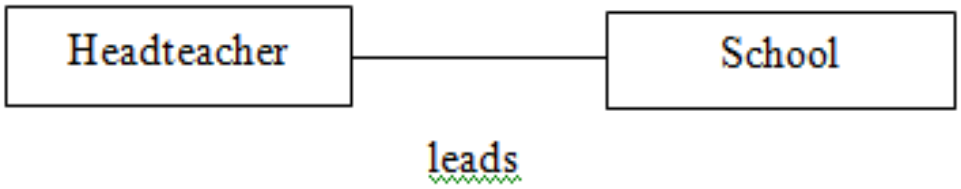
1:1

1:M

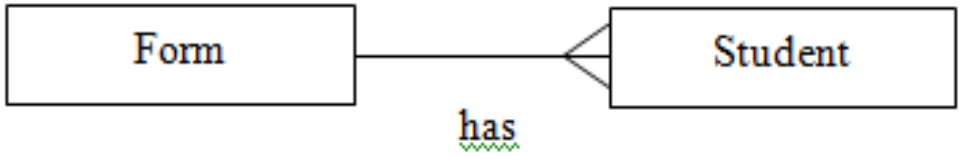
M:N



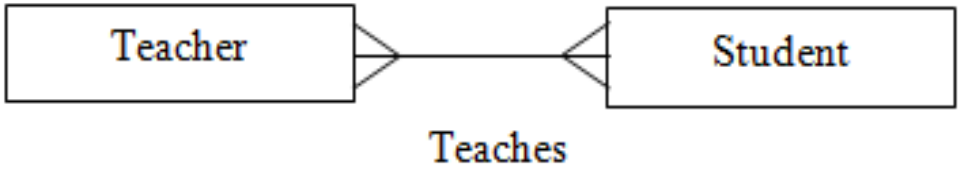
Examples:



A Headteacher is in charge of only one school and every school only has one headteacher.



Every form has many students, but every student only belongs to one form



Every teacher has many students, and every student has many teachers

The entities would be each represented by one table in your database.

Note:

M:N Relationships are not acceptable in E-R Modelling, as this would result in databases having duplication. Relationships of this type must be decomposed

SDLC

Example – CD Store

Four entities are used here:

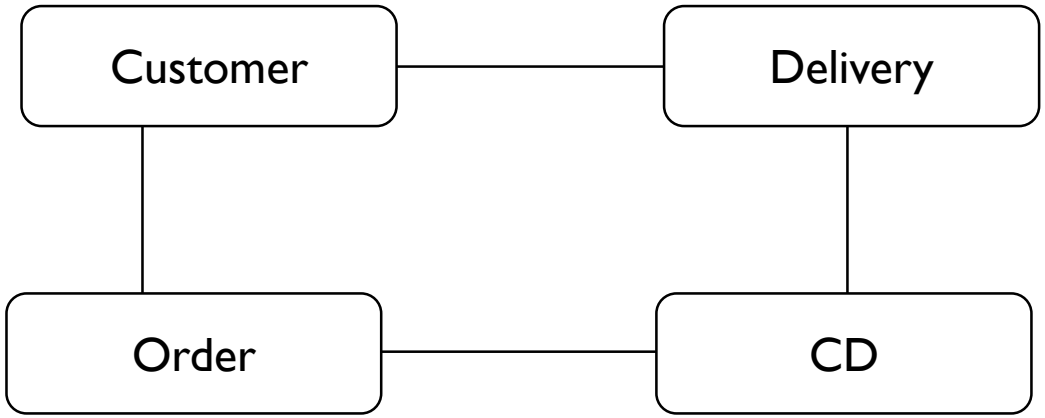
- CUSTOMER
- CD
- ORDER
- DELIVERY

We must now consider how these entities are related.

It is a good idea to write these as a list like this:

- a customer places an order
- an order consists of one or more CDs
- delivery consists of the CDs in the order
- delivery is made to the customer.

So far, our E-R diagram looks like this –

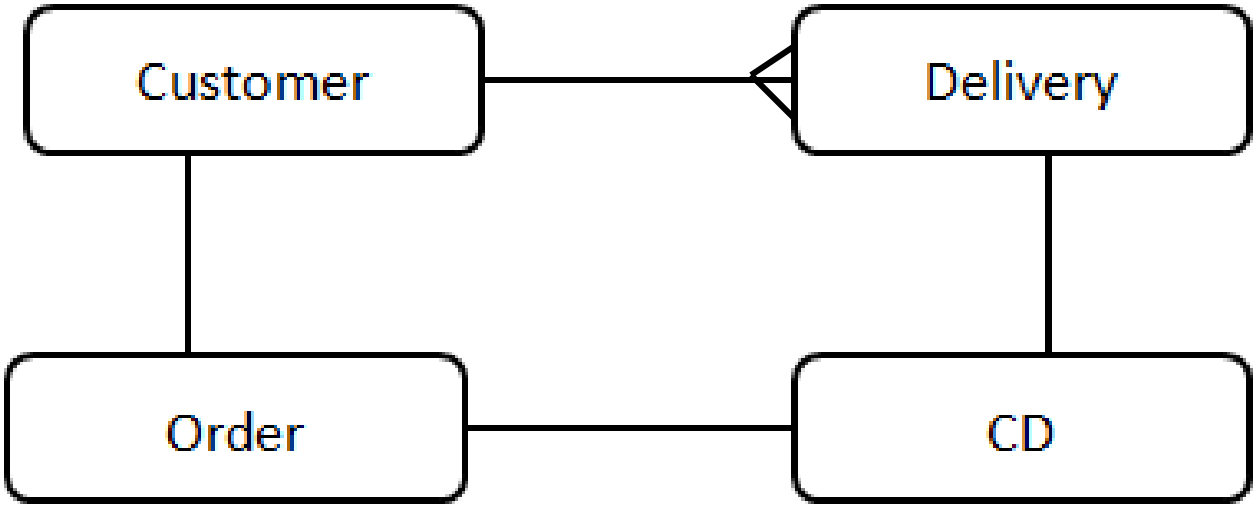


But since there are only 1:1 relationships, clearly something is wrong.

SDLC

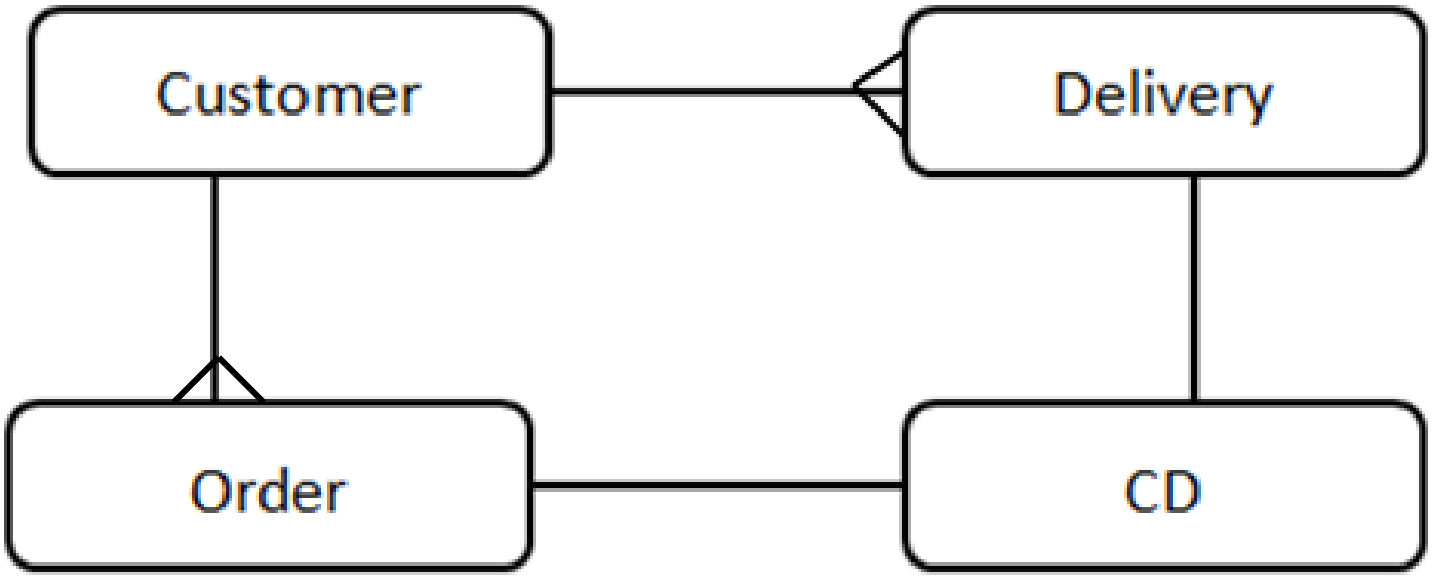
Our first relationship can be between **customer** and **delivery**.

A **customer** may have *many* **deliveries**, but each **delivery** only goes to *one* **customer**:



SDLC

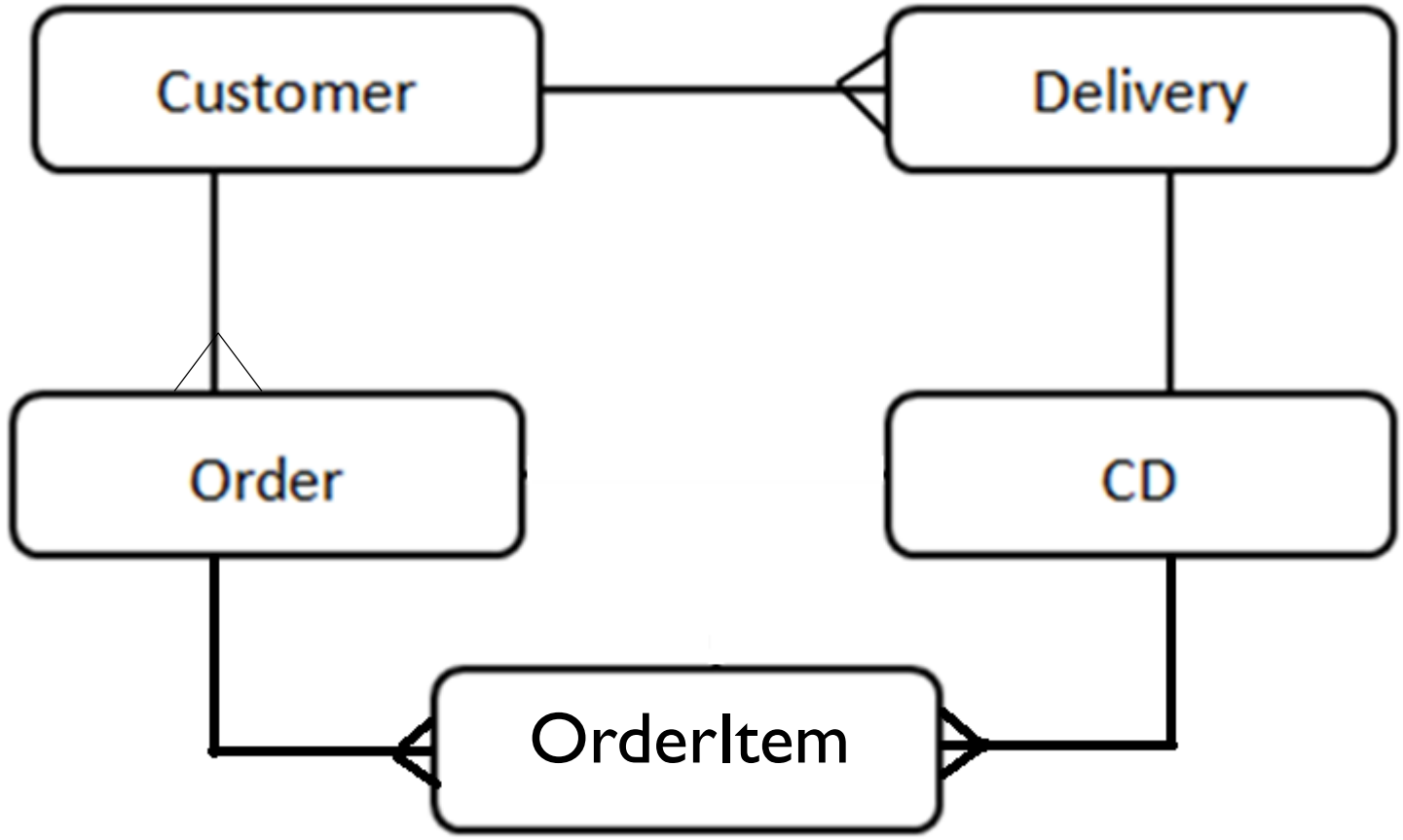
Next, a **customer** may have *many* **orders**, but each **order** belongs to only *one* **customer**:



SDLC

- Finally, the relationship between **order** and **CD** causes a problem.
- Since an order can have many CDs, and a CD can be on many orders, it would be impossible to track which CD belongs to which order and so on in a database. To overcome this, we must ***decompose*** the relationship, by inserting a sensibly named entity in-between the entities, and having a 1:M and M:1 relationship.

- Eg:



The

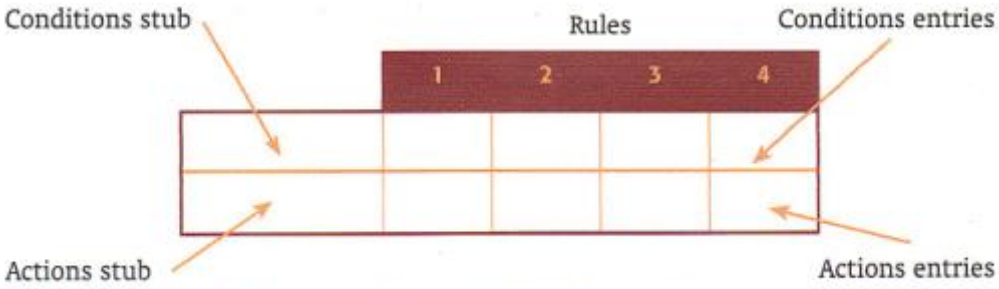
‹s to

as

SDLC

Decision Tables

A decision table
certain cond



The standard way of laying out a decision table is shown here

be taken under

Conditions stub – the rules that are being tested

Actions stub – the actions that are taken as a result of combinations of conditions being met

Conditions entries – shows whether or not conditions apply

Action entries – show actions that must be taken depending upon the conditions

SDLC

Traffic Lights

The first step is to write the conditions that could occur:

Red light

Amber light

Green Light

These are written in a separate row in the conditions stub.

Next, we have to decide what are the different outcomes that could occur from the lights being on or not:

Stop

Go

Call police (as lights aren't working)

These are written in a separate row in the action stub

SDLC

Conditions stub

Actions stub

RED
AMBER
GREEN
STOP
GO
CALL POLICE

SDLC

Next, we must consider all sensible possible combinations of each condition, and note them in the conditions entries section of the decision table:

	Rules							
	1	2	3	4	5	6	7	8
RED	Y	Y	Y	N	N	N	Y	N
AMBER	Y	Y	N	Y	N	Y	N	N
GREEN	Y	N	Y	Y	Y	N	N	N

SDLC

And lastly, in the actions entries section of the decision table we mark the action that must be taken with an **X**.

	Rules							
	1	2	3	4	5	6	7	8
RED	Y	Y	Y	N	N	N	Y	N
AMBER	Y	Y	N	Y	N	Y	N	N
GREEN	Y	N	Y	Y	Y	N	N	N
STOP	X	X	X	X		X	X	X
GO					X			
CALL POLICE	X		X	X				X

SDLC

- **Advantages of decision tables**

- Ensures you consider all combinations of conditions and their actions
- Easy to understand
- Standard layout
- Helpful for programmers

Creating a carriage costs decision table

In some situations, there is no point in writing down and considering all the rules, since some of them may be impossible. Take the following example:

Suppose the carriage to be paid when ordering a CD from a club is as follows:

1–3 CDs carriage is £2.50
4–6 CDs carriage is £3.00
7+ CDs carriage is £4.00

Since there are 3 general conditions there are 8 rules. If we look at some of these rules we find that some of them are impossible. For instance YYY would be impossible since the number of CDs ordered can only have one Y. We get impossible rules when the questions in the decision table are related to each other.

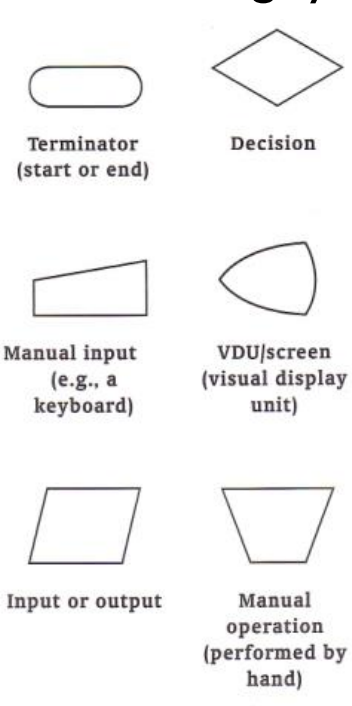
To take account of these impossible rules, we leave them out of the decision table.

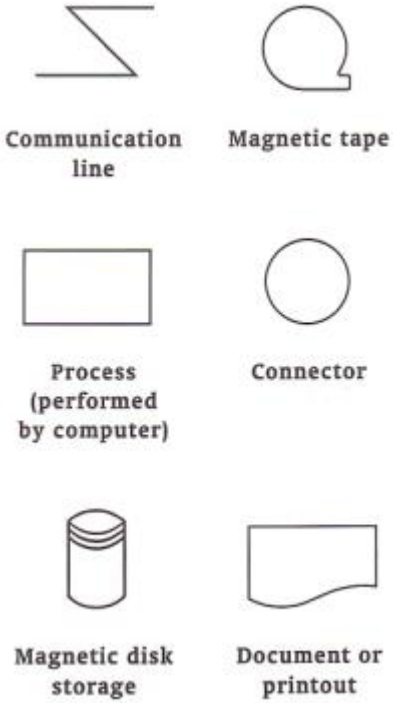
SDLC

System Diagrams

Systems diagrams show a diagrammatic way of how an ICT works, what its inputs and outputs are, what is done to data and so on.

It uses the following symbols:





SDLC

System design

System design will usually involve the following:

- Specifying **hardware** and **software**.
- Design of **data**, **file structures**, **fields** and **table** structures for the relational database.
- Design of **input and output methods** for information. E.g. forms used to input data and reports and queries used to output information. Specialist documents such as invoices, pay slips, delivery notes, etc., would also be designed here.
- The **design of information systems** that will allow users to extract information on which decisions can be made.

SDLC

- **The design of networks and transmission issues** such as topology, data transmission media, protocols, etc.
- **Personnel issues -** completely new systems often mean that staff need training and departments need reorganising.
- **Security processes and procedures**. If personal data is being stored, its use needs to be registered with the Information Commissioner so there need to be procedures in place for this to happen. Consideration needs to be given to the security of the data stored and plans need to be made using levels of access, user-IDs and passwords to ensure the security of all data held.

SDLC

System implementation

This is where the system is built according to the design produced in the previous stage. This involves:

- Purchase and installation of hardware
- modifying existing software
- programmers producing any programming code need for the working solution
- installing software on hardware
- Creating the databases
- Training users.

SDLC

Testing

Each person responsible for their own part of the system must test it to ensure it works.

Testing will normally involve the following:

- testing at very detailed levels (i.e., individuals will thoroughly test their part)
- testing at a higher level (i.e., when the various parts of the system are joined together)
- testing at a systems level where all the parts are tested as a whole system
- testing each field using **correct (valid)**, **erroneous (invalid)** and **extreme** (big, small) data

SDLC

Changeover Methods

In order to change from one system to another it is necessary to have a changeover strategy:

- **Direct changeover** – you stop using the old system on a set date, and start using the new system from then on
- The disadvantage of this the risk of hardware and software problems. If the system fails then it can be disastrous to the business. The advantage of this method is that it requires fewer resources (people, money, equipment) and is simple, provided nothing goes wrong.

SDLC

- **Parallel changeover -** this method is used to minimise the risk in introducing a new ICT system.
- The old ICT system is run alongside the new ICT system for a period of time until all the people involved with the new system are happy it is working correctly. The old system is then abandoned and all the work is done entirely on the new system. The disadvantages of this method are that it involves a lot of unnecessary work (as the work is being done twice) and is therefore expensive in people's time. It also adds to the amount of planning needed for the implementation.

SDLC

- **Phased conversion -** a module or part of the new system is introduced in phases until the whole system is transferred. The advantage of this is that IT staff can deal with problems caused by a module before moving on to new modules. The disadvantage is that it is only suitable for systems consisting of separate modules.
- **Pilot conversion -** this method is ideal for large organisations that have lots of locations or branches where the new system can be used by one branch and then transferred to other branches over time. The advantage of this method is that the implementation is on a much smaller and manageable scale. The disadvantage is that is takes longer to implement the system in all the branches.

SDLC

Choosing a changeover method

Choosing a changeover method is based on a number of factors such as:

- Is there an existing system? If not, then parallel changeover could not be used.
- Is the system cutting edge (new technology, newly written software etc.)? Parallel changeover will reduce the risk or pilot conversion will reduce the problems that could occur.
- Is the system to be implemented in lots of different locations? If so, pilot implementation would be ideal. You could get the system working in one branch and then transfer the implementation to other branches.

SDLC

Implemented systems must be maintained, but the people involved in the original project may leave the organisation, so new staff will need to understand the new system.

They will need documentation to do this, so the first stage of the system maintenance process is the production of both **user** and **technical** documentation.

SDLC

User documentation (or user guide) - documentation that the user can refer to learn the new system or for help with a problem.

The guide should cover:

- minimum hardware and software requirements
- how to perform all main functions of the software
- frequently asked questions (FAQ)
- Dealing with error messages and troubleshooting
- how to back up data.
- examples and exercises to help the user understand the system. Since users are usually non-technical, any specialist, technical language should be avoided.
- details of what to do in exceptional circumstances. E.g. if the system fails to read a disk.

Users have the best view of a system and so should be asked to evaluate any proposed user guide. Their comments should be incorporated into the guide.

SDLC

Technical documentation – documentation to help systems analysts and programmers understand the technical workings of the system.

The following should be included:

- a copy of the system design specification
- all the system diagrams (flowcharts, system flowcharts, DFDs, E-R diagrams, etc.)
- the data dictionary
- macro designs, spreadsheet formulae or program listings
- screen layout designs
- user interface designs
- test plan

SDLC

Maintenance could be needed because of:

- Adding extra functions to the existing system that are identified at the review meetings
- maintenance teams altering existing programs or creating additional ones
- Correcting any operational issues such as poor performance or software bugs will be identified at the review meeting
- Investigating system crashes to find out the reasons for their occurrence
- managing interfaces with other systems, such as Internet, email and intranets.

SDLC

The three types of system maintenance are **perfective, adaptive and corrective**

Perfective – to improve the performance of the ICT system. Usually this will involve adding features not originally present to the software to make it produce the information from a database faster or to improve the speed of a network.

Adaptive - the way of doing things changes in an organisation. E.g., there may be new laws which mean that the system needs changing.

Corrective - correcting faults or bugs that did not arise during testing. Software manufacturers often produce updates to deal with these issues and these have to be installed.

SDLC

There are several maintenance issues to keep a developed ICT system working properly:

- **Identification of errors -** no matter how thoroughly a system is tested errors can still arise and must be dealt with.
- **Security issues -** certain programs (particularly operating systems) can present security weaknesses which were not envisaged when the software was originally created. Security issues are addressed by writing software code to alter the original software to close the security loophole.

SDLC

- **Changes in the business environment** – business' needs change over time and the system must be altered to cope with these changes. Examples include changes to legislation, changes to taxation, etc.
- **Dissatisfaction with hardware and software -** users may become dissatisfied with the hardware and software, which may not function at an acceptable speed or give the information needed to keep the business up with the competition.
- **Updating the system -** software often needs updating to cope with changes to operating systems or by adding extra functionality.

SDLC

System Evaluation

Evaluation normally takes place a few weeks after the implementation as only then will the users have found any problems or shortcomings.

Evaluation and review normally involves:

- checking that the original user requirements have been fully met by the new system
- assessment of how happy the clients are with the development of the new system
- setting up a review cycle so that the system is checked periodically to make sure that it is still meeting requirements.

SDLC

Evaluation Criteria

Before evaluating a new system it is useful to list some evaluation criteria such as:

- how closely does the solution match the user requirements?
- how easy is the new system to use?
- how satisfied are users with the information the system gives?
- how reliable is the system?
- how secure are data and programs?

SDLC

Information gathering tools for the evaluation report

- **Quantitative data**- it is always easier to evaluate satisfaction if it can be expressed numerically. E.g. Users could rate their satisfaction on a scale of 1 to 5. This can then be analysed statistically
- **Error logging interviews -** help-desk calls are logged and are an important source of information on such things as:
  - how well the training given to the users met their needs
  - how often the software crashed.
- **Questionnaires** - users can be given questionnaires to collect information about their satisfaction or otherwise with the new system. It is a good idea to allow users to suggest limitations of the new system, and improvements that could be made.

SDLC

Methods of avoiding post-implementation cost

Once a system is built and is being used, the financial costs can still be ongoing. Some of these costs include:

- **Training costs -** the initial training may not have covered all of the software, or new software modifications may be needed and this can lead to additional training.
- **Modification costs -** the software may not perform all of the tasks the user required, so additional modification to the system is needed. With better identification of user requirements these post-implementation costs can be reduced.

SDLC

- **Help-desk and other support costs** – this can be reduced with good quality initial training
- **Need to purchase additional hardware -** organisations often expand so systems need to be made larger by the addition of more storage, faster processors, etc. Building a system with plenty of additional capacity can reduce this cost.
- **Correction of bugs -** with comprehensive testing these should not occur or should at least be reduced.