



# ICT4

# Revision

This booklet is intended to support your existing revision in your final approach to the first A2 ICT exam. Continue using the past papers, revision materials and revision exercises that you are already using!

[www.A2ICT.co.uk](http://www.A2ICT.co.uk)

## Structure of organisations

Hierarchical = rigid, slow decision making

Flat = flexible, autonomous

Three levels of hierarchy:

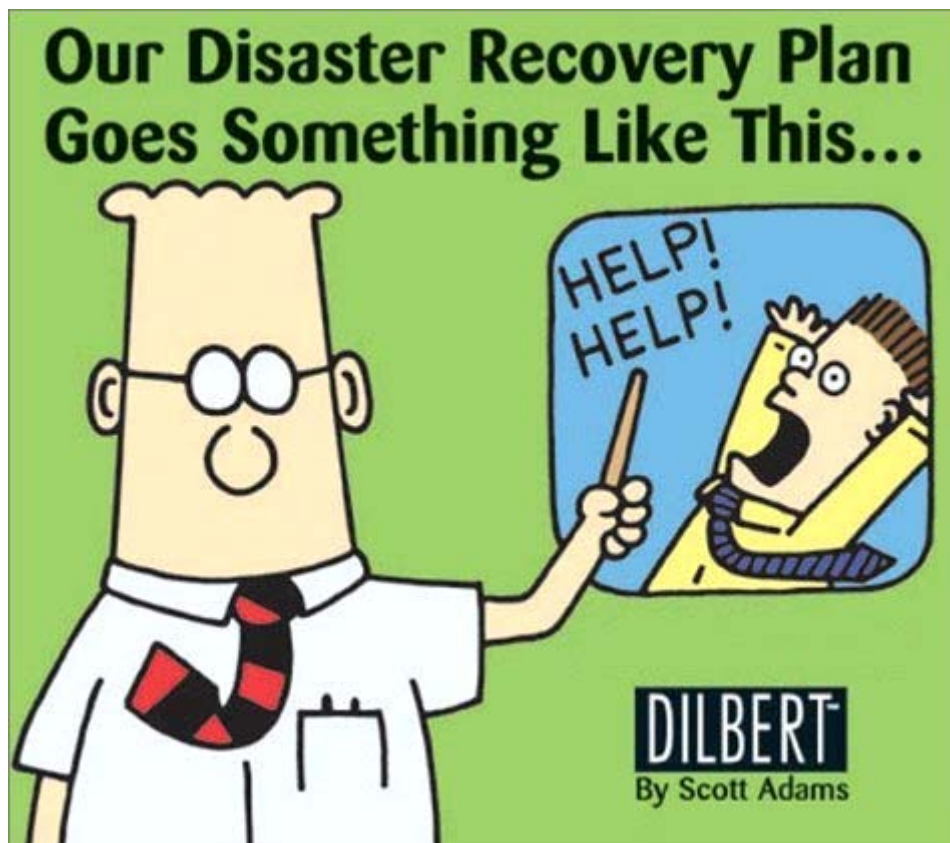
Strategic

Tactical

Operational

New technologies have affected the structure of many businesses, leading to flatter structures and more dynamic companies.

ICT means information can be made available at all levels of a company's structure.



**A Data Processing System** = system that carries out day to day operational activities of an organisation

**Information System** = provides information for the use that can be used in decision making

**Management Information System (MIS)** = a system that provides information for managers. It converts data from internal and external sources into information. Communicated to managers at different levels to allow them to make effective decisions

i.e. MIS tool to enable managers to do their job effectively

Decision can be made at different levels:

- Strategic
- Tactical
- Operational



**Success / Failure of an MIS:**

- Analysis
- Management involvement
- Computer system
- Concentration on low-level data
- Management knowledge of ICT systems
- Management demands
- Team work
- Professional standards

The above points can be either positive or negative. For example, a reason for success could be there is sufficient analysis whereas a reason for failure could be that there is insufficient analysis. Pick any of the above and try the same. You will normally be asked to explain 3 reasons for a success or failure.

**System life cycle** = series of stages involved in replacing an existing system with a new one.

**Preliminary study** - initial look at current system

**Feasibility study** - look at the **TELOS** of required new system (Technical, Economical, Legal, Operational and Schedule feasibility)

**Systems Analysis** - how current system works and what is required - interviews, questionnaires, observations, detailed study

**Deliverables** - agreements about the project such as timetables, agreed functions, documentation, UI design and testing

**Design** - elements of the new system - inputs, outputs, data storage, HCI, test plan

**Implementation & testing** - thorough testing using realistic data.

**Monitoring** - system's performance is closely monitored

**Evaluation and Review** - new system is evaluated for effectiveness.



Think about the type of questions you might get  
e.g. "Explain why a feasibility study might  
recommend the replacement of an existing  
system" or "Explain why deliverables are  
important in a system life cycle"

Corporate Information Systems Strategy is affected by:

- Organisation structure
- Decision making methods
- Legal requirements
- Information flow (see below)
- Hardware and Software
- Behavioural factors

**Formal information flow** = fully documented system with agreed procedures stating every aspect. Clear procedures for communication.

**Informal information flow** = information that naturally arises from phone calls, conversations.

**Information flow** affected by:

- Structure of organisation
- Size of organisation
- Geography structure of organisation
- How data originates from organisation
- Form of information
- Volume of data



Look through the past-papers to see how questions on Corporate Information Systems strategy continually come up. Normally they ask what factors can affect it

**Information** - required to make good decisions

**Formal information** = created by organisation's procedures e.g. filling in application form

**Informal information** = info that rises naturally e.g. through conversations.

Many ways to **classify** information:

**Source** (internal, external, primary, secondary)

**Nature** (quantitative, qualitative, formal, informal)

**Level** (strategic, tactical, operational)

**Time** (historical, present, future)

**Frequency** (continuous, hourly, daily, monthly)

**Use** (planning, control, decision making)

**Form** (written, aural, visual)

**Type** (detailed, sampled, aggregated)

'Good' information is:

**Relevant**

**Accurate**

**Complete**

**Reliable**

**In Time**

**Appropriate level of detail**

**Shared / delivered through appropriate communication**

**Understandable**



As you look at past-paper questions, here again the types of questions are very similar—they ask you how information is classified or what is 'good' information. Try to come up with examples for all your answers though!

## Data

May require translation or transcription prior to entry into a system  
- potential accuracy problems?

Method of data capture depends on:

Nature of data and where it comes from

Current state of technological development

Quantity of the data to be collected

Verification = check to see if data has been entered correctly.

Validation = computerised checking to identify data that is not reasonable or incomplete.

Control mechanisms to ensure no transactions are lost or missed -  
e.g. batch totals, control totals, hash totals (all checks using validation)

Audit mechanisms = used to keep track of data movement (and also used by auditors)



Here you may be asked to explain about data, data capture or data checking—verification or validation. Try to identify the key example questions

**Management of change** = introduction of a new information system will always involve management of change:

**Factors to consider:**

- Reskilling employees
- Attitudes of employees
- Organisational structure
- Employment patterns and conditions
- Internal procedures

**To prepare for change,** businesses need to:

- Plan ahead
- Consult
- Explain
- Train

**Employees may be concerned about:**

- Redundancy
- New Work Patterns
- Relocation
- Deskilling



You can see the three areas you might be asked questions about in relation to management of change - issues to consider, how to prepare or how employees might react.

**Corporate ICT security policy** = to prevent misuse, to enable misuse to be detected and investigated, lay down procedures and expectations and establish disciplinary procedures.

**Audit trail** = automatic record made of any transactions carried out on a computer system e.g. updates of files. Allows an auditor to check to see if the company accounts are accurate.

Organisation must make sure that employees are aware of **legislation** in relation to ICT:

Data Protection Acts 1984 and 1998  
Computer Misuse Act 1990  
Copyright, Designs and Patents Act 1988  
Health and Safety at work Act 1974  
EU Health and Safety Directive 87/391

**Enforcing and controlling data protection:**

Appoint Data Protection Officer  
Establish security methods e.g. firewalls  
Ensure code of practice prevents employees building up personal data  
Use a range of methods to train all staff  
Ensure staff are aware of disciplinary measures



### Enforcing and controlling software misuse:

- Ban employees from installing unauthorised, unlicensed software
- Ban employees from copying software for home use.
- Separate duties between more than one employee
- Centrally control purchase and maintenance of all software licences
- Carry out regular audits and checks
- Discipline employees who break the rules

### Enforcing and controlling health and safety legislation:

- Appoint a safety officer
- Regularly inspect workstations:
  - Health & safety criteria
  - Ergonomic criteria
- Carry out regular staff training
- Ensure software correctly used
- Establish procedures to fix issues
- Produce memos & leaflets for info
- Establish disciplinary procedures



Over this and the previous page you can see lots of potential questions that could be asked - something along the lines of one of these three appears each year in the exam.

### Recognise threats to information systems:

- Telecommunication
- Computer crime and abuse
- Invalid data
- System design failure
- Physical failure
- Hardware failure
- Software failure



**NASA's  
CONTINGENCY  
PLAN**

### Ways to avoid disaster:

- Virus scanning software
- Fault tolerance components
- Smoke detectors
- UPS
- Strict password policy (e.g. change each week)
- Regular maintenance

### A contingency plan includes:

- Backup strategies
- Contract with disaster recovery company
- Arrangement to share hardware with another company
- Distributed systems on different sites.

*Here you need to consider questions about threats and disaster recovery / contingency plans. Questions about how to avoid / prevent disaster are always likely.*

**Support** - ways in which software houses can support customers:

- On-site help
- Call-out
- Help desks
- E-mail
- User manuals
- On-screen
- Online help

Software package must have **support** if it is to **retain credibility** with the public.

Other methods of obtaining help are:

- Books
- Newsletters
- Online forums and blogs
- Online tutorial sites
- FAQs
- User groups



Copyright © 1999 United Feature Syndicate, Inc.  
Redistribution in whole or in part prohibited

Here you need to think carefully to explain all the ways in which software support can be provided - many of these are obvious, but you need to be able to mention and discuss them all.

**Training** - vital for highly skilled area such as ICT. Training often continuous due to the rapidly changing nature of computers.

Training courses can be:

On the job training

In house

External

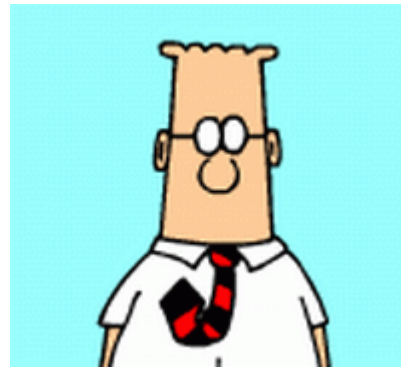
Training also includes:

Reading user manuals

Online tutorials

On-screen help

Interactive video / DVD



**ICT training strategy** = strategy to ensure that each employee has the skills necessary to carry out their job.



## Successful ICT teams

ICT projects require careful management to ensure successful completion.

A large project needs to be broken down into manageable subtasks each allocated to a small, manageable team.

Characteristics of a **successful team** are:

- Good leadership
- Appropriate balance of skills and areas of expertise amongst members
- Adequate planning and scheduling of tasks
- Skills to monitor and control progress against the plan and to control costs
- Adherence to agreed standards
- Good communication skills



## Social, moral and ethical issues

Employers need to establish a code of practice to lay down **responsibilities of ICT users**.

Code of practice will **extend legal requirements** rather than replace them - for example:

“You cannot use e-mail for personal use”

“You cannot visit internet chat rooms during work time”

Code of practice will also cover **security standards**:

Password policy

Not using another’s User ID

Logging off when leaving your workstation

It will also describe the **penalties** for breaking the code of practice (vital to enforce so the code is respected and taken note of):

Verbal / written warning

Reduced access rights

Demotion

Dismissal

Prosecution (if a law has been broken)

*Again, use the past-papers and consider what types of questions ask you about SME issues? They might ask you to explain about a code of practice or ask something like “Why do you need penalties...” Do your best to explain.*



Good luck  
in your exam!

