1. *Understand the need for a corporate information system security policy and the rôle it would fill within an organisation. Factors could include prevention of misuse, detection, investigation, procedures, staff responsibilities, disciplinary procedures.*
2. *Describe the content of a corporate information technology security policy. (Chapter 46)*

a) *Describe methods of improving awareness of security policy within an organisation. cross referencing to training and standards. (Chapter 47)*

Audit requirements

Understand that many information technology applications are subject to audit.

- *Understand the impact of audit on data and information control.*
- *Describe the need for audit and the role of audit management/software tools software.*
- *Understand the function of audit trails and describe applications of their use; e.g. ordering systems, student tracking, police vehicle enquiries.*

Disaster recovery management

Be able to describe

- *The various potential threats to Information systems. Factors could include*

physical security	*document security*
personnel security	*hardware security*
communications security	*software security*

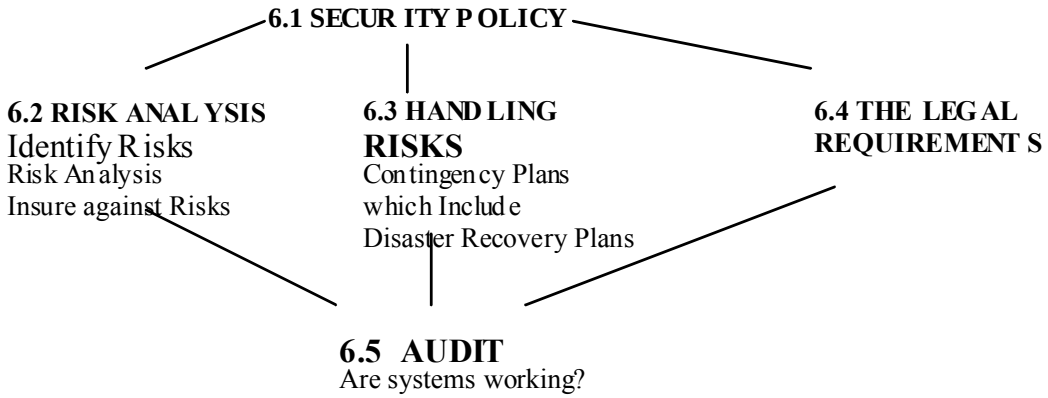
- *Understand the concept of **risk analysis***
- *Understand the **commercial need** to ensure that an information system is protected from threat*
- *Describe a range of **contingency plans** to recover from disasters and relate these to identified threats*
- *Describe the **criteria** used to select a contingency plan appropriate to the scale of an organisation and installation*

Legislation

Understand that the impact that the** implementation of legislation **will have on the procedures within an organisation

- *Describe the methods of enforcing and controlling **data protection legislation** within an organisation*
- *Describe the methods of enforcing and controlling **software misuse legislation** within an organisation*
- *Describe the methods of enforcing and controlling **health and safety legislation** within an organisation*

Discuss the implications of the various types of legislation



The commercial need is to ensure that an IS is protected from threat. This is emphasised by the following statistic:-

Seventy percent of companies that suffer a major hit do not survive the next year. Insurance may replace most of the money but, if you do not know where you spend it, your company does not survive.

6.1 THE CORPORATE IT SECURITY POLICY

This is part of an organisations' **strategic management.**

It is important to get right because

- **Costs** are involved as measures are needed to reduce the danger from deliberate or accidental damage
- **User confidence** in computer systems - no business wishes their system to contain errors or break down or be open for hackers, fraudsters, thieves and the malicious to tamper with.

IT security policies seek to secure systems against loss of **availability, integrity or confidentiality. They seek to: -**

1 **Prevent** misuse i.e.

Protect data from accidental or deliberate **disclosure** to unauthorised individuals or groups
Preserve data integrity i.e. protect data from accidental or deliberate corruption or modification.
Prevent data loss caused by software or procedural errors, or by physical hazards
Preserve data privacy protect the rights of individuals and organisations to restrict access to information which relates to them and is of a private nature, to those entitled or authorised to receive it.

2 **Detect** it if it does happen
3 **Investigate** and establish the cause of the event and the responsibility for it
4 Set up **procedures** to deal with security
5 Set out Staff **responsibilities** to prevent and report if detected
6 Set out **Disciplinary procedures**
7 **Limit** the damage to the organisation of an untoward event
8 **Recover** fully from any untoward event

http://ted.see.plym.ac.uk/ishtar/tutorial/intro3/sld001.htm	HTML slideshow and notes covering security management in healthcare.

A Good Summary of processes involved		
First Line of Defence	**PREVENTION**	Prevents threats occurring or succeeding e.g. no smoking
Second Line of Defence	**DETECTION**	Detects loss of security despite first line of defence e.g. smoke detector
Third Line of Defence	**RECOVERY**	Recovers from loss of security with minimal loss e.g. off-site back-ups.

6.2 RISK ANALYSIS

This involves investigating the following questions

What are the sources of potential threats?
Which assets are vulnerable?
Where are these assets?

Identifying risks. The most common threats to systems are:

Accidental	
Physical	**Logical**
Hardware failure, network or power failures	Human Error - made by users inputting data, programmers writing software, operators in mounting wrong media
'Acts of God' such as Lightening, Fire, Flood etc.	Software bugs - use of untested software
	Configuration faults
Deliberate	
Physical	**Logical**
Theft or physical damage to equipment	Fraud - perpetrated by users through abuse of system functionality, by programmers in manipulating software
Sabotage	Viruses - self-replicating programs which can damage data or other programs. Viruses are largely a PC phenomenon and are best guarded against by always checking incoming diskettes for existence of known viruses
	Hackers - individuals who gain unauthorised access to systems and telecommunication lines. Hackers can frequently be kept at bay by excellent access controls
	Piracy

Performing the Risk Analysis

Once threats have been identified their **potential impact must be analysed** i.e. the probability of the risk happening and the severity of its consequences e.g. loss of customer goodwill, effects on staff morale.

Risks can be approximated using actuary tables, historical evidence and reasoned estimates. Probabilities can then be accorded a % and a very high, high, medium etc. rating.

Threat	Probability	x Probability of success	'= Frequency
Incorrect data entry	Very high 90%	Medium 50%	'45%
Fine	Medium 50%	High 70%	'35%
Hacking	Low 20%	Medium 50%	'10%

A further calculation can be made whereby the annual loss exposure = cost x frequency and figures can be produced e.g. power reduction has £100 of consequent loss every time it occurs. Faulty cabling occurs once a day throughout the building with an annual cost of £30000

Other risks that can be insured against include

- Hardware replacement which will reflect the replacement cost
- Data and information loss which is perhaps the most serious but hardest to quantify
- Software loss is difficult to assess the time taken to develop
- The loss of key staff through head-hunting

Consequences of risks may include -

Interruption of processing in the long or short term	Corruption of data records
Destruction of storage media	Running of unauthorised software - clogging up the network
Disclosure of sensitive information	Theft of hardware/software
Loss of accounting records	Lost production
Delayed deliveries	Cash Flow problems
Loss of customer goodwill	Inaccurate accounting and tax statements
Meaningless and inaccurate or untimely management information	Penalties from breach of statutory obligations
Inability to continue system function	Loss of competitive position
Inability to continue business	

http://www.drj.com/new2dr/w3_030.htm	Brief notes on disaster recovery management, risk analysis and contingency planning
http://secinf.net/info/policy/hk_polic.html	
http://www.webopedia.com/TERM/a/audit_trail.html	Audit trails
http://www.disastercenter.com/abrintro.htm	Disaster recovery plans
http://www.cnn.com/TECH/computing/9908/25/disaster.ent.idg/ http://www.utoronto.ca/security/drp.htm	Disaster recovery plans - University of Toronto
http://www.grsoftware.net/backup_strategies.html	Back up strategies

6.3 Handling Risks i.e. avoidance and reduction

Tightening up Operating Standards

- Rationalise practices to aid communication and simplify education and training
- Compatibility of software, hardware, data, staff and communication channels
- All data is input to the system (by the right people) at the proper time;
- All software used to process the data has been properly tested and authorised
- Changes made to data and/or software are only made by appropriate people;
- All output from the system is delivered on time to the right people in a form appropriate for the use to which it is to be put.
- Developing clear plans to fully recover all systems, over a period of time, in an organisation in the event of a failure from whatever cause; be it a bomb which blew up the building, a failure of a chip or disk in a computer, a software 'bug', etc. These procedures are described as 'disaster recovery plans'
- Detection of any corruption of data or software in the system;
- Correction of data and software;
- Ensuring that if a recovery of the system is necessary then the recovery procedures have resulted in a complete recovery.

Segregation of responsibilities

- Users of systems to be identified;
- The functions which the user is entitled to use to be identified - Think of Jurassic Park where responsibilities were not segregated
- Provision in the software to prohibit the users from functionality which they are not allowed to use

Network Security

- Identifying elements of the system that are vulnerable
- Designing the system to limit the vulnerability. This may include providing duplicate processing facilities, alternate communication routings etc.
- Access to network restricted and protected - handshaking, dial-back
- Physical access controls - locks on computer rooms, filing cabinets
- Network users carefully classified and assigned a level of security appropriate to their jobs.
- Users who need system data to perform their jobs should have fairly easy access, while users who do not need such data should have little or no access.
- Controls to ensure recruitment of personnel who are honest and competent
- Segregation of duties between different types of job (to minimise the chance of unauthorised tampering with data)

Passwords

- Access control measures are employed to identify users and the facilities they can use. Once identified a user may

Be prohibited from access
Be allowed to read data
Be allowed to change data
Be allowed to execute programs
Be allowed to change programs

Or any combination of the above.

Data Encryption

Anti-Virus

- Restriction of third party software in case of virus infection

Fire detection and prevention

Contingency planning against disasters

Contingency planning is the process of learning how to **survive the disaster** and the longer-term processes of being able to **recover from the disaster** from the inevitable security breakdowns. It is like taking out an insurance policy. (Hope for the best, and prepare for the worst). It must be documented, tested, and ready for immediate use

Lloyds have a mandatory list which must be complied with before they are prepared to underwrite any insurance

- First line physical defences and detectors
- Off-site back-up for data, software and documentation
- Standby hardware if appropriate
- Thorough and reliable maintenance contracts
- Rules for software development and acceptance
- Good personnel procedures

Objectives of a contingency plan are to:

- **Limit financial losses** and hardships by identifying, prioritising and safeguarding those assets that the need the most protection
- **Minimise the extent of interruption.** Without a plan, the lost motion, mistakes, guesswork, and other fumbling will make the recovery plan several times longer and often impossible.
- **Define service alternatives** for accomplishing critical applications
- **Ensure controlled emergency recovery** by defining remote locations where backup files, software, documentation, etc. are stored. In addition, the plan will identify outside support that will be utilised if needed and specify the steps necessary to relocate to an alternative site if required
- **Regain total processing capability**
- **Provide trained personnel to handle emergency conditions** and recovery operations and assures adequacy and proficiency of personnel and plans through regular training, testing and maintenance.

Disaster Recovery Plan

Will minimise the loss suffered by a catastrophic disruption in service.

FIRST STAGE	To cope with the disaster by ensuring safety, minimising damage and enabling a return to work
SECOND STAGE	To minimise the consequent effects of the disaster

A key component is therefore **backing up and restoring** data for critical applications. Plans should be sensitive to how much data flows through minicomputers and telecommunication links and how much reside in mainframes. Firms use either internal or external disaster recovery facilities.

The Disaster Recovery Plan must include: - A step-by-step documentation i.e. a course of action for implementing the plan, the procedures for restoring parts of the network and the telephone numbers of key technical experts

- Knowing what hardware and software, files and human resources are required to resume processing of critical applications
- Training personnel to follow the recovery plan correctly
- Providing redundant file servers or disk drives

The people involved in security

All organisations will assign security tasks to **appropriate people**, who will be involved in

- Setting policy,
- Creating and maintaining a business recovery plan,
- Implementing access controls software,
- Investigating incidents

Many large **consultancies** offer services in IS security to supplement resources in organisations. For example:

- Advice on IS security policy and strategy provided by experienced management or IS consultants;
- Carrying out security risk analyses;
- Reviewing information systems designs and testing implemented systems to ensure security requirements are met;
- Preparation of business recovery plans.

Software engineers are employed to design and develop security products available in the marketplace-to perform independent security evaluations of systems and products. Such evaluations require highly skilled software engineers able to plan, perform and draw conclusions from rigorous evaluations using mathematical and other techniques.

Academic and applied research in IS security and related fields is carried out in many universities and private institutions often sponsored by the IS industry.

References

- As security affects most of IS the various standards covering telecommunications, operating systems, electronic data interchange messages etc. include security requirements.
- In addition specific security standards exist such as **ITSEC**: the EU standards for Information Technology Security Evaluation Criteria and the US "**Orange Book**".
- The **British Computer Society** has published Security Guidelines in Information Technology for the professional Practitioner (available from the Society).
- A British Standard (No. **BS7799**) for Information Security management was issued in February 1995 based on the Department of Trade and Industry (DTI) code of practice for Information Security Management (available from the British Standards Institution (BSI)).

6. 4 Legislation

THE BIG FOUR ISSUES

1) Confidentiality and Privacy
2) Copyright and Software Protection
3) Health and Safety
4) ICT and crime

Confidentiality and privacy

- **Privacy** is the individuals' right to determine for themselves what about them is communicated to others - limited rights through a number of laws - contract, confidence, defamation, trespass, copyright
- **Confidentiality** is an organisations right to determine what will be communicated about commercially held information that is not about people e.g. sales data, R&D findings etc.
- Increasing importance - CCTV, smart cards, PNC, document image processing

Data Protection Act 1998

- Be able to cite the Eight principles
- Be able to cite Offences and Exemptions

Costs to an organisation

- Management need to provide staff training in order to educate its staff - individual as well as corporate liability
- Siting of terminals in department store - personal data in full view of other customers
- Data management housekeeping - shredding redundant details
- Public liability insurance to cover any possible civil action
- Cost of registration
- Systems and procedures audits

Consumer Credit Act 1974 - all data subjects to have access to all credit reference data held

Copyright and software protection

In effect the protection of intellectual property

Patent Law protects hardware only

- The **Copyright, Designs and Patents Act** 1988 confirms that software is a 'literary' work for the purpose of copyright.
- Adaption is a restricted act - including compiling code. Source code is copyright.
- A software licence is permission to do something normally forbidden by copyright.
- **Software Piracy** - The best known UK group is FAST (Federation against Software Theft). The extent of software piracy is difficult to gauge but an estimate of £300 to £400 million in lost sales per year in the UK is not far off the mark.
- Work written by an internal employee in the normal course of their employment , ownership is held by the employer
- Consultants normally owns their own

Health and Safety

Health and Safety (Display Screen Equipment) Regulations 1992
Costs

- Immediately assess all workstations
- Reduce risks
- Meet minimum ergonomic standards
- Plan display screen work
- Offer eye tests
- Provide information and training

Information systems and crime

Be familiar with offences under **Computer Misuse Act 1990**

Code

- Establish and publish strong house rules on computer use that forbids employees loading personal software onto machines. This must be backed by a willingness to proceed to disciplinary action if illegal or offensive material is found
- Conduct routine and random checks of systems. Print directories and question non-registered ones
- Monitor access to public networks, call-barring
- Institute a confidential contact point.

Readings will provide up to the minute accounts e.g.
Barclaycard users on unusual spending sprees may find themselves being interrogated by store detectives because the credit card company has a knowledge based system Fraud 2000 that warns stores about apparently out-of-character purchases.
Police and Emergency services are ones to look for**.**

6.5 Audit Requirements

What is a Computer Software / Hardware Audit?

An audit is a survey, by competent persons in the Information Technology field, who are seeking to verify data on computer products (all items of software, also hardware and its components), using manual or automated means (i.e. auditing software) with the records held centrally by I.T. Services.
This includes products bought, on loan or provided by others.

What is the Purpose of such an Audit?

- To trap errors
- To monitor the efficiency of systems
- A legal requirement

It serves to:

- Bring the use of software within licence agreements, as agreed with a licence provider. An audit would ensure that software is being used legally, and would highlight any software that falls outside the scope of currently held licences.
- Reconcile records for products that have been obtained with existing records.
- Whilst most software and hardware purchases are carefully recorded, there is nonetheless a need to determine where the records may be inaccurate. This may be because products have been moved between computers, original descriptions / serial numbers were inaccurate, new products have been added which have not been recorded centrally, or items have been removed / replaced (with authority or otherwise).
- Allows for better capacity planning.
- Determining what computer system items are installed will provide a picture of what items are in use, disk capacities used, types of application, linking these to hardware requirements (e.g. RAM requirements).
- Standardise, by determining most used or possessed products;
- Assess value for insurance purposes, and replacement planning.
- Provides Information to those supporting software / hardware by knowing what computer items are installed and under what configuration, standard set-ups can be agreed which make supporting users easier, and make the user more aware of the machines, setting when contacting support personnel, e.g. in I.T. Services.

The task of Computer Auditors is to

- See that all transactions are entered
- Ensure there are no duplicate entries
- Check that arithmetic is correct (manual and computerised)
- That proper documents exist for all recorded transactions

Internal auditing

Is performed under the direction of the business itself (not a legal requirement but many companies use specialist auditors)

- To minimise the incidence of accidental or fraudulent errors in financial accounting systems
- To monitor non-financial operations e.g. production control for operational efficiency
- Data controls check entries as they occur (see validation and verification) internal auditing makes additional, physical checks after entries have been made

External auditing

An examination of accounting records only, by an independent party - usually a professional auditor

- Not concerned with the efficiency of the system, only the completeness and accuracy of its operation
- A legal requirement to ensure that a business's accounting statements provide a true picture of its financial operations

Audit management/software techniques

There are two main techniques -

1) Use of test data
2) Use of audit enquiry programs

Use of test data

- Runs the target application with test data, expected results are already known e.g. payroll figures can be tested in a variety of circumstances.
- Can be used to test source document design for input purposes
- Test batch preparation procedures
- Test input verification and validation techniques - i.e. how are normal and exceptional data handled.
- Test an applications computational and logical processes

Live Data Testing	Auditor selects examples of live data. Results are calculated manually and checked against computer output. Disadvantage auditor may not have at hand data examples that cover all possible exceptions.
Historical Data Testing	Sampling of transactions that have already passed through the system. Original transactions documents are made available for inspection, validity, authorisation and consistency with results checked.
Dummy Data Testing	Auditor constructs fictitious data which contains the conditions to be tested, used with dummy customer files since you do not want these figures entering the system

Problems

- Can be time-consuming e.g. setting up dummy files

- Provides only a snapshot at the time of the audit
- System has to be made available to auditor - not available for operational use.

Use of audit enquiry programs

- Examine contents of computer files
- Retrieve data from computer files
- Compare the contents of files e.g. two versions of the same file are compared to ensure structure has not been altered e.g. by inserting an extra field
- Produce formatted reports according to the auditors requirements
- Note that there are circumstances where updating overwrites the master file. But provided that source documents are retained or the transactions are logged onto a separate file, the auditor can still reconcile their expected effect on the master file with the actual values held there.

Audit trail .

A record of the file updating that takes place during a specific transaction. It enables policy within an organisation cross-referencing to training and standards

- Allows the trailing of a transactions history as it progresses from input to output. Computerised systems provide particular difficulties in that the trail disappears as it enters the computer system
- Auditor may ignore the computer system and pick up the trail at the output stage (auditing around the computer)
- Although audit enquiry programs allow the auditor to examine the contents of the files not every transaction effect is permanently on computer file
- Audit trails need to be designed into the system such that intermediate stages of a transaction progress are recorded for audit purposes
- A record of the file updating that takes place during a specific transaction. It enables a trace to be kept of all operations on files. An automatic record made (in journal file) of any transaction carried out by a computer system, such as updates to files. May be required for legal reasons (so auditors can confirm the accuracy of the company accounts) for security reasons (so that data maliciously or accidentally deleted can be recovered) or simply to monitor the performance of the system.

EXAMINATION QUESTIONS

1996 Many accounts packages have an audit trail facility. Explain why such a facility is necessary, what data is logged and how this information can be used.

Necessary to meet formal audit requirements and ensure protection of the system from fraud or the use of the system from the accusation of fraud (2).
An audit trail is the software functionality to produce a selective record of what has been happening on the system; who has been using it, when, how long for and what this person did with the data (2).
There must be several ways of analysing the record relating to different levels of task (2).

1996 A particular college use a computer network for storing details of its staff and students and for managing its finances. Network stations are provided for the Principal, Vice-Principal, Finance Officer, clerical staff and teaching staff. Only certain designated staff have authority to change data or to authorise payments.

(a) What are the legal implications of storing personal data on the computer system? (4)
(b)What measures should be taken to ensure that the staff understand the legal implications?(3)

ANSWER
(a) Any from:

The college must apply for registration under the Data Protection Act. *Adequate protection should be applied to the system and data.* *The registration will specify the data use and data can be held.* *Only authorised users should have access to the data as specified under the registration.* *The college must supply details of the data held to the data subject on request.* *amplifications or equivalents accepted*

(b)Any from:

There should be an in-house policy to inform staff of the college terms of registration. *This may include a list of 'good and bad practice' points for staff. Appropriate examples may include:*	
handling data and discs,	*access levels,*
password changes,	*file security measures,*
log-on/off procedures,	*physical security measures etc.*
Back up copies kept off site	*roll back of failed transactions*
This may include any contractual matters of disciplinary measures for staff who fail to comply.	

1996 Some software packages can be set up to monitor and record their use, this is often stored in an access log.
Name **four** items you would expect to be stored in such a log. (4)

Time and date of access	*Terminal ID*
Person ID	*Person Password*
Files accessed	*Activity e.g. menu route*
Log off time	

1997 A company uses a computer network for storing details of its staff and for managing its finances. The network manager is concerned that some members of staff may install unauthorised software onto the network.
(a) Give reasons why it is necessary for some software to be designated as unauthorised. (2)
(b) What guidelines should the network manager issue to prevent the installation of unauthorised software onto the network? (2)
(c) What procedures might be available to the company to enforce the guidelines? (2)

(a) The company has not purchased a license. *The company has purchased a fixed number of licenses however the particular user has not been allocated access rights (or had loaded onto local disc).* *The software is share-ware but not authorised by the network manager.* *Authorised source code has been modified without authorisation.* *Personally owned software has been installed* *Software may introduce non-standardisation* *Software may facilitate unauthorised data changes e.g. by-pass audit log* *Software may compromise network security=causes a virus=prevent data corruption*

Distracts from work (1)
(b) A written IT policy or Security Policy (1)
stating the responsibilities of staff as defined in the Computer Misuse Act (1).
explicitly forbidding the installation of any software except by authorised staff (1)
OR reverse equivalent e.g. it must be authorised by Network Manager
specifying how to request new software (1)
specifying how to request changes in access rights (1)
ACCEPT
code of conduct (1)=signed booklet(1)=in written contract (1)
NOT audit log software, training, log-on screens etc
(c) formal written warning
suspension or termination of contract
legal action under the terms of Computer Misuse Act
restrict file creation rights (perhaps to withhold executable status)
*automatic logging of **executables** and reporting of **changes** must have the bolded*
disciplinary procedure (0) instant dismissal (1)
NOT contact FAST

1998.9 (20 marks)
"Information systems are mission critical, the consequences of failure could prove disastrous."
Discuss this statement, including in your discussion:

- the potential threats to the system
- the concept of risk analysis
- the corporate consequences of system failure
- the factors which should be considered when designing the 'contingency plan' to enable a recovery from disaster.

*Mark allocation: approximately **4 for points made on threats**, approximately **4 for the concept of risk analysis**, approximately **4 for the corporate consequences of system failure**, approximately **4 the factors which should be considered when designing the 'contingency plan' to enable recovery from disaster**, approximately **4 for the coherence of argument** and quality of language.*
Ceiling of 4 on each. Ceiling for content is 17

***the potential threats to the system (max 4)** e.g. fire, virus, hacker, bugs (4), [millennium bug (1)] (1) for main aspect then a further (1) for expansion to a max of 4*
cannot gain 4 for a list...max for any list =2
(a) physical..fire, flood, power failure, cables, coffee
(b) hardware failure...processor failure, disc crash
(c) telecommunications failure...cable faults, data corruption, gateway down
(d) data control failure...data inaccurate e.g. rounding, incorrect codes
(e) software failure...bugs, unsuitable to task
(f) invalid data...user errors, undiscovered corruption e.g. upgrade, processing cycle fault
(g) computer crime/abuse...hacking (1) viruses (1)
(h) system design failure...failure to build into the design the appropriate measures

***the concept of risk analysis** mark as (1) for each aspect if explained to a max of 4*
(a) determine risks and design countermeasures to appropriate level e.g. estimate impact, limited (1 day), severe (1 week), major (1 month), critical (!)
(b) risks change from system to system
(c) risks change from data to data and time to time

(d) risks change from time to time e.g. pc system in 'open office' storing local stock records at greater risk than multi-national mainframe system storing latest car design but the latter is more likely to be a target
{this answer would obtain approx 2}
(e) in order to determine risk a review of threat must be undertaken review may be:
*(f) on a quantitative basis e.g. Expected annual loss = probability of fire over 10 years (=0.02) * cost of fire (=£1000,000) i.e £20K per annum. Repeat this for each potential risk area.*
(g) on a subjective basis e.g. consult all staff, consider nature of business, operation, competition, likelihood of problems and 'work-arounds'
(h) using a checklist e.g. a software package to compare to all recognised dangers for this type of installation/activity. The package attaches weights to risks and provides an index rating of risk.

1989.1 (3 marks)
Some IT applications use software which maintains an audit trail.
Name **one** such application and state why this facility is necessary.

Application: any acceptable e.g. police vehicle enquiries, ordering systems, student tracking. accounting (NOT 'in bank')
Why necessary: to meet formal or legal (1) audit requirements, to ensure protection of the system from fraud (1) or the accusation of fraud (1).
Track & check for mistakes (1)
Network Software (1) Log of network access (1) Monitor network abuse (1)
Log of internet access (1) to track sites visited (1) to track source of virus if one downloaded (1) or monitor net. abuse (1)
Supermarket (0) Transaction log (0)
What an audit trail does (0)

June 2000.2 (10 marks)
An insurance company is reviewing its disaster recovery management policy
b) At a strategic level, state six potential threats to an information system. (6)
c) Explain the concept of risk analysis. (4)

2 (a) Possible strategic level threats:
Mark a 6 @ 1 per point max 6
- *Physical security=natural disaster, electrical spikes,access to building*
- *Document security*
- *Personnel security=human error inputting data, disgruntled employee*
- *Hardware security=failure=hardware theft*
- *Communications security=hacker=virus=firewall*
- *Software security=failure=passwords, access levels*
- *Data security=data loss, theft, backup strategy*

Computer crime (1) but includes many of the above
Computer failure=0
(b) Risk analysis mark as (1) for each aspect to a max of 4 for single issue OR 2 @ 2 if explained
- *determine risks and design countermeasures to appropriate level e.g. estimate impact, limited*
- *(1 day), severe (1 week), major (1 month), critical (!)*
- *risks change from system to system, data to data and time to time*
- *on a quantitative basis e.g. Expected annual lost=probability of fire over 10 years (=0.02)*
- *cost of fire (=£1000,000) i.e £20K per annum. Repeat this for each potential risk area. on a subjective basis e.g. consult all staff, consider nature of business, operation, competition,*

likelihood of problems and ‚work-arounds™ e.g. pc system in ‚open office™ storing local stock records at greater risk than multi-national mainframe system storing latest car design but the latter is more likely to be a target {this answer would obtain approx 2}

June 2002.4

A Medical Practice has installed a new information system that links patient records and prescriptions to the financial systems of the practice. The financial records must be secure against fraud as they are used to claim money from the Health Authority.

a. Describe **four** factors that should be included in an IT security policy for the practice. (8 marks)

b. Describe **one** measure the practice could take to show that their records were accurate. (2 marks)

c. Describe **three** criteria that could be used to select a disaster contingency plan to recover from a breakdown of this system. (6 marks)

a. 1 for factor (F), 1 for description/example (E) - max. 4 x (2, 1, 0)

- *prevention of misuse/protection against misuse/prevent unauthorised access (F); allow any sensible prevention example e.g. physical, anti- hacking etc (NOT vetting of staff)*
- *detection of misuse; e.g. finding an anomaly/discrepancy by regular checking investigation of misuse; e.g. by using monitoring software, audit trail etc*
- *procedures for keeping data safe e.g. data backup, file passwords etc*
- *staff responsibilities e.g. network manager monitors,' responsibilities for backup procedure*
- *disciplinary procedures*

b. By using an audit trail (1) to show what was amended and by whom/when (1)

c. 1 for name, 1 for description/expansion/example - max. 3 x (2,1,0) Generic answers/example accepted, therefore context not important, but do not allow examples using contexts that are definitely not medical centre related

- *Scale/size of organisation*
- *Timing e.g. how quickly to recover system and be up and running, how important for the company*
- *Costs of implementation/contingency site/external contract (make sure costs are of the plan, NOT costs if no disaster recovery plan or as a result of a disaster)*
- *Likelihood of disaster*
- *NOT*
- *volume of data*
- *any of the contents of the plan*

January 2003.8

A growing organisation has realised that so far they have been lucky in that their information systems have not failed. Before they expand their business operational reliance on ICT, they have been advised by their insurer to carry out a risk analysis and then plan what to do next.

a. Explain what is meant by risk analysis. (3 marks)

b. State three different potential threats to an information system, and describe a counter-measure for each one. (9 marks)

c. Describe three of the criteria that could be used to select a disaster contingency plan. (6 marks)

a.
(Any 3x1)

- To identify each element of a successful information system (1)
- place a value - to the business - on that element (1)
- identify any potential threats to that element (1)
- the likelihood of the threat occurring (1)

b.

1 for threat(T), 1 for counter-measure(C), 1 for description of why/how it would counteract the threat(E). Any 3 x (3,2,1,0)

- Physical - e.g. theft/terrorists - use locks etc - prevent easy entry
- Personnel - e.g. accidental overwrite - have procedures - trained staff less likely to make mistakes
- Hardware - e.g. disk crash - have duplicate system - so that system can be up and running asap
- Communications breach - e.g. hacking in - firewalls, encryption, passwords -to lessen ability to see/steal/tamper with data
- Virus - e.g. Trojan - anti-virus software - to stop files getting infected
- Natural disaster causing hardware/software/data loss - e.g. Fire/flood/earthquake - backup kept off-site - so that a safe copy is held and system can be reloaded
- Electrical surge/power loss - e.g. caused by weather - UPS/ off-site duplication/RAID/Mirror - as above
- Data errors, inaccurate data in system - verification and validation - pick up data errors before they get into the system

c.

1 for criterion(C), 1 for description(E), Any 3 X (2,l ,0)

- Scale of the organisation and its ICT systems
- Nature of the operation (e-business, on-line, batch)/Timing of recovery - how long until the system would be operating, and if this is important to the business
- Costs of recovery options relative to "value" of systems
- Perceived likelihood of disaster happening, based on risk analysis

NOT:

- Volume of data
- Size of the system
- Any of the contents of the recovery plan (e.g. how to set up, reciprocal site, who does what or anything to do with back-ups)

6 marks

January 2003.9 (20 marks)

Puregreens, a retailer of organic vegetables, has recently launched a marketing website. The e-mail response from the "contact us" button has been overwhelming, so they are thinking of expanding into selling on-line. Discuss the implications of this, paying particular attention to the following:

- methods of data capture that will be available for on-line or offline payment;
- the control and audit issues associated with this method of selling;
- the information needs of the management of this system;
- the additional information that might be generated.

The Quality of Written Communication will be assessed in your answer.

Continuous prose is expected for this answer. Discuss is the question, so each point made must be full, not just a single word/phrase. Mark as M, C and I or

A for four bullets - no more than the given marks awarded in each section
Methods (M) - max 4 - could be

- *filling in credit/debit card details on-line and submitting the payment*
- *printing a form for off-line filling in, either by word processor or by hand or .pdf; submitting by e-mail, or by non-electronic means (i.e. post with a*
- *cheque)*

Control and audit (C) - max 6 -

- *ask for pre-shopping registration - e-mail back access codes*
- *confirm order to e-mail address (insist e-mail address provided, check exists)*
- *use of credit checking agencies*
- *use of electronic payment, normally specialist applications/services - get authorisation before dispatching goods*
- *basic cross-field validation - e.g. checking address is correct for postcode; restricting values in fields*
- *keeping customer details secure and protected during communication (SSL or equivalent)*
- *holding previous orders and/or payment details, making easy to reorder same (like Tesco)*
- *adherence to Data Protection Legislation e.g. not passing data on unless the customer has given permission*

Information needs (I) - max 4 -

- *different levels of information (Strategic, tactical and operational)*
- *source*
- *frequency*
- *(gathering) customer info, demographics, spending habits/patterns and so on*

Information generated (A) - max 5 -

- *targeted market research/opinion, also targeted advertising/special offers to generate more sales*
- *food, seasonal, supply and demand issues (no point stocking up on*
- *certain items out of season if no/little demand - esp. as most is produce with short shelf life*
- *importance of having up-to-date information of use for*

16 marks may for content

June 2000.10 (20 Marks)

IT managers have to be aware of certain legislation that will impact on the procedures within both their department and the rest of their organisation.
Discuss this statement. Particular attention should be given to:

- . methods of enforcing and controlling the protection of data within the organisation,
- . methods of enforcing and controlling the use of software within the organisation,
- . the role of the IT department in developing and implementing suitable strategies to assist in these tasks.

Quality** of **language will be assessed in this nnsww

Mark allocation:
• approximately 6 in total for methods of enforcing (both bullet points, i.e. no repetition)
• approximately 6 for methods of controlling the protection of data
• approximately 6 for methods of controlling the use of software
• approximately 6 the role of the IT department in developing and implementing suitable strategies
Up to 4 for the quality of language

Ceiling for content is 16
NOT Health & Safety, Copyright, Data Protection Act
approximately 6 in total for methods of enforcing *(both bullet points, i.e. no repetition)*

- *Concept of implementation of appropriate legalisation (NOT 1 mark for mention of DP Act) (0/1/2/3) e.g. need to register (1)*
- *Concept of internal policies & procedures to implement legislative framework (0/1/2/3) e.g. appoint a DP Co-ordinator (1) e.g. sign an agreement when join company (1)*
- *Concept of monitoring and reporting procedures within the organisation (0/1/2/3) e.g. audit trail (1), reminders to staff (1) e.g. need to sign a contract (1) or may get sacked (no 2 nd mark)*

approximately 6 for methods of controlling the protection of data
(note this is IT04–we are looking for broader concepts rather than single words)

- *Concept of environmental & physical controls.eg locked doors (1/2)*
- *Concept of access controls e.g. logon/password/terminal/times (1/2/3) MUST BE Hierarchy*
- *Concept of application controls e.g. document/report/storage/ (1/2)*
- *Accept any 2 aspects of DP Act control e.g. how do they keep data accurate OR facilitate requests for access to personal data (2)*

approximately 6 for methods of controlling the use of software

- *Concept of systematic identification of software needs e.g. audit (1/2/3)*
- *Concept of installation control & licensing e.g. formal requests via software manager (1/2)*
- *Concept of monitoring controls e.g., monitoring software, collection of notebooks (1/2) e.g. well described use of audit software (2)*

approximately 6 the role of the IT department in developing and implementing suitable strategies
Strategies should be contained within an IT Security Policy
Formulation of IT Security Policy: stages: -
Analysis of risks
• measurement of past occurrences
• adequacy of current safeguards
• likelihood of future failure
• potential disruptive impact
Definition of IT Security Objectives
• cross reference to organisational strategic objectives
• management objectives
• operational objectives
Preparation of IT Security Policy:
• review of institution needs
• application of Standards e.g. FAST
• IS facilities in place
• Personnel procedures
• Legal and audit requirements
• Formal procedures
Implementation of IT Security Policy
Monitoring of IT Security Policy
• Number & duration of incidents
• Cost recurrent and capital
• Other factors e.g. insurance, recovery
• Formal reporting of above to management
It is highly unlikely that candidates will use this approach. Marking should be @1 mark per concept listed above.

Examples
lock away master copies of software (1)
firewall (1)
encryption (1)
force change in passwords regularly (1)
dongle (1)
call back routines (1)™
separation of duties (1) plus another if explained
escort from building procedures

June 2003.7

Organisations that operate TCT systems have to comply with the relevant legislation. Most have procedures to ensure that this happens.

(a) Describe **three** methods of enforcing and controlling data protection legislation within an organisation. *(6 marks)*

(b) Describe **three** methods of enforcing and controlling software misuse legislation within an organisation. *(6 marks)*

(c) Describe **three** methods of enforcing and controlling health and safety legislation within **an** organisation. *(6 **marks)***

June 2003.9

The expansion of e-business using the Internet in the past few years has led to more businesses including this medium for their operations. In the absence of 'a regulatory body to police the Internet, the 1CT and computing industry must regulate itself.

Using **specific examples,** discuss this statement. Include in your discussion:

- why regulation might be required;
- the issues in devising regulation across a world-wide medium;
- the potential problems in enforcing regulation.