Answers

1 (a) A matrix structure is likely to be found in contracting, research and development and consultancy and essentially 'crosses' functional and product/project organisation so that staff in different functional or regional departments are responsible to both their department manager and also to a product or project manager. They are responsible to their departmental or functional manager for activities specific to the department or function and to the project manager for activities specifically relating to the product or project. Typically, staff from various disciplines are assigned to projects. While engaged on the project individuals will be responsible on a day-to-day basis to the project leader but will continue to be functionally responsible to the head of their department.

(b) The key advantages of a matrix structure are: it enables the organisation to quickly assemble teams consisting of people with the most appropriate expertise and experience; it allows speed of response and flexibility; it provides a variety of experiences to team members; it supports inter-disciplinary co-operation and multi-functional working; it develops tolerance of ambiguity; it encourages team members to see the broader picture rather than over focus on their own specific department or functional area; it encourages greater market and customer awareness, it brings conflicts out into the open.

(c) The key disadvantages of a matrix structure are: it can be fragmented; it can be difficult to develop and maintain commitment to the organisation; it requires individuals to be responsible to two bosses simultaneously; it needs careful planning; it can lack continuity; it can lead to competition and conflict between managers; staff can have conflicting demands; decision making can be slower.

2 (a) The external auditor is usually a firm of chartered or certified accountants whose role is to undertake an independent examination of the financial statements of an organisation and to express an opinion on those financial statements. If the organisation is a limited company, external audit means statutory audit, under for example the Companies Act 1985 in the UK.

(b) The purpose of the external auditor's report is to summarise their conclusions on the company's financial statements to the shareholders. The report must state whether in the auditor's opinion:

- The balance sheet is a true and fair view of the financial state of affairs of the company at the end of the financial year. The words true and fair are generally used together rather than separately and the term is generally considered to mean 'reasonably accurate and free from bias or distortion'
- The profit and loss account or income statement gives a true and fair view of the financial performance of the company for the financial year being audited.
- The financial statements have been properly prepared in accordance with Companies Act 1985, or other similar legislation.

(c) There are three main differences between the internal and the external auditor:

- Appointment. External auditors are appointed by the shareholders and must be independent of the company whereas internal auditors are employees of the organisation
- Responsibility. External auditors are responsible to the owners, who can be shareholders, the public or parliament whereas internal auditors are responsible to senior management
- Objectives. The objectives for external auditors are defined by law whereas those for internal auditors are set by management and the audit process is a key part of evaluating the effectiveness of the management control system in the light of risks identified.

3 (a) The classical theorists were primarily concerned with the maintenance of control from the top of an organisation. They wrote at a time when relatively little was understood about the ways in which organisation design can affect human motivation and about the human relations aspects of management and work organisation. The classical school of management held the view that there were universal principles that can be applied to all organisations. Management was seen as a matter of **controlling resources and processes** rather than people. Classical theory focuses on the efficient **structuring of** organisations. Henri Fayol was one of the most influential classical theorists – a French industrialist who pioneered ideas about how organisations might best be structured – he advocated that there should be **division of labour** i.e. the practice of dividing work into specialised tasks that enable people to specialise in what they do best. Other important elements of the classical school were the ideas of **limited spans of control** (i.e. number of direct subordinates) – typically a limit of three to six were recommended and also that there should be a limited number of hierarchical levels. Spans of control were to be limited so that it was possible to retain adequate supervisory control over subordinates, sufficient communication with them and adequate coordination between their activities. **A restricted number of hierarchical levels** were advocated so that loss of control down a hierarchy and any dilution of instructions before they reached the required level were minimised.

(b) **Planning** involves working out, in broad outline, the things that need to be done and the methods for doing them to accomplish the overall purpose set for the organisation. This involves setting objectives and the procedures for ensuring that the objectives are achieved. This can be for the whole organisation or for a part of it. **Organising** involves setting up and staffing the most appropriate form of organisation to achieve its overall aims and objectives. This will include grouping task and activities into jobs for individuals and groups, creating groups of jobs into sections and departments and delegating authority to carry out jobs. **Commanding** involves giving instructions to others to carry out tasks where the manager has

authority over decisions and responsibility for performance. This also involves exercising leadership to motivate people to work together to the best of their ability as part of a team. **Coordinating** involves harmonising the activities of individuals and groups within the organisation and integrating various parts of the work. **Controlling** involves measuring, monitoring and correcting, as necessary, the progress of work in relation to the overall plan – this will include the activities of individuals and groups.

4 **(a)** Conflict takes place in organisations because they function by means of adjustments and compromises. People's views often conflict because individuals and teams have their own goals, interests and priorities which may not always be compatible. In addition there can be personality clashes. Conflict can arise when there is change because change may be seen as a threat to be challenged or resisted. Power and resources in organisations are limited and people compete for them - this can also lead to conflict. There may also be differences and incompatibilities of work methods, timescales and working style so that individuals or teams frustrate each other with apparent lack of co-ordination. Poor communication can often lead to conflict.

(b) This approach suggests that there are three basic ways in which a conflict or problem can be worked out: win-lose, lose-lose or win-win. Firstly, win-lose – this is quite common and describes a situation where one party gets what it wants at the expense of the other party. Secondly, lose-lose – this describes a situation where neither party gets what it really wanted - in essence a poor compromise. This is often a common outcome to resolving conflict. Thirdly, win-win – this is not necessarily common but working towards it often leads to the best solution. It describes a situation where both parties get as close as possible to what they really want. It is critical to this approach to fully understand what both parties really want, and what they really don't mind giving up.

5 **(a)** The main risks to data are as follows:

(i) human error – individuals can lose, damage or incorrectly input or store data;

(ii) technical problems – data can be lost or corrupted when equipment fails;

(iii) catastrophic events such as natural disasters or accidents such as fire or burst pipes can break or destroy data storage and transmission facilities;

(iv) malicious damage by individuals inside or outside the organisation who deliberately attempt to damage or tamper with data;

(v) industrial espionage or sabotage by individuals who deliberately attempt to steal or damage data and information from the organisation with a view to commercial gain;

(vi) dishonesty by those who may wish to access information for personal gain;

(vii) when data is transmitted over a network or a telecommunications line, especially the internet, there may be additional specific security dangers which arise because the data is carried by third party carriers and is outside the direct control of the organisation;

(viii) additional dangers include the following: corruptions from viruses, the possibility of inadvertently overwriting someone else's data, unauthorised individuals being able to access parts of the network, risks from hackers, the downloading of inaccurate or imperfect information or information being intercepted leading to loss of service;

(ix) in addition to the above, all organisations have a responsibility to ensure that data is adequately protected against any breaches of confidentiality.

(b) There are a number of ways in which the risks to data identified above can be minimised. Risks of human error can be reduced by checks and controls, systematic procedures, ongoing employee training and also appropriate supervision. Rigorous recruitment and selection procedures go some way to ensuring that staff employed are honest and trustworthy and will not engage in malicious acts or any form of espionage. Risk of malicious damage can also be minimised by controlling access, both physically (using locks and security checks) and electronically (using passwords, encryption of data, anti-virus software etc). Risks of disaster are difficult to foresee, but contingency plans may be made, including off-site back-up storage of files, emergency power generators and adequate insurance for any loss or damage to data and associated systems. Organisations should take care to ensure that paper files or computer disks are not left where they are generally accessible. Safes, strongboxes and filing cabinets should be locked when not in use. Passwords should be used where advised and should not be shared. Confidential information should not be copied or transmitted without specific authorisation and appropriate security measures. It is important to ensure that appropriate communication channels are selected to protect data where necessary. Back-up systems are important to minimise the risks associated with data held electronically. E-mail, intranets and the Internet mean that computer systems are increasingly connected over telecommunications lines and these are rarely completely secure. Use of passwords and userprofiles make an important contribution to minimising risk. A password is a unique code a person uses to enter the system. For a password system to be effective, passwords should be changed regularly, difficult to guess, confidential and hidden. A user profile in a networked system only allows certain people access to certain files. Records can be kept of access to files, so that a trail can be left of unauthorised attempts at entry. Despite passwords and user profiles, expert hackers may still be able to enter the system. Keeping track of any attempts made can alert managers to repeated attempts to break into the system or of any emerging patterns. Use of anti-virus software which can detect and eradicate viruses is an important way to minimise risks to electronic data. Latest upgrades should be used to ensure that any new viruses could be dealt with. Organisations must also guard against the introduction of unauthorised software to their systems as many viruses are spread on pirated versions of popular software. Any disks received from outside should be checked to ensure that they are virus free. Systems should also make use of firewalls to ensure the safety and security of their data.

ACCA Certified Accounting Technician Examination – Paper T5
Managing People and Systems **June 2005 Marking Scheme**

1	**(a)**	4 marks for clear explanation of matrix structure	4 marks
	(b)	2 marks for each advantage up to a maximum of	8 marks
	(c)	2 marks for each disadvantage up to a maximum of	8 marks
			Total 20 marks

2	**(a)**	3 marks for a clear explanation of the role	3 marks
	(b)	2 marks for the purpose of the report. 2 marks for each item included up to a maximum of	8 marks
	(c)	3 marks for each difference identified up to a maximum of	9 marks
			Total 20 marks

3	**(a)**	10 marks for clear explanation of classical management, to include control issues, spans of control, hierarchy, universal rules, top down, and consideration of human aspects.	10 marks
	(b)	5 marks for each full explanation of any two functions.	10 marks
			Total 20 marks

4	**(a)**	2 marks per valid point made about each source of conflict identified up to a maximum of	12 marks
	(b)	3 marks for clear description of win-win, 2·5 marks for contrast with win-lose, 2·5 marks for contrast with lose-lose.	8 marks
			Total 20 marks

5	**(a)**	2 marks per valid point made about each potential risk identified and explained up to a maximum of	10 marks
	(b)	2 marks per valid point made about each method of minimising risk explained up to a maximum of	10 marks
			Total 20 marks