An **internal audit** department should be able to verify that the control system is working and to review the system to ensure that it is still appropriate for current circumstances.

Activity 3: Threats to systems and data

Fire

Fire is the **most serious hazard** to computer systems. Destruction of data can be even more costly than the destruction of hardware.

A fire safety plan is an essential feature of security procedures in order to prevent fire, detect fire and put out the fire.

Water

Water is a serious hazard. Flooding and water damage are often encountered following firefighting activities elsewhere in a building.

This problem can be countered by the use of waterproof ceilings and floors together with the provision of adequate drainage.

Weather

Wind, rain and storms can all cause substantial **damage to buildings.** In certain areas the risks are greater, for example the risk of typhoons in parts of the Far East. Many organisations make heavy use of prefabricated and portable offices, which are particularly vulnerable.

Lightning

Lightning and electrical storms can play havoc with power supplies, causing power failures coupled with power surges as services are restored.

Power failure can be protected against by the use of a **separate generator** or rechargeable battery. It may be sufficient to maintain power only long enough to close down the computer system in an orderly manner.

Terrorist activity

Political terrorism is the main risk, but there are also threats from individuals with **grudges.**

In some cases, there is very little that an organisation can do: its buildings may just happen to be in the wrong place and bear the brunt of an attack aimed at another organisation or intended to cause general disruption. **Physical access** to buildings should be controlled.

Accidental damage

People are a physical threat to computer installations: there can be few of us who have not at some time spilt a cup of coffee over a desk covered with papers or tripped and fallen doing some damage to ourselves or to an item of office equipment.

Combating accidental damage is a matter of having a good office layout and eliminating hazards, such as trailing cables.

Activity 4: Security measures (1)

'Postcode' all pieces of hardware. Invisible ink postcoding is popular, but visible marking is a better deterrent. Heated soldering irons are ideal for imprinting postcodes onto objects with a plastic casing.

Mark the equipment in other ways. Some organisations spray their hardware with permanent paint, perhaps in a particular colour (bright red is popular) or using stencilled shapes.

Hardware can be bolted to desks. If bolts are passed through the desk and through the bottom of the hardware casing, the equipment can be rendered immobile.

Ensure that the organisation's standard security procedures (magnetic passes, keypad access to offices, signing in of visitors, etc) are followed.

Activity 5: Security measures (2)

Don't worry if your suggestion is not in the solution - these are just illustrations to give you an idea of the sort of thing you would see when considering IT security risks and controls.

Risk	Example	Control
Human error	Input error when recording an invoice	System limitations on acceptable entries
Malfunctioning hardware or software	Breakdown due to poor treatment	Proactive maintenance and user education
Natural disasters	Fire in an office containing systems and data	Off-site back-up and physical controls (such as Halon gas)
Deliberate actions	Fraud by staff	Segregation of duties
Commercial espionage	Insider dealing	Systems monitoring
Malicious damage	Viruses or other malware	Anti-virus software and user education on emails
Industrial action	Strike action	Maintain good relations with staff

Activity 6: Fintech

Again, your explanation may not exactly match the ones used in the solution, but as long as you have a good, general understanding of each term, you should be prepared.

Type of Fintech	Explanation
Automation	Accounting software can automatically download transactions from an organisation's online bank account. This saves the accountant time and frees them up to focus on more value-adding activities (such as analysis).
Artificial intelligence	Artificial intelligence (AI) in accounting software can assign transactions to appropriate nominal codes and record the transactions appropriately in the accounts. This intelligence is achieved by the accountant recording the transactions manually a few times before the system learns what types of transactions should be assigned to which nominal codes. Auditors can use AI systems that perform complete checks on financial data held, allowing 100% of transactions to be audited automatically on a continuous basis, removing the need for an auditor to perform routine audit checks to verify transactions.
Big data and data analytics	Predictive analytics helps auditors better target their work on key risks, improving the relevance of audits, for example it can be used by an auditor to find all sales transactions recorded near to or over the materiality level.
Distributed ledger technology	Blockchain is an example of a distributed ledger. For accountants and auditors, distributed ledgers and Blockchain allow for increased clarity and transparency in the recording of business transactions. This is because transactions are posted to a public ledger on a Blockchain. Distributed ledgers also reduce the need for auditors to audit transactions and verify the ownership of assets because they have a source of information about the assets that they can trust (this is due to records being encrypted and as such, secure).

11 Identifying and preventing fraud

Learning outcomes

On completion of this chapter you should be able to:

	Syllabus reference no.
Explain the circumstances under which fraud is likely to arise.	C7 (a)
Identify different types of fraud in the organisation.	C7 (b)
Explain the implications of fraud for the organisation.	C7 (c)
Explain the role and duties of individual managers in the fraud detection and prevention process.	C7 (d)
Define the term money laundering.	C7 (e)
Give examples of recognised offences under typical money laundering regulations.	C7 (f)
Identify methods for detecting and preventing money laundering.	C7 (g)
Explain how suspicions of money laundering should be reported to the appropriate authorities.	C7 (h)

Exam context

This chapter considers the various types of fraud that an organisation may be prone to and which may have to be investigated by internal audit. It is important that you are able to identify signs of fraud in different circumstances.

You also need to have a good knowledge of both how fraud is prevented and detected. Although there may be significant costs involved in implementing a good system of fraud prevention, the consequences of successful fraud may be very serious, both for the reputation of the organisation and the position of its directors. Money laundering represents a serious problem, but systems can be set up to help detect and prevent this.

The practical aspects of fraud (where it might occur and how it can be detected) are the most likely areas to be examined, as shown by the specimen exam where there was one Section A question on the topic and part of one of the Section B questions featured the issue of internal controls and fraud.