Unit 5 –Security

LO3. Review mechanisms to control organisational IT security.

9. Risk Assessment and Integrated Enterprise Risk Management.-2

Hardware and Software Risk Assessment

- A security risk assessment identifies, assesses, and implements key security controls in applications. It also focuses on preventing application security defects and vulnerabilities.

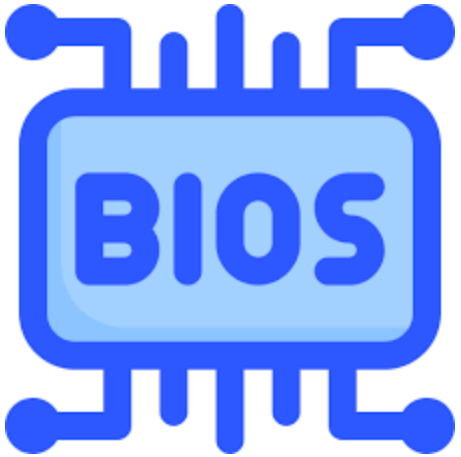
Hardware Risks and Software Risks

Hardware Risks	Software Risks
Computers with conventional BIOS.	Unpatched or out-of-date operating systems
Computers without pre-boot authentication (PBA) or a Trusted Platform Module (TPM)	Unpatched web browsers

Hardware Risk

- **Computers with conventional BIOS.**

Older PCs, as well as laptops and notebooks, with conventional BIOS cannot run Secure Boot. Secure Boot helps to prevent malware from loading onto a computer during the boot process.



Software Risks

- **Unpatched or out-of-date productivity software**

Running unpatched versions of Microsoft Office, especially older versions like Office 2002, Office 2003 and Office 2007, is risky.

A common vulnerability is the potential for remote code execution when a user opens or previews a maliciously prepared file or visits a website containing content that exploits the vulnerability.

Data Protection Act of 1998

- The Data Protection Act 1998 (DPA 1998) is an act of the United Kingdom (UK) Parliament defining the ways in which information about living people may be legally used and handled.
- The main intent is to protect individuals against misuse or abuse of information about them.
- The DPA was first composed in 1984 and was updated in 1998.

Why the Data Protection Act was developed?

- Give protection
- Lay down rules about “how data about people can be used?”
- The Data Protection Act (1998) states that organizations which store personal information must register and state the purpose for which they need the information.

Data Protection Act of 1998

Information or data stored on a computer or an organized paper filing system about living people in different departments such as:

- Tax Office
- National Insurance
- Driver and Vehicle Licensing Centre
- Police etc.

Tax

How the Act works?

- By setting up rules that people have to follow.
- Having an Information Commissioner to enforce the rules

Who's involved?

- **The Information Commissioner**

The person (and her office) who has powers to enforce the Act.

- **A data controller**

A person or company that collects and keeps data about people.

- **A data subject** is someone who has data about them stored somewhere, outside their direct control.

Computer Misuse Act of 1990

- This is an Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

It is designed to stop the 3 main offences under the act:

- Unauthorised access to computer material (hacking).
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material.

ISO 31000 Risk Management

- **Risk is:** The effect of uncertainty on the ability of an organization to meet its objectives.
- **Risk management is:** The range of activities that an organization intentionally undertakes to understand and reduce these effects.

ISO 31000 Risk Management

- **Effective risk management is:** Executing these activities efficiently and in a way that actually and demonstrably improves the ability of the organization to meet its objectives in a repeatable fashion.

ISO 31000 Risk Management

- ISO 31000 provides direction on how companies can integrate risk-based decision making into an organisation's governance, planning, management, reporting, policies, values and culture.
- It is an open, principles-based system, meaning it enables organisations to apply the principles in the standard to the organisational context.

ISO 31000 contains:

- A set of risk management terms and their definitions.
- Set of principles for guiding and informing effective risk management for an enterprise.
- An outline and process for creating a risk management framework.
- An outline and process for creating a risk management process.

Lesson Summary

- Hardware and Software Risk Assessment
- Data Protection Act of 1998
- Computer Misuse Act of 1990
- ISO 31000 Risk Management