**Unit 7 Assignment 1 Checklist**

P1 - **Explain** the different security threats that can affect the IT systems of organisations.

* Internal threats - e.g. employee actions, data theft, accidental loss, unintentional disclosure or damage to data, unsafe practices (use of external flash storage, visiting untrusted websites, downloading/uploading files to/from the internet, users overriding security controls, file sharing apps
* Unsafe practices: BYOD, Use of USB
* External threats - e.g. data theft, destruction, withholding and/or disruption of systems (by competitors, cyber criminals, governments, terrorists) for political purposes or financial gain
* Physical threats - e.g. theft of equipment or data, malicious damage to equipment or data, damage or destruction by fire, flood, terrorist action or other disaster
* Social engineering
* Software threats(Malware) - Techniques used to obtain secure information (software that has a malicious intent), e.g. malware, viruses, worms, Trojan horses, ransomware, spyware, adware, rootkits and backdoors.
* Network threats –
  + Passive threats, including wiretapping, port scanning and idle scanning.
  + Active threats, including denial-of-service attack, spoofing, man in the middle, Address Resolution Protocol (ARP) poisoning, smurf attack, buffer overflow, heap overflow, format string attack, Structured Query Language (SQL) injection and cyber attack.
* Cloud computing security threats

P2 - **Explain** the principles of information security when protecting the IT systems of organisations.

* Principles of the CIA model
* Policies and procedures
* Firewall and Intrusion detection systems.
* File/folder access controls
* Deliberate or accidental loss of information.
* The need to protect intellectual property from theft or malicious damage, e.g. personal information, bank account details, employment details.

P3 - **Explain** why organisations must adhere to legal requirements when considering IT system security.

* DPA
* Computer misuse
* Fraud act
* Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations
* Copyright, Designs and Patents Act

P4 - **Explain** the principles and uses of cryptography to secure and protect data.

* Cryptographic principles - The principles and uses of encryption, including digital rights management (DRM); password storing and salts; obfuscation and steganography; secure transactions; two-factor authentication; file, folder, disk encryption; encryption of communication data, e.g. police, mobile phone.
* Legal and ethical issues
* Computational hardness assumption.
* Key cryptography methods, e.g.:
  + shift ciphers, one-time pads, hash functions (e.g. MD4, MD5, SHA-2 SHA-3), block ciphers, stream ciphers
  + cryptographic primitives, e.g. pseudo random functions, one-way functions
  + cryptographic salts and their use in storing passwords
  + encryption algorithms, e.g. RSA, DES, 3DES
  + mathematical principles, integer factorisation, prediction of prime numbers
* The types and application of cryptography, including:
  + symmetric key encryption
  + public key encryption
  + key exchanges (Diffe-Hellman)
  + digital certificates (including certificate authorities)
  + HTTPS protocol
  + virtual private networks (VPNs)
  + Generic Routing Encapsulation (GRE) tunnels
  + encryption of data on Wi-Fi networks.

M1 - **Assess** the impact that IT security threats can have on organisations’ IT systems and business whilst taking account of the principles of information security and legal requirements.

* Loss of service
* Loss of reputation
* Legal impact
* Forensic research.

M2 - **Analyse** how the principles and uses of cryptography impact on the security and protection of data.

* Digital Rights
* Password storage
* Financial transactions
* File, folder and disk encryption
* Mobile communication
* Legal and ethical issues
* Applications of cryptography within the company

D1 - **Evaluate** the effectiveness of the techniques used to protect organisations from security threats whilst taking account of the principles of information security and legal requirements.

* Summary of dangers faced in the context of the scenario
* How dangers they can be mitigated against
* How successful are the steps taken to mitigate threats
* Legal implications of failing to protect data in context of the scenario

**References**

* Full list of sources you have used