Exercise 1
Introduction

Task 1: Security vulnerabilities (Points: 9)
Security vulnerabilities observed in the image can contribute to the compromise of confidentiality, Integrity and availability security objectives of the organization or office.

Confidentiality

1. It can be observed from the image that a “Strictly confidential” document with information clearly visible on it being left in the tray of the scanner without any restrictions to be accessed by an adversary or a non-adversary. An adversary can have access and sniff the confidential data and make meaning out of it even if it's encrypted. The document could be any sort of information such as authorization data such as username or password, private data that can be used for further escalating system access privileges.
2. It is assumed from the image that an adversary can access and read data off the exposed data storage medium such as CD/DVD labeled “Privat” which is left in the open floor and can be easily accessed. Also, the same medium labeled “save” is left on the desk in the bottom-left room, accessed data read or copied from these mediums by an adversary which compromises the confidential security objectives.
3. It can be observed the listing of valuable confidential accounting data on a monitor by a window where onlookers or an adversary can access and read the information on the screen. This could be valuable information to the organization and access to this information by an adversary can be used for a negative effect on the organization.

Integrity

1. The data on the CD/DVD storage mediums observed labeled “Privat” and “save” if rewritable can be changed by an adversary to make the data less meaningful or include integrity violation security data to gain a positive advantage.
2. The observed computer with the valuable accounting data when accessed by an adversary can easily manipulate the figures. For example, if this is a list of employee salary then the adversary if included can change his salary figure hence influencing compromise of the integrity violation.
3. It can also be observed a piece of information “ABBA NEIN OKOK” on a paper exposed under the keyboard which is assumed to be the password of the user, an adversary can access and use this password to authenticate and get access to the computer and system to change or damage and records or configuration to compromise the integrity of the data.
4. It was observed that all doors and for both offices are open and does not exist any adversary entry restrictions features as such, an adversary can access for example the servers, create a backdoor or manipulate any information stored on them.

Availability

1. The observed lighted cigarette in the server room may trigger a fire incident or smoke detection system which may permanently destroy the servers along with its data residing on them or cause a temporary inaccessibility of service to the authorized entities.
2. An adversary can change configurations or destroy all devices observed in the image such as the scanner, computers, printers, laptop etc from responding to a request for a service by a legitimate entity hence can compromise the availability of the system.

Task 2: Security vulnerabilities in the real (Points: 3)

With the observed exposed printers and scanners and the secret information that compromises the integrity and confidentiality of the organization as such, a real example of attack as a result of this was reported by Reuters.

Reuters reported that disabled printers that confirm SWIFT network transfers during attacks on numerous Indian and Bangladesh banks. The attacks infected the system with malware that disabled the SWIFT printer. Bank officials initially assumed there was simply a printer problem. The attackers stole the money from Bangladesh Bank's account at the Federal Reserve using fraud orders on SWIFT. The money sent to accounts at a Manila Banking Corp then disappeared into a Philippines-based casino (Reuters, 2016).

Also, the observed freely accessible CD/DVD storage mediums, server room and computers in the image collectively contribute to compromises of all security objectives(C.I.A) had a similar effect on real attack such as reports from the medical sector.

BBC news reported that Brighton and Sussex University Hospital was fined £325,000 over the theft of thousands of patient's data. The sensitive information, which included medical results, were reportedly put up for sale on ebay. The thief accessed the sensitive data by stealing hard drives that were supposed to have been destroyed (bbc, 2012).

Task 3: Security Goals (Points: 3)

1. **Confidentiality**: It is a service that assures keeping information or data hidden from unauthorized access either over a network communication or physical storage of information. Attacks such as Data Spoofing (Unauthorized access to data) and Traffic analysis(Intercept and encipherment) can be used to compromise this security objective.
2. **Integrity**: It is a service that assures that information communicated over a network or stored locally can only be changed by authorized entity(s) and through authorized mechanisms. Attacks such as power surges can create unwanted alterations in the data as well Man-in-the-middle attacks such as Replaying(resending an obtained data at a later time) and modification(Sending an altered information to a receiver) can be used to compromise this security objective.
3. **Availability**: This is a service that assures that information created and stored needs to be available to authorized entity(s) when being requested for . Attacks such as Denial of Service (Sending requests to increase load, delay response and crash server) can threaten this security objective.

Task 4: Symmetric methods (Points: 3)

The main problem with symmetric methods is the key exchange between communicating entities and the scalability of adding new users or entities and keys, which is expensive and complicated..

A possible solution is to use a method that allows for easy key access and scalability such like the asymmetric method where an intended receiver of communication creates two sets of keys: one published for the public to encrypt or encode data to be sent to the owner of the key and a private key to be used to retrieve the content of the aforementioned encryption.

Also, a hybrid of encryption methods can be used such as using the public method such as deffie-hellman to exchange symmetric keys between communicating entities and further using the keys to communicate symmetrically.

Task 5: Symmetric and asymmetric encryption schemes (Points: 3)

In Symmetric encryption scheme, it involves the use of a single key where both the sender and receiver know and share the secret key that will be used by both communicating entities to encrypt (change of message to unreadable format) and decrypt(convert unreadable data back to information) data.

Whiles, in Asymmetric encryption scheme, each communicating entities must have two keys, a private key and a public key where the private is kept secret and will be used for decrypting an encrypted data whiles the public key will be made available which then will be used to encrypt data for the intended receiver to use his private key to decrypt.

For a distributed system to be convenient, considering the speed or performance in such a system then the symmetric encryption scheme will be more suitable for implementation as the same key is used for both encryption and decryption. For example such implementations are often used in data storage in banking systems.

For the convenience of security as a priority over speed then Asymmetric encryption scheme will be implemented in such a system as use of a dual-key encryption scheme will be much beneficial to this goal. An example of such use preference is exhibited in the implementation of Digital Signature.

Task 6: RSA vs. ECC (Points: 3)

There are several decisions that will influence our decision to choose such as:

1. Although computationally expensive, there are known algorithms for breaking RSA based on modular arithmetic. However, there does not yet exist a mathematical algorithm for breaking an ECC system thus is more secure.

2. Encryption and decryption using RSA is computationally more expensive than use of ECC which consumes lower CPU and memory resources when processing.

3. The small keys size exhibited with ECC has a great advantage as such can increase speed of the encryption and decryption process such as in the implementation of an SSL handshake.RSA though secure has a large key size with minimum of 512 bits.

Given the reasons aforementioned, we will choose ECC,which is more ideal over RSA as a preferred cryptographic method.