LO1 - ANSWER KEYS:

SELF CHECK 1:

1. **A user account**
2. **A standard user account**
3. **An administrator account**
4. **A guest account**
5. **User profile**
6. **Authentication**
7. **The authorization process**
8. **Username** and **Password** method.
9. The standard account can help protect your computer by preventing users from making changes that affect everyone who uses the computer, such as deleting files that are required for the computer to work. We recommend creating a standard account for each user.

   When you are logged on to Windows with a standard account, you can do almost anything that you can do with an administrator account, but if you want to do something that affects other users of the computer, such as installing software or changing security settings, Windows might ask you to provide a password for an administrator account.

10. Authentication methods used to authenticate users
    - ***Username with static passwords*** - the password stays the same until changed by the user at some time
    - ***Usernames with dynamic passwords*** - the password is constantly changed by a password generator synchronized with the user and system.
    - ***Other challenge response systems*** - this may involve PINs, questions to the user requiring various answers or actions
    - ***Certificate Based*** - this requires the user to have an electronic certificate or token. This may also need to be digitally signed by a trusted authority.
    - ***Physical devices*** - these include the use of smartcards and biometrics. Generally the entire authentication process occurs on
11. **User Account Control**

LO1 - ANSWER KEYS:

12. When your permission or password is needed to complete a task, UAC will notify you with one of four different types of dialog boxes.

- A setting or feature that is part of Windows needs your permission to start.
- A program that is not part of Windows needs your permission to start.
- A program with an unknown publisher needs your permission to start.
- You have been blocked by your system administrator from running this program.

13. The UAC settings and the potential impact of each setting to the security of your computer.

Setting	Security Impact
Always Notify	• This is the most secure setting. • When you are notified, you should carefully read the contents of each dialog box before allowing changes to be made to your computer.
Notify me only when programs try to make changes to my computer	• It's usually safe to allow changes to be made to Windows settings without you being notified. However, certain programs that come with Windows can have commands or data passed to them, and malicious software can take advantage of this by using these programs to install files or change settings on your computer. You should always be careful about which programs you allow to run on your computer.
Notify me only when programs try to make changes to my computer (do not dim my desktop)	• This setting is the same as "Notify only when programs try to make changes to my computer," but you are not notified on the secure desktop. • Because the UAC dialog box isn't on the secure desktop with this setting, other programs might be able to interfere with the dialog's visual appearance. This is a small security risk if you already have a malicious program running on your computer.
Never Notify	• This is the least secure setting. When you set UAC to never notify, you open up your computer to potential security risks. • If you set UAC to never notify, you should be careful about which programs you run, because they will have the same access to the computer as you do. This includes reading and making changes to protected system areas, your personal data, saved files, and anything else stored on the computer. Programs will also be able to communicate and transfer information to and from anything your computer connects with, including the Internet.

14. **Security Identifiers** (**SIDs**) and **Windows privileges**

15. **Admin Approval Mode**

LO1 - ANSWER KEYS:

SELF CHECK 2:

1. **The organisation's policies**
2. **Administrators**
3. Some basic parameters covered by most operating systems to consider when setting up user account options:
    - ***Password requirements*** - whether a password is required, minimum length, complexity, needs to be changed at intervals, etc
    - ***Account lock out settings*** - disabling accounts that have made a number of bad logon attempts
    - ***Access hours*** - the standard days and time that users will be permitted to access the network
    - ***Account expiry dates*** - date when account will be disabled
    - ***Logon restrictions*** - accounts can only be used at specified locations or workstations.
    - ***Home directory information*** - a home directory is a folder that usually has the name of the user and the user has full permissions over.
    - ***Logon scripts*** - these perform specific tasks or run specific programs when the user logs on
4. **Access permissions**
5. **Permissions**
6. The user account or group can be set with the following type of permissions
    - No access at all to files and directories
    - Read only.
    - Modify where the contents of files and directories may be accesses but changed or added to but not deleted
    - Full Control or Supervisory where files and directories can be view modified and deleted.
7. **Rights (or privileges)**
8. To manage user accounts appropriately administrators should
    - Regularly review organisational policies and procedures to be aware of requirements and address any organisational or network changes
    - Conduct regular checks to ensure the change management procedures are working for new, changed and deleted users
    - Review and investigate current work practices regarding user network access
    - Conduct information and training sessions for network users to reinforce appropriate practices and organisational policy
    - Conduct regular audits of network access—verifying current users and
9. **Policy and procedures**

LO1 - ANSWER KEYS:

SELF CHECK 3:

1. **Security requirements.**
2. **Incorrect credentials**
3. “your account has time restrictions that prevent you from logging on at this time. Please try again later.”
4. Changing user passwords accomplishes two things:
    - If attackers are attempting to guess a password, it forces them to restart their efforts. If users never change their passwords, attackers would be able to guess them eventually.
    - If an attacker has guessed a user’s password, changing the password prevents the attacker from using these credentials in the future.
5. **Change their password automatically.**
6. **Disable user accounts**

LO1 - ANSWER KEYS:

SELF CHECK 4:

1. **A *password***
2. ***Letters***, ***numbers***, ***symbols***, and ***spaces***.
3. ***Strong password*.**
4. ***Passphrases***
5. **It's difficult to guess or crack.**
6. Compare a strong **password and** a strong **passphrase**

A strong password:	A strong passphrase:
• Is at least eight characters long. • Does not contain your user name, real name, or company name. • Does not contain a complete word. • Is significantly different from previous passwords.	• Is 20 to 30 characters long. • Is a series of words that create a phrase. • Does not contain common phrases found in literature or music. • Does not contain words found in the dictionary. • Does not contain your user name, real name, or company name. • Is different from previous passphrases.

7. The four categories of characters Strong passwords and passphrases contain:
   - Uppercase letters
   - Lowercase letters
   - Numbers
   - Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces
8. A **password policy**
9. Password policies include advice on proper password management such as:
   - never share a computer account
   - never use the same password for more than one account
   - never tell a password to anyone, including people who claim to be from customer service or security
   - never write down a password
   - never communicate a password by telephone, e-mail or instant messaging
   - being careful to log off before leaving a computer unattended
   - changing passwords whenever there is suspicion they may have been compromised
   - operating system password and application passwords are different
   - password should be alpha-numeric
10. **Minimum password age**
11. **Maximum Password Age**
12. **Password Complexity Requirements**

LO1 - ANSWER KEYS:

SELF CHECK 5:

1. **Authentication**
2. Windows supports a variety of authentication techniques, including
   - The traditional user name and password,
   - Smart cards, and
   - Third-party authentication components.
3. **The smart card**
4. **Multifactor authentication**.
5. **Biometrics**
6. **Auditing for logon events**
7. Windows 7 (and earlier versions of Windows) provides two separate authentication auditing policies:
   - **Audit Logon Events** This policy audits authentication attempts for local resources, such as a user logging on locally, elevating privileges using a UAC prompt, or connecting over the network (including connecting using Remote Desktop or connecting to a shared folder). All authentication attempts will be audited, regardless of whether the authentication attempt uses a domain account or a local user account.
   - **Audit Account Logon Events** This policy audits domain authentications. No matter which computer the user authenticates to, these events appear only on the domain controller that handled the authentication request. Typically, you do not need to enable auditing of account logon events when troubleshooting authentication issues on computers running Windows 7. However, successful auditing of these events is enabled for domain controllers by default.