Question 1

a.

- If the control would reduce risk more than needed, then a less expensive alternative could be used.
- If the control would cost more than the risk reduction provided, then an alternative should be used.
- If a control does not reduce the risk sufficiently, then either more or different controls should be used.
- If the control provides sufficient risk reduction and is the most cost effective, then use it.

b. The security officer need to check that :

- The implementation costs and resources used stay within identified bounds.
- The controls are correctly implemented as specified in the plan, in order that the identified reduction in risk level is achieved.
- The controls are operated and administered as needed.

c.

1. What assets do we need to protect?
   Asset Identification - Identifying and interviewing personnel to identify the key assets (things such as hardware, software, documents, people that need to be protected).
2. How are those assets threatened?
   Threat identification - Identifying the potential threats to assets such as confidentiality, availability, integrity, authenticity, accountability and reliability
   Threat source -
3. What can be done to counter those threats?
   Risk treatment alternatives - There are five broad alternatives to counter the identified risks such as risk acceptance, risk avoidance, risk transfer, reduce consequences and reduce likelihood.

d. Organizational security policy is a single large document or a set of related documents that describe what are the objectives and strategies as well as the process to achieve them. 3 topics that typically need to be addressed are the scope and purpose of the policy, IT security requirements and assignment of responsibility.

Question 2

a. **Logical security** - It is a type of security that protects computer data from communication and software-based systems.

   Physical security - It is a type of security that protects the data/information and personnel that use, maintain and operate the information system.

   Premises security - It is a type of security that protects property and personnel within the whole building, facility and area.

b. **Prevent damage to the physical infrastructure** such as information system hardware, physical facility, supporting facilities and personnel.

   Prevent misuse of the physical infrastructure that will cause misuse of damage or damage of the protected information. The misuse can be categorized as accidental or malicious. The example of misuse includes vandalism, theft of equipment, theft of copying and unauthorized entry.

c. -
   i. IPsec can secure the branch office connectivity over the internet. For example, an organization can build a secure private virtual network over the network.
   ii. IPsec can establish extranet and intranet connectivity with partners. For example, IPsec can be used to establish secure communications with other companies such as supplier/vendor companies.
   iii. IPsec can secure remote access over the Internet. For example, the staff can gain secure access to a company's network over the Internet regardless of the location and time.

d. HTTPS is the secure version of HTTP protocol in which it uses authentication and encryption to secure data.

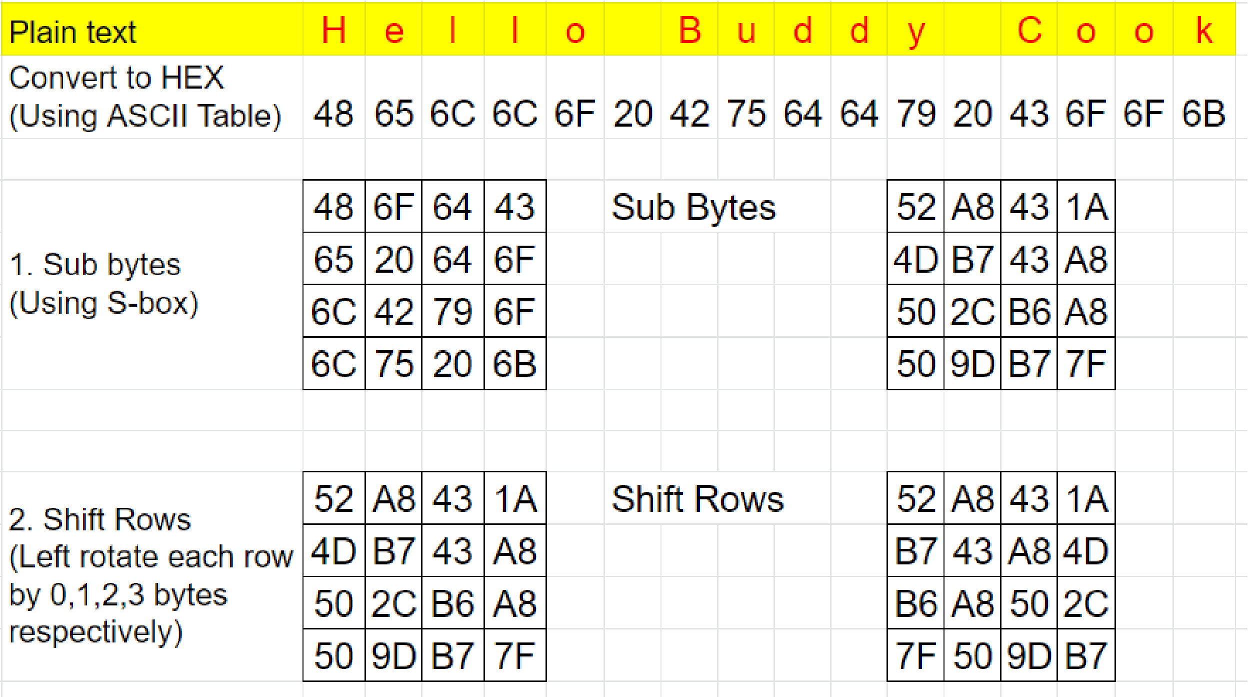
   5 elements of the communication which are encrypted when HTTPS is used are:
   i. URL
   ii. Plain text data
   iii. Binary data
   iv. Header
   v. Cookies

Question 3

a. -

- Brute force
- Timing attacks
- Mathematical attacks
- Electronic monitoring

b. (i)



Plain text	H	e	l	l	o		B	u	d	d	y		C	o	o	k
Convert to HEX (Using ASCII Table)	48	65	6C	6C	6F	20	42	75	64	64	79	20	43	6F	6F	6B
1. Sub bytes (Using S-box)	48	6F	64	43		Sub Bytes					52	A8	43	1A		
	65	20	64	6F							4D	B7	43	A8		
	6C	42	79	6F							50	2C	B6	A8		
	6C	75	20	6B							50	9D	B7	7F		
2. Shift Rows (Left rotate each row by 0,1,2,3 bytes respectively)	52	A8	43	1A		Shift Rows					52	A8	43	1A		
	4D	B7	43	A8							B7	43	A8	4D		
	50	2C	B6	A8							B6	A8	50	2C		
	50	9D	B7	7F							7F	50	9D	B7		

(ii)

1. {01.EB}

   EB = 11101011

2. {01.93}
   93 = 10010011

3. {02.C7}
   C7 = 11000111
   {C7} . {02}
   = 11000111 << 1
   = 10001110 XOR 00011011
   = 10010101

4. {03.20}
   20 = 00100000
   = {03} . {20}
   = {10 XOR 01} . {00100000}
   = {00100000 . 10} XOR {00100000}
   = 01000000 XOR 00100000
   = 01100000

Answer :
= {01.EB} XOR {01.93} XOR {02.C7} XOR {03.20}
= 11101011 XOR 10010011 XOR 10010101 XOR 01100000
= 10001101
= 8D

(iii)
F4 = 11110100
FC = 11111100
F4 XOR FC = 11110100 XOR 11111100 = 00001000 (**08** in hex)

8D = 10001101
91 = 10010001
8D XOR 91 = 10001101 XOR 10010001 = 00011100 (**1C** in hex)

06 = 00000110
E4 = 11100100
06 XOR E4 = 00000110 XOR 11100100 = 11100010 (**E2** in hex)

7D = 01111101
A2 = 10100010
7D XOR A2 = 01111101 XOR 10100010 = 11011111 (**DF** in hex)

Final answer:

08	1C	E2	DF

Question 4

a. The salt can **prevent duplicate passwords** from existing in the same password file. This is because if the user enters the same password which conflicts with another user, each of those passwords will be assigned a different salt value to make the hashed password of these 2 users totally different. Hence, it prevents the password duplication from existing in the same password file.

   The salt can **increase the difficulty level of offline dictionary attacks.** To illustrate, for a salt value of length n bits, it will increase the number of possible passwords by a factor of 2n, thus increasing the difficulty for an attacker to guess the password using dictionary attacks.

b. An access right describes the way a subject may access an object. There are 6 access rights which includes:
   - Read - The user can view the information such as file, selected record of a file, selected fields within a record. Moreover, read access also includes the ability to print and copy.
   - Write - The user can add, modify or delete in the system resource. Write access includes read access.
   - Execute - The user may execute specified programs
   - Delete - The user can delete certain system resources such as files or records.
   - Create - The user can create new files, records or fields
   - Search - The user may list the files in a directory or otherwise search the directory

c.

- **Exploiting multiple password use** - This can make the attacks become easier and effective as the user uses the same or similar password for a different network device.

    - Countermeasure - Implement a policy to forbid the same or similar password being used on particular network devices.
- **Specific account attacks** - In this attack, the attacker will target a specific account and submit the password guesses until the correct password has been identified.
    - Countermeasure - Use the account lockout mechanism such as if the password attempt has exceeded 5 times, the account will be automatically blocked and restricted for access. In this case, the user will only be able to regain access by calling the customer support to unblock the system.