

- 1) Can you provide examples of security controls within the three broad categories (technical, operational, and managerial), and explain their respective roles in cybersecurity?

Answer:

- **Technical** security is something that is implemented as software, hardware or firmware. Examples could include firewalls, antivirus and OS access controls.
- **Operational** security could be implemented primarily by people rather than systems. For example, security guards and training programs are operational controls.
- **Managerial** control gives oversight of the information system. This could include risk identification or a tool allowing the evaluation and selection of other security controls.

- 2) How do physical, deterrent, and compensating controls contribute to overall cybersecurity, and in what situations are they typically used?

Answer:

- **Deterrent** control may not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion. This could include signs and warnings of legal penalties.
- **Physical** controls such as alarms, gateways, locks, lighting, security cameras and guards that deter and detect access to premises and hardware are often classified separately.
- **Compensating** controls serve as a substitute for principal control, as recommended by a security standard, and affords the same or better level of protection. However, it uses a different methodology or technology.