

Security answers are marked on precision: a threat is not a vulnerability, and a control is not a policy. Using the right word is usually the difference between a described answer and a scoring one.

Core principles

- Confidentiality** – ensuring information is accessible only to those authorised to have it
- Integrity and use** – ensuring information has not been altered, accidentally or maliciously, between creation and use
- Availability** – ensuring authorised users can access information and services when they need them
- Authentication** – establishing that a user is who they claim to be
- Authorisation** – determining what an authenticated user is permitted to do
- Non-repudiation** an action – assurance that a party cannot deny having sent a message or performed an action
- Least privilege** more – granting each user or process only the access its task requires, and no more
- Defence in depth** system – layering independent controls so that the failure of one does not expose the system

Threats and vulnerabilities

- Threat** – a potential cause of harm to a system – an actor, an event or a circumstance
- Vulnerability** – a weakness in a system that a threat could exploit; a vulnerability with no threat is not yet a risk
- Risk** – the combination of the likelihood a threat exploits a vulnerability and the impact if it does
- Attack surface** data – the sum of the points at which an unauthorised user could try to enter or extract data
- Malware** – software written to damage a system, steal data or gain unauthorised access
- Ransomware** – malware that encrypts a victim’s data and demands payment for the key
- Social engineering** – manipulating people into revealing information or taking actions that compromise security, bypassing technical controls entirely
- Phishing** malware – a message impersonating a trusted sender, designed to obtain credentials or deliver malware
- SQL injection** SQL – supplying input that a program inserts into a database query unchecked, so the input is executed as code
- Zero-day vulnerability** – a vulnerability unknown to the vendor, for which no patch yet exists

Controls

- Firewall** – a control that inspects traffic crossing a network boundary and permits or blocks it against a rule set
- Encryption** – transforming data with a key so that it is unreadable without the corresponding key
- Hashing** – producing a fixed-length digest from data by a one-way function; unlike encryption it cannot be reversed, which is why it suits password storage
- Digital signature** origin and integrity – a hash of a message encrypted with the sender’s private key, which proves origin and integrity
- Multifactor authentication** – requiring two or more independent kinds of evidence: something you know, something you have, something you are
- Patch management** vulnerabilities are closed – the process of tracking, testing and applying vendor fixes so known vulnerabilities are closed
- Intrusion detection system** – a system that monitors traffic or hosts for signs of an attack and raises an alert; it detects rather than blocks
- Air gap** – physically isolating a system from unsecured networks so no network path exists to it
- Operations and response**
- Incident response** recovery and lessons learned – the planned process of preparation, identification, containment, eradication, recovery and lessons learned
- Penetration testing** – authorised simulated attack to find exploitable weaknesses before an attacker does
- Backup (3-2-1 rule)** – three copies of data on two kinds of media with one held off-site – the control that makes ransomware survivable
- Security policy** mechanism that enforces it – a documented statement of what an organisation requires; a control is the mechanism that enforces it