Security Acronyms

Acronym	Stands for	What it is
	01 THE FOUNDATIONS	
CIA	Confidentiality, Integrity, and Availability	The triad every security policy is built on: information is disclosed only to those authorised, is not altered without authorisation, and is there when it is needed.
AAA	Authentication, Authorization, and Accounting	Who are you, what may you do, and what did you actually do. The three questions every access control system answers.
PII	Personally Identifiable Information	Any data that identifies a specific person, directly or indirectly — name, government ID number, address, telephone, email.
PHI	Protected Health Information	Health information tied to an individual and protected under HIPAA: medical records and anything else that could identify the patient.
AUP	Acceptable Use Policy	The rules governing what users may do with the organisation's networks, systems and resources — and the document you point at when they do not.
ACP	Access Control Policy	Which people may reach which data, systems and places, and under what conditions.
GDPR	General Data Protection Regulation	EU law giving individuals rights over their own data — access, rectification, erasure, restriction, portability and objection.
	02 IDENTITY AND ACCESS	
IAM	Identity and Access Management	The framework for creating, maintaining and removing identities, and deciding what each one may reach.
SSO	Single Sign-On	Authenticate once, reach many applications without entering credentials again.
SAML	Security Assertion Markup Language	The open standard an identity provider and a service provider use to exchange authentication and authorisation. What makes SSO work between organisations.
MFA	Multi-Factor Authentication	Two or more of: something you know, something you have, something you are.
PAM	Privileged Access Management	Controlling, rotating and monitoring the credentials that matter most — the accounts that can undo everything else.
RADIUS	Remote Authentication Dial-In User Service	Centralised AAA for network access. Used by service providers and enterprises to decide who gets on and to record what they did.
TACACS+	Terminal Access Controller Access-Control System Plus	Cisco's AAA protocol for administering network devices. Where RADIUS is for network access, this is for logging in to the router itself.
LDAP	Lightweight Directory Access Protocol	Vendor-neutral access to directory services holding users, groups and devices in a hierarchy. Used to authenticate and to look up who is who.
EAP	Extensible Authentication Protocol	The authentication framework wireless and point-to-point links run inside. A framework, not one method — PEAP, EAP-TLS and the rest are its methods.
NAC	Network Access Control	Only authorised and compliant devices get on the network. The enforcement half of a zero-trust posture.
GPO	Group Policy Object	Centralised Windows configuration — security settings, software, user environment — pushed from Active Directory.
	03 ACCESS CONTROL MODELS	
ACL	Access Control List	Per-object permissions: who may do what to this file, directory or interface.
RBAC	Role-Based Access Control	Permissions attach to a job role; users inherit whatever their role carries. The model most organisations actually run.
ABAC	Attribute-Based Access Control	Decisions from attributes of the user, the resource and the context — including time of day and location. The most expressive, and the hardest to audit.
RuBAC	Rule-Based Access Control	Predefined rules decide, regardless of who is asking. A firewall rule set is the everyday example.
MAC	Mandatory Access Control	A central authority sets the policy and users cannot change it — not even on data they created. The model used where classification is law.
DAC	Discretionary Access Control	The owner of the resource decides who else may have it. Flexible, and the reason data spreads.
	04 CRYPTOGRAPHY AND PKI	
PKI	Public Key Infrastructure	The policies, technology and procedures for creating, distributing, storing and revoking digital certificates — and so for proving who anything is.
CA	Certificate Authority	The trusted entity that issues and manages certificates. Trust in the whole system reduces to trust in this.

Acronym	Stands for	What it is
RA	Registration Authority	Verifies the identity behind a request before the CA will issue. The intermediary between applicant and authority.
CSR	Certificate Signing Request	The application itself: the public key to be certified, plus identifying detail such as the domain name.
CRL	Certificate Revocation List	A list published by the CA of certificates revoked before their expiry date.
OCSP	Online Certificate Status Protocol	Checks one certificate's revocation status in real time, rather than downloading and searching a whole CRL.
MD5	Message Digest Algorithm 5	128-bit hash from 1991. Cryptographically broken — still seen as a file checksum, and should be nowhere else.
SHA	Secure Hash Algorithm	The family that replaced it. SHA-2 and SHA-3 are current; SHA-1 is deprecated for signatures.
FDE	Full Disk Encryption	Everything on the drive encrypted, so pulling the disk and reading it elsewhere yields nothing.
TPM	Trusted Platform Module	A chip on the board holding keys, enabling secure boot and sealing data to that specific machine.
HSM	Hardware Security Module	A dedicated tamper-resistant device for key storage and cryptographic operations. What a TPM is for one machine, this is for an organisation.
05 NETWORK PROTOCOLS AND SERVICES		
DNS	Domain Name System	Translates names people can remember into the addresses devices actually use.
DHCP	Dynamic Host Configuration Protocol	Hands out addresses and options automatically as devices connect.
NAT	Network Address Translation	Maps many private addresses to one public address on the way out. Conserves addresses, and hides the inside as a side effect.
ARP	Address Resolution Protocol	Finds the MAC address behind an IP address on the local segment. No authentication at all, which is why ARP spoofing works.
VLAN	Virtual Local Area Network	A broadcast domain defined in software rather than in cabling, so hosts can be grouped whatever switch they sit on.
SNMP	Simple Network Management Protocol	Collects information from managed devices and changes their behaviour. Use version 3 — v1 and v2c send the community string in clear text.
HTTP	HyperText Transfer Protocol	Moves hypermedia documents between a browser and a server. Everything it carries is in the clear.
HTTPS	HyperText Transfer Protocol Secure	The same protocol inside TLS, so the exchange is private and cannot be tampered with in transit.
SSH	Secure Shell	Encrypted remote administration over an untrusted network. The reason telnet should not be running anywhere.
IPSec	Internet Protocol Security	A suite that authenticates and encrypts IP packets. The usual basis of a site-to-site VPN.
VPN	Virtual Private Network	A secure, encrypted connection across a network you do not control.
SQL	Structured Query Language	The standard language for storing and retrieving data in relational databases — and the target of injection attacks.
CRC	Cyclic Redundancy Check	Detects accidental corruption in transmission or storage. An integrity check, not a security control — it stops mistakes, not attackers.
06 EMAIL AUTHENTICATION		
SPF	Sender Policy Framework	A DNS TXT record naming which mail servers may send for your domain. The receiver checks it and rejects what does not match.
DKIM	DomainKeys Identified Mail	A digital signature added to the message headers, which the receiving server verifies against a published key.
DMARC	Domain-based Message Authentication, Reporting, and Conformance	Ties the other two together: says what a receiver should do when they fail, and sends you reports on who is sending as you.
07 SECURITY CONTROLS AND ARCHITECTURE		
IDS	Intrusion Detection System	Watches traffic for attacks and raises an alert. Out of band — it sees, it does not stop.
IPS	Intrusion Prevention System	The same detection, placed in line, so it can block or reject the traffic rather than only reporting it.
WAF	Web Application Firewall	Filters HTTP and HTTPS to a web application, blocking SQL injection, cross-site scripting and file-inclusion attacks.

Acronym	Stands for	What it is
DLP	Data Loss Prevention	Monitors and controls data transfers so confidential information does not leave, by accident or otherwise.
FIM	File Integrity Monitoring	Alerts when files or system configurations change unexpectedly — the tripwire on everything that should be static.
MDM	Mobile Device Management	Software that monitors, manages and secures employees' mobile devices across multiple carriers and operating systems.
CASB	Cloud Access Security Broker	The policy enforcement point sitting between users and cloud services, applying encryption, access control and DLP to what passes.
SASE	Secure Access Service Edge	WAN capability and a full security stack delivered together from the cloud — FWaaS, SWG, CASB and ZTNA, with access granted by identity.
BYOD	Bring Your Own Device	Employees use their own laptops and phones for work. Cheaper, more productive, and much harder to control.
CYOD	Choose Your Own Device	Employees choose from an approved list. The compromise: some choice, and devices you can still hold to a standard.
08 THREATS AND ATTACKS		
APT	Advanced Persistent Threat	A skilled, well-funded intruder who gets in and stays undetected for a long time — often state-sponsored, and there to steal, watch or disrupt.
DoS	Denial of Service	Overwhelm a machine or service until the people who need it cannot reach it.
DDoS	Distributed Denial of Service	The same attack from many compromised hosts at once, so blocking a single source address achieves nothing.
C2	Command and Control	The infrastructure an attacker uses to issue orders to compromised hosts and collect what they steal. Also written C&C.
IoC	Indicators of Compromise	The forensic traces that say a breach has already happened — odd traffic, changed files, impossible logins, known signatures.
CVE	Common Vulnerabilities and Exposures	The standard identifier for one known vulnerability, so every tool and vendor can mean the same thing by it.
CVSS	Common Vulnerability Scoring System	The severity score attached to a CVE, so remediation can be prioritised consistently.
OSINT	Open-Source Intelligence	Intelligence assembled from publicly available sources — sites, social media, forums, public records. Used by both sides.
09 MONITORING AND OPERATIONS		
SIEM	Security Information and Event Management	Collects, aggregates and correlates logs from applications, devices, servers and users in real time, so one platform shows the whole picture.
SOAR	Security Orchestration, Automation, and Response	Automates what happens next: integrates the tools, runs the response playbook, removes the repetitive work.
UBA	User Behavior Analytics	Baselines normal behaviour, then flags the deviations that suggest a compromised account, an insider, or data leaving.
SCAP	Security Content Automation Protocol	A standard framework for automating vulnerability assessment, security measurement and compliance checking.
CERT	Computer Emergency Response Team	The people who handle the incident — contain it, limit the damage, get things back.
10 RISK, CONTINUITY AND GOVERNANCE		
AV	Asset Value	What the asset is worth. The starting number for every calculation below.
EF	Exposure Factor	The proportion of that value a single incident would destroy, as a percentage.
SLE	Single Loss Expectancy	**AV × EF.** What one occurrence costs you.
ARO	Annualized Rate of Occurrence	How many times a year the incident is expected to happen.
ALE	Annualized Loss Expectancy	**SLE × ARO.** The yearly figure — and the one that decides whether the control is worth buying.
SPF	Single Point of Failure	The one component whose failure stops everything. Nothing to do with the other SPF on this sheet.
BCP	Business Continuity Plan	How the business keeps operating *during* the event.

Acronym	Stands for	What it is
DRP	**Disaster Recovery Plan**	How the systems and data come back *afterwards*. A subset of the BCP, not a synonym for it.
11 AGREEMENTS AND CONTRACTS		
SLA	**Service Level Agreement**	Binding. Defines the service levels, the metrics, and the remedy when they are missed.
MSA	**Master Services Agreement**	The framework terms governing a whole relationship, so later projects do not renegotiate them.
SOW	**Statement of Work**	The specifics for one project: tasks, deliverables, timeline, standards, acceptance criteria.
MOU	**Memorandum of Understanding**	Intent and mutual expectations. Signals that a contract is coming; not necessarily binding itself.
MOA	**Memorandum of Agreement**	Terms, roles and commitments between the parties, set out formally.
BPA	**Blanket Purchase Agreement**	A standing arrangement for repeated purchases, so each one does not need its own contract. Common in government procurement.
NDA	**Non-Disclosure Agreement**	Binding confidentiality over what one party shares with the other.
12 PLATFORMS, CLOUD AND OPERATIONAL TECHNOLOGY		
IaaS	**Infrastructure as a Service**	You rent servers, storage and networking. The provider owns the hardware and the data centre; you own the operating system upward.
PaaS	**Platform as a Service**	You rent the platform — runtime, database, middleware. The provider owns up to that; you own the application and the data.
SaaS	**Software as a Service**	You rent the finished application. The provider owns almost everything; you own user access, your data and the configuration.
IaC	**Infrastructure as Code**	Infrastructure defined in machine-readable files rather than clicked into existence — so it is version-controlled, reviewable and can be rolled back.
SDN	**Software-Defined Networking**	A controller programs the network through APIs instead of configuring boxes one at a time.
IoT	**Internet of Things**	Everyday objects with sensors, software and connectivity, collecting and exchanging data.
ICS	**Industrial Control System**	The systems running industrial processes — manufacturing, handling, production, distribution. Covers SCADA, DCS and PLCs.
SCADA	**Supervisory Control and Data Acquisition**	The supervisory layer of an ICS: computers, networked data and operator screens monitoring and controlling plant in real time.
RTOS	**Real-Time Operating System**	An operating system that guarantees response times. It switches between tasks fast enough to look simultaneous, though only one executes at a time.
BIOS	**Basic Input/Output System**	Firmware on the motherboard that initialises the hardware at power-on, before any operating system exists.
SDLC	**System/Software Development Life Cycle**	The structured process a system goes through from requirement to retirement.
13 THE ONES THAT COLLIDE same letters, different meanings — check which one the question is asking about		
SPF	**Sender Policy Framework** *or* **Single Point of Failure**	Both are on this sheet. Email authentication, or the single component whose failure stops everything. Nothing whatever in common.
MAC	**Mandatory Access Control** *or* **Media Access Control** *or* **Message Authentication Code**	An access control model, the hardware address on a NIC, or a keyed integrity check. Three unrelated things, and all three appear in security material.
AV	**Asset Value** *or* **Antivirus**	In risk analysis it is what the asset is worth. Everywhere else it is the endpoint software.
EF	**Exposure Factor** *or* **Expedited Forwarding**	A percentage in risk analysis, or DSCP 46 in QoS. Context is the only clue.
CERT	**Computer Emergency Response Team** *or* **a certificate**	The team, or the file — and the file is properly a cert, lower case.
ACL	**Access Control List**	One term, two objects: a permission list on a file or directory, and a packet filter on a router interface. Related in idea, unrelated in practice.