CISSP Flash Table

- Yashodhan Vivek Mandke

Category	Terminology	Explanation
Number	802.11 standard	A legacy set of wireless LAN standards developed by Working Group 11 of the IEEE LAN/MAN Standards Committee. 802.11 is known for its use of WEP and RC4.
	802.11i standard	One of the replacements for 802.11. 802.11i uses 802.11i standard WPA and AES
A	Acceptable use policy (AUP)	A policy that defines what employees, contractors, and third parties are authorized to do on an organization's IT infrastructure and its assets. AUPs are common for access to IT resources, systems, applications, Internet access, email access
	Access control	A control that monitors the flow of information between a subject and an object. It ensures that Access control only the operations permitted are p
	Access control list (ACL)	A table or list stored by a router to control access to and from a network by helping the device determine whether to forward or drop packets that are entering or exiting it.
	Access creep	The result of employees moving from one position to another within an organization without losing

		the privileges of the old position but gaining additional access in the new position. Thus, over time, employees build up much more access than they should have.
	Access point spoofing	The act of pretending to be a legitimate access point to trick individuals to pass traffic using the fake connection so that it can be captured and analyzed.
	Accountability	The traceability of actions performed on a system Accountability to a specific system entity or user
	Accreditation	Management’s formal acceptance of a system or Accreditation an application.
	ACID test	A test that addresses atomicity, consistency, isolation, and durability. Programmers involved in database management use the ACID test to determine whether a database management system has been properly designed to handle transactions.
	Active fingerprint	An active method of identifying the operating system of a targeted computer or device that involves injecting traffic into the network.
	Address Resolution Protocol (ARP)	A protocol used to map a known IP address to an Address Resolution unknown physical address.
	Ad hoc mode	A mode that makes it possible for an individual computer to communicate directly with other client units, with no access point required. Ad hoc operation is ideal for small networks of

		no more than two to four computers
	Administrative law	A body of regulations, rules, orders, and decisions to carry out regulatory powers, created by administrative agencies.
	Advanced Encryption Standard (AES)	The encryption standard that was originally known Advanced Encryption as Rijndael and serves as the replacement to DES.
	Aggregation	Collection of data from disparate sources.
	Algorithm	A mathematical procedure used for solving a problem. Commonly used in cryptography.
	American Standard Code for Information Interchange (ASCII)	A standard code for transmitting data, consisting of 128 letters, numerals, symbols, and special codes, each of which is represented by a unique binary number. An ASCII word typically is 8 bits of binary data.
	Anomaly detection	A type of intrusion detection that looks at behaviors that are not normal with standard activity. These unusual patterns are identified as suspicious.
	Appender	A virus infection type that places the virus code at the end of the infected file.
	Applet	A small Java program that can be embedded in an HTML page. Applets differ from full-fledged Java applications in that they are not allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, and so on), and they are prohibited from communicating with most

		other computers across a network. An applet can make an Internet connection only to the computer from which the applet was sent.
	Application	A software program designed to perform a specific task or group of tasks, such as word processing, Application communication, or database management.
	Application controls	A category of controls used to verify the accuracy and completeness of records made using manual or automated processes. Controls used for applications include encryption, batch totals, and data input validation controls.
	Application layer	The highest layer of the seven-layer OSI model. The application layer is used as an interface to applications or communications protocols.
	Application programming interface (API)	A set of system-level routines that can be used in an application program for tasks such as basic input/output and file management. In a graphics�oriented operating environment such as Microsoft Windows, high-level support for video graphics
	Arithmetic logic unit (ALU)	A device used for logical and arithmetic operations Arithmetic logic unit (ALU) within a computer.
	Artificial intelligence (AI)	Computer software that can mimic the learning Artificial intelligence capability of a human
	Assembler	A program that converts the assembly language of a

		computer program into the machine language of the computer.
	Assessment	An evaluation and/or valuation of IT assets based on predefined measurement or evaluation criteria. It is not typically necessary for an accounting or auditing firm to conduct an assessment, such as a risk or vulnerability assessment.
	Asset	Anything of value owned or possessed by an individual or a business.
	Asymmetric algorithm	A routine that uses a pair of different but related cryptographic keys to encrypt and decrypt data.
	Asymmetric encryption	In cryptography, a form of encryption in which an asymmetric key algorithm is used with a pair of cryptographic keys to encrypt and decrypt. The two keys are related mathematically: A message encrypted by the algorithm using one key can be decrypted by the same algorithm using the other. In a sense, one key lock the data, and a different key is required to unlock it.
	Asynchronous Transfer Mode (ATM)	Communication technology that uses high⍰bandwidth, low-delay transport technology and multiplexing techniques.
	Asynchronous transmission	A method whereby data is sent and received 1 byte at a time.
	Attenuation	A weakening of a signal that increases as the signal Attenuation travels farther from the source
	Attribute-based access control (ABAC)	A modern access control methodology in which access

		rights are granted by means of policies made up of attributes mapped to subjects and objects.
	Audit	An examination typically done by an accounting or auditing firm that conforms to a specific and formal methodology and definition for how an investigation is to be conducted, with specific reporting elements and metrics being examined (such as a financial audit according to public accounting and auditing)
	Audit trail	A set of records that collectively provide documentary evidence of processing that is used to aid in tracing from original transactions forward to related records and reports and/or backward from records and reports to their component source transactions.
	Authentication	A method of verifying that someone is who he or she purports to be. Authentication involves verifying the identity and legitimacy of an individual to access the system and its resources. Common authentication methods include passwords, tokens, and biometric systems.
	Authorization	The process of granting or denying access to a network resource based on a user's credentials.
	Authorization creep	A phenomenon that occurs when employees not only maintain old access rights but gain new ones. It results

		in too much access over time.
	Availability	One of the three items considered part of the security triad, in addition to confidentiality and integrity. It is a measure of the degree to which data or systems are available to authorized users.
B	Backdoor	A piece of software that allows access to a computer without using the conventional security procedures. Backdoors are often associated with Trojans.
	Back Orifice	A backdoor program that infects the end user with a Trojan and gives the attacker the ability to remotely control the user’s system.
	Backup	A copy of programs, databases, and other files that is made so that information can be restored in the event that it is lost due to, for instance, a computer failure, a natural disaster, or a virus infection.
	Bandwidth	The range of frequencies, expressed in hertz (Hz), that can pass over a given transmission channel. The bandwidth determines the rate at which information can be transmitted through the circuit.
	Baseband	The name given to a transmission method in which the entire bandwidth (the rate at which information travels through a network connection) is used to transmit just one signal.
	Baseline	A consistent or established base used to establish a

		Baseline minimum acceptable level of security.
	Bayesian filter	A technique used to detect spam. A Bayesian filter gives a score to each message based on the words and numbers in a message. These filters are often used by antispam software to filter spam based on probabilities. Messages with high scores are flagged as spam and can be discarded, deleted, or placed in a folder for review
	Bell-LaPadula	A formal security model based on confidentiality that is Bell defined by two basic properties
	Benchmark	A standard test or measurement used to compare the performance of similar components or systems.
	Binary code	A sequence of 0s and 1s used by computer systems as the basis of communication.
	Biometrics	A method of verifying a person’s identity for authentication by analyzing a unique physical attribute of the individual, such as a fingerprint, retina, or palm print.
	Blackbox	A form of testing in which the tester has no Blackbox knowledge of the target or its network structure
	Block cipher	An encryption scheme in which data is divided into fixed-size blocks, each of which is encrypted independently of the others.
	Blowfish	A form of symmetric block encryption designed in Blowfish 1993.
	Blu-ray disc	A storage medium designed as a replacement for DVDs.

		Blu-ray is a high-density optical disk that can hold audio, video, or data.
	Bluejacking	The act of sending unsolicited messages, pictures, Bluejacking or information to a Bluetooth user.
	Bluesnarfing	The theft of information from a wireless device Bluesnarfing through a Bluetooth connection.
	Bluetooth	An open standard for short-range wireless communications of data and voice between both mobile and stationary devices. Used in cell phones, PDAs, laptops, and other devices.
	Bluetooth Low Energy (BLE)	It's a variation of the classic Bluetooth technology but designed specifically for low power consumption. Introduced as part of the Bluetooth 4.0 specification by the Bluetooth Special Interest Group (Bluetooth SIG) in December 2009, BLE is optimized for transferring small amounts of data with minimal power usage. It operates on same frequency of 2.4 GHz that of classic Bluetooth
	Bollard	A heavy round post used to prevent vehicles from Bollard ramming buildings or breaching physical security.
	Botnet	A term used to describe a collection of robots-controlled workstations.
	Brewer and Nash model	A security model developed to prevent conflict of interest (COI) problems.
	Bridge	A Layer 2 device for passing signals between two LANs or two segments of a LAN.

	Broadband	A wired or wireless transmission medium capable of supporting a wide range of frequencies, typically from audio up to video frequencies. It can carry multiple signals by dividing the total capacity of the medium into multiple independent bandwidth channels, with each channel operating on only a specific range of frequencies.
	Broadcast	A type of transmission used on local and wide area networks in which all devices are sent the information from one host.
	Brute-force attack	A method of breaking a cipher or an encrypted value that involves trying many possibilities. Brute-force attacks function by working through all possible values. The feasibility of brute-force attacks depends on the key length and strength of the cipher and the processing power available to the attacker.
	Buffer	An amount of memory reserved for the temporary storage of data.
	Buffer overflow	In computer programming, a problem that occurs when a software application somehow writes data beyond the allocated end of a buffer in memory. Buffer overflow is usually caused by software bugs and improper syntax and programming that open or expose the application to malicious code injections or other targeted attack commands.

	Bus	A common channel shared among multiple Bus computer devices.
	Bus LAN configuration	A LAN network design that was developed to connect computers used for 10BASE-5 and 10BASE-2 computer networks. All computers and devices are connected along a common bus or single communication line so that transmissions by one device are received by all.
	Business case	A document developed to establish the merits and desirability of a project. It contains the information necessary to enable approval, authorization, and policymaking bodies to assess a project proposal and reach a reasoned decision, as well as justify the commitment of resources to a project.
	Business continuity plan (BCP)	A document that describes how an organization will resume partially or completely interrupted critical functions within a predetermined time after a disaster or disruption occurs. The goal is to keep critical functions operational.
	Business impact analysis (BIA)	A component of a business continuity plan that looks at all the components that an organization relies on for continued functionality. It seeks to distinguish which components are more crucial than others and require more funds in the wake of a disaster.
	Caesar cipher	A basic ROT3 cipher that works by means of a substitution. Each letter is

C		replaced with another letter from a fixed number of letters down the alphabet. A Caesar cipher is easily cracked.
	Capability Maturity Model (CMM)	A structured model designed by Carnegie Mellon's Software Engineering Institute to improve and optimize the software development lifecycle.
	Carrier-sense multiple access with collision avoidance (CSMA/CA)	An access method used by local area networking technologies such as Ethernet.
	Carrier sense multiple access with collision detection (CSMA/CD)	An access method used by local area networking Carrier technologies such as token ring.
	Catastrophe	A calamity or misfortune that causes the destruction of a facility and/or data.
	Central processing unit (CPU)	One of the central components of a computer system, which carries out the vast majority of the calculations performed by the computer. It can be thought of as the "brain" of a computer or as a manager or boss that tells what the other components of the system should be doing at a given moment
	Certificate	A digital file that uniquely identifies its owner. A certificate contains owner identity information and its owner's public key. Certificates are created by certificate authorities.
	Certificate authority. (CA)	An entity in the PKI infrastructure that issues certificates and reports status information and Certificate authority certificate revocation lists.

	Certificate Practice Statement (CPS)	A detailed explanation of how a certificate authority manages the certificates it issues and associated services such as key management. The CPS acts as a contract between the CA and users, describing obligations and legal limitations and setting the foundation for future audits
	Certificate Revocation List (CRL)	A certificate authority's list of invalid certificates, such as compromised, revoked, or superseded certificates. The CRL is used during the digital signature verification process to check the validity of a certificate from which a public verification key is extracted.
	Challenge-Handshake Authentication Protocol (CHAP)	A protocol for securely connecting to a system. CHAP functions as follows: (1) After the authentication request is made, the server sends a challenge message to the requestor. The requestor responds with a value obtained by using a one-way hash. (2) The server checks the response by comparing the received hash to a hash calculated locally by the server. (3) If the values match, the authentication is acknowledged; otherwise, the connection is terminated.
	Channel service unit/data service unit (CSU/DSU)	A telecommunications device used to terminate telephone company equipment, such as a T1, and prepare data for a router interface at the customer's premises.
	Ciphertext	The form of data after it has been encrypted; contrast with the form before encryption, called plaintext.

	Civil law	A type of law that usually pertains to the settlement of disputes between individuals, organizations, or groups and having to do with the establishment, recovery, or redress of private and civil rights. Civil law is not criminal law. It is also called tort law and is mainly for redress or recovery related to wrongdoing.
	Clark-Wilson model	An integrity-based security model focused on the integrity properties of real-world data; it uses CDIs, UDIs, and TPs.
	Client/server	Describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Clients rely on servers for resources such as files, devices, and processing power.
	Clipping level	The point at which an alarm threshold or trigger occurs.
	Cloning	A process that occurs when a hacker copies the electronic serial numbers from one cell phone to another, thereby duplicating the cell phone.
	Closed-circuit television (CCTV)	A system of television cameras used for video surveillance, in which all components are directly linked via cables or other direct means. Also, a system comprising video transmitters that can feed
	Closed system	A system that is not “open” and, therefore, is a proprietary system. Open systems employ modular designs, are widely

		supported, and facilitate multivendor, multi technology integration.
	Cloud computing	The use of a network of remote servers hosted on the Internet, rather than local servers, to store, manage, and process data.
	Coaxial cable	A cable composed of an insulated central conducting wire wrapped in another cylindrical conductor (the shield). The whole thing is usually wrapped in another insulating layer and an outer protective layer. A coaxial cable has great capacity to carry vast quantities of information. It is typically used in high-speed data and cable TV applications.
	COBIT	A framework that was designed by ISACA to aid in information security best practices. COBIT is an acronym for Control Objectives for Information and Related Technology.
	Cohesion	The extent to which a system or subsystem performs a single function
	Cold site	A location that contains no computing-related equipment except for environmental support, such as air conditioners and power outlets, and a security system made ready for installing computer equipment.
	Collision	A problem that occurs when a hashing algorithm, such as MD5, creates the same value for two or more different files.

	Combination lock	A physical lock that can be opened by turning dials in a predetermined sequence.
	Committed information rate (CIR)	The data rate guaranteed by a Frame Relay data communications circuit.
	Community cloud	Cloud infrastructure that is shared between several Community cloud sources.
	Compact disc (CD)	An optical disc that can store video, audio, and other data. CDs were originally designed for digital audio.
	Compensating control	An internal control designed to reduce risk or weakness in an existing control.
	Compiler	A computer program that translates a computer program written in one computer language (called the source language) into an equivalent program written in another computer language (called the object, output, or target language).
	Completely connected (mesh) configuration	A type of network configuration in which all devices are connected to all others with many redundant interconnections between network devices.
	Computer-aided software engineering (CASE)	The use of software tools to assist in the development and maintenance of software. Tools used in this way are known as CASE tools.
	Computer incident response team (CIRT)	An organization developed to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve the ability of organizations to respond to computer and network security issues.

	Concurrency control	In computer science, a method used to ensure that database transactions are executed in a safe manner (that is, without data loss). Concurrency control is especially applicable to database management systems, which must ensure that transactions are executed safely and that they follow the ACID rules.
	Confidentiality	One of the three parts of the security triad, in addition to integrity and availability. Confidentiality is a measure of how well data and systems are protected against access by unauthorized persons.
	Confidentiality agreement	An agreement that employees, contractors, or third-party users must read and sign prior to being granted access rights and privileges to an organization’s IT infrastructure and assets.
	Content delivery network (CDN)	A high-availability, high-performance network used to serve content to end users from multiple data centers.
	Contingency planning	The process of preparing to deal with calamities and non-calamitous situations before they occur to minimize the effects.
	Cookie	A message from a website given to an individual’s web browser on a workstation device. The workstation browser stores this text message in a text file, and the message is sent back to the web server each time the browser goes to that website.

	Copyright	Legal protection given to authors or creators that protects their expressions on a specific subject against unauthorized copying. It is applied to books, paintings, movies, literary works, and any other medium of use.
	Corporate governance	The method by which a corporation is directed, administered, or controlled. It includes the laws and customs affecting that direction, as well as the goals for which the organization is governed. How objectives of an organization are set, the means of attaining such objectives, how performance-monitoring guidelines are determined, and ways to emphasize the importance of using resources efficiently are significant issues of corporate governance.
	Corrective controls	Controls designed to resolve problems soon after Corrective controls they arise.
	Coupling	The extent of the complexity of interconnections Coupling with other modules.
	Covert channel	An unintended communication path that allows a process to transfer information in such a way that it violates a system's security policy.
	Cracker	A hacker who acts in an illegal manner. The term is Cracker derived from "criminal hacker."
	Criticality	The quality, state, degree, or measurement of the Criticality highest importance.

	Crossover error rate (CER)	A comparison measurement for different biometric devices and technologies that measures their accuracy. The CER is the point at which FAR and FRR are equal or cross over. The lower the CER, the more accurate the biometric system.
	Cryptographic key	A string of bits used by a cryptographic algorithm Cryptographic key during the encryption or decryption process.
	Cryptology	The science of secure communications.
D	Data breach	The exposure of sensitive information to Data breach unauthorized individuals.
	Data communications	The transmission or sharing of data between Data communications computers via an electronic medium.
	Data custodian	A data owner who has the responsibility for Data custodian maintaining and protecting an organization's data
	Data Encryption Standard (DES)	A symmetric encryption standard based on a 64-bit block. DES processes 64 bits of plaintext at a time to output 64-bit blocks of ciphertext. DES uses a 56- bit key and has four modes of operation because DES has been broken.
	Data leakage	Any type of computer information loss. It can involve removal of information by CD, floppy disk, USB thumb drive, or any other method.
	Data owner	A person, usually a member of senior management, in an organization who is ultimately responsible for

		ensuring the protection and use of the organization’s data.
	Data security	The science and study of methods of protecting data in computer and communications systems against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.
	Data structure	A logical relationship among data elements that is designed to support specific data-manipulation functions.
	Database	A collection of data that is organized and stored on a computer and can be searched and retrieved by a computer program.
	Database administrator (DBA)	A person (or group of people) responsible for maintenance activities related to a database, including backup and recovery, performance, and design.
	Database management system (DBMS)	An integrated set of computer programs that provides the capabilities needed to establish, modify, make available, and maintain the integrity of a database.
	Deadman door	A linked pair of doors that allows one person to enter the first door and then, after it is closed, allows the person to exit the second door. Deadman doors are used to control access and are also known as a mantrap.
	Decentralized computing	A type of computing in which activities and computer processing are distributed to different locations

	Decision support system (DSS)	A software application that analyzes business data and presents it so that users can make business decisions more easily.
	Decryption	The process of converting encrypted content into its original form, which is often plaintext. Decryption is the opposite of encryption.
	Defense in depth	Multilayered security in which the layers may be Defense in depth administrative, technical, or logical.
	Demilitarized zone (DMZ)	The middle ground between a trusted internal network and an untrusted external network. Services that internal and external users must use, such as HTTP, are typically placed in a DMZ.
	Denial of service (DoS)	A type of attack that occurs when an attacker consumes the resources on a computer or network for things it was not intended to be doing, thus preventing normal use of the computer or network resources for legitimate purposes.
	Destination NAT (DNAT)	A type of network translation that alters the destination address in an IP header. DNAT can also change the destination port in the TCP/UDP headers. The purpose of DNAT is to redirect incoming packets with the destination of a public address/port to a private IP address/port inside a network.
	Destruction	The act of destroying data so that it is denied to legitimate users

	Detective controls	Controls that identify and correct undesirable events
	Device lock	A physical lock used to secure laptops and other Device lock devices from theft.
	DevOps	The concept of blending development and operations together so that developers, programmers, engineers, and others can work together to build more secure software faster.
	Dictionary attack	A type of cryptographic attack in which the attacker uses a word list or dictionary list to try to crack an encrypted password. A newer technique is to use a time/memory trade-off, such as in rainbow tables.
	Digital certificate	A certificate, typically issued by a trusted third party, that contains the name of a user or server, a digital signature, a public key, and other elements used in authentication and encryption. An X.509 certificate is the most common type of digital certificate.
	Digital signature	An electronic signature that can be used to authenticate the identity of the sender of a message. A digital signature is usually created by encrypting the user's private key and is decrypted with the corresponding public key.
	Digital watermark	A hidden indicator of copyright information added to a document, picture, or sound file.
	Direct sequence spread spectrum (DSSS)	A technique used to scramble wireless signals.

	Disaster tolerance	The amount of time that an organization can accept Disaster tolerance the unavailability of IT facilities and service
	Discretionary access control. (DAC)	An access policy that allows the resource owner to Discretionary access control determine access.
	Distributed denial of service (DDoS)	An attack that is similar to DoS, except that it is Distributed denial launched from multiple distributed agent IP devices.
	Domain Name System (DNS)	A hierarchy of Internet servers that translate alphanumeric domain names into IP addresses and vice versa. Because domain names are alphanumeric, they are easier to remember than IP addresses.
	Downtime report	A record that tracks the amount of time a computer or other device is not operating because of a hardware or software failure.
	Due care	The standard of conduct taken by a reasonable and prudent person. When you see the term due care, think of the first letter of each word and remember “do correct” because due care is about performing the ongoing maintenance necessary to ensure the proper level of security
	Due diligence	Reasonable examination and research. When you see the term due diligence, think of the first letter of each word and remember “do detect.”
	Dumpster diving	The practice of rummaging through the trash of a potential target or victim to gain useful information.

	Dynamic Host Configuration Protocol (DHCP)	A protocol that dynamically assigns IP addresses to host devices.
E	Eavesdropping	The unauthorized capture and reading of network traffic.
	Echo request	The first part of an ICMP ping message, officially a Type 8.
	eDiscovery	The process of searching electronic data for evidence for a civil or criminal case.
	Electronic serial number (ESN)	A number that is used to identify a specific cell phone when it is turned on and requests to join a cell network.
	Email bomb	A hacker technique that involves flooding the email account of a victim with useless emails.
	Encapsulation of objects	A technique used by layered protocols that involves adding header information to the protocol data unit (PDU) from the layer above. Think of data encapsulated in a TCP header followed by an IP header as an example.
	Encryption	The process of turning plaintext into ciphertext
	Endpoint security	A client/server approach to network security that places security controls on end hosts, such as laptops, tablets, and smartphones.
	End-user licensing agreement (EULA)	A software license that a software vendor creates to protect and limit its liability and hold the purchaser liable for illegal pirating of the software application. The EULA typically has language in it that protects the software manufacturer from software bugs and flaws and limits the liability of the vendor

	Enterprise resource planning (ERP)	A software system used for operational planning and administration and for optimizing internal business processes. The best-known supplier of ERP systems is SAP.
	Enterprise vulnerability management	The overall responsibility and management of vulnerabilities within an organization and how that management of vulnerabilities will be achieved through dissemination of duties throughout the IT organization.
	Entity relationship diagram (ERD)	A diagram that helps map the requirements of and define the relationship between elements when designing a software program.
	Ethical hacker	Ethical hackers must obey rules of engagement, do no harm, and stay within legal boundaries. A security professional who legally attempts to break into a computer system or network to find its vulnerabilities
	Evasion	The performance of activities to avoid detection
	Evidence	Information gathered by an auditor during an audit that stands as proof to support the conclusions of an audit report.
	Exception report	A report that uses data selection based on a very specific set of circumstances to identify process exceptions. Reports that identify items with negative quantities of a product are examples of exception reports

	Exploit	A vulnerability in software or hardware that can be used by a hacker to gain access to a system or service.
	Extensible Authentication Protocol (EAP)	A protocol that supports multiple authentication methods, such as tokens, smart cards, certificates, and one-time passwords.
	Extranet	A private network that uses Internet protocols and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. An extranet requires security and privacy.
F	Failsafe	In a logical sense, the process of discovering a system error, terminating the process, and preventing the system from being compromised.
	False acceptance rate (FAR)	A biometric system measurement that indicates the percentage of individuals who are incorrectly granted access. This is the worst type of error that can occur because it means that unauthorized individuals have been allowed access.
	False rejection rate (FRR)	A biometric device error that indicates the percentage of authorized individuals who are incorrectly denied access.
	Fault Injection attack	A fault injection attack is a type of security breach where an attacker deliberately induces errors or "faults" into a system's hardware or software to

		cause it to behave in unintended ways. The typical goals of such attacks include bypassing security measures, gaining unauthorized access, or leaking sensitive information. Fault injection attacks can threaten even the most robust cryptographic algorithms by altering their operation and potentially revealing sensitive data or cryptographic keys. It's a significant concern in the field of cybersecurity, especially with the proliferation of Internet of Things (IoT) devices and embedded systems that interact with sensitive data.
	Field	In a database, the part of a record reserved for a particular type of data; for example, in a library catalog, author, title, ISBN, and subject headings would all be fields.
	File infector	A type of virus that copies itself into executable programs.
	Finger	On some UNIX systems, a command that identifies who is logged on and active and that may also provide personal information about that individual.
	Firewall	Hardware or software used to control network connectivity and network services. Firewalls act as chokepoints for traffic entering and leaving a network and prevent unrestricted access. Firewalls can be stateful or stateless

	Firmware	A computer program stored permanently in PROM or ROM or semi-permanently in EPROM. Software is “burned in” on the memory device so that it is nonvolatile (that is, so it will not be lost when power is shut off).
	Flooding	The process of overloading a network with traffic so that no legitimate traffic or activity can occur
	Frequency-hopping spread spectrum (FHSS)	A basic modulation technique used in spread�spectrum signal transmission. FHSS makes wireless communication harder to intercept and more resistant to interference
	Fuzzing	A black box testing technique that involves inputting random values and examining the output while looking for failures or exceptions.
G	Gateway	A device that allows for the translation and management of communication between networks that use different protocols or designs. A gateway can also be deployed in a security context to control sensitive traffic
	Gray box testing	Testing that occurs with only partial knowledge of the network or is performed to see what internal users have access to.
H	Hardware keystroke logger	A form of key logger that is a hardware device. When placed in a system, it is hard to detect without a physical inspection. A logger may be plugged in to the keyboard connector or can be built in to the keyboard.

	Hash	A cryptographic sum that is considered a one-way value. A hash is considerably shorter than the original text and can be used to uniquely identify it. You might have seen a hash value next to applications available for download on the Internet. By comparing the hash of an application with the one on the application vendor's website, you can make sure that the file has not been changed or altered
	Hashing algorithm	An algorithm that examines every bit of data while it is being condensed so that even a slight change to the data will result in a large change in the message hash. It is considered a one-way process. MD5 and SHA-256 are examples of hashing algorithms.
	Heuristic scanning	A form of virus scanning that looks at irregular activity by programs. For example, a heuristic scanner would flag a word processing program that attempted to format the hard drive, as that is not normal activity for a word processor.
	Honeypot	An Internet-attached server that acts as a decoy, luring in potential hackers to study their activities and monitor how they are able to break into a system.
	Hot site	A fully prepared and configured off-site location that is fully configured and supplied and ready for use in case of disaster.
	Hybrid cloud	A type of cloud that involves a combination of public and

		private cloud services. These services may be private on-premises or public cloud services.
I	Identity theft	An attack in which an individual’s personal, confidential, banking, and financial information is stolen and compromised by another individual or individuals. For example, use of a person’s Social Security number without that person’s consent or permission could result in identity theft.
	Impact	The extent of the consequences that would result if a given event occurred.
	Indexed sequential access method (ISAM)	A combination or compromise between indexed blocks of data arranged sequentially within each block; used for storing data for fast retrieval.
	Inference attack	A form of attack that relies on the attacker’s ability to make logical connections between seemingly unrelated pieces of information.
	Information Technology Security Evaluation Criteria (ITSEC)	A European standard that was developed in the 1980s to evaluate confidentiality, integrity, and availability of an entire system.
	Insecure computing habits	Bad habits that employees, contractors, and third-party users accumulate over time and that can be attributed to an organization’s lack of security awareness training, security controls, and security policies or acceptable use policies (AUPs).

	Integrity	One of the three items considered part of the security triad, along with confidentiality and availability. Integrity is a measure of the accuracy and completeness of data or systems.
	Internet Assigned Numbers Authority (IANA)	An organization dedicated to preserving the central coordinating functions of the global Internet for the public good. IANA oversees three key aspects of the Internet: top-level domains (TLDs), IP address allocation, and port number assignments. IANA is used by hackers and security specialists to track down domain owners and their contact details
	Internet of Things (IoT)	A network of consumer devices, vehicles, building controls (such as HVAC controls) embedded with electronic sensors and network connectivity so that they have the ability to collect and exchange data.
	Internet Protocol Security (IPsec)	An IETF standard used to secure TCP/IP traffic. It can be implemented to provide integrity and confidentiality.
	Intrusion detection system (IDS)	A network-monitoring device typically installed at an Internet ingress/egress point that is used to inspect inbound and outbound network activity and identify suspicious patterns that might indicate network or system attack from someone attempting to break in to or compromise a system.

J	Just a bunch of disks (JBOD)	A technique that is somewhat like RAID in that two or more hard drives are combined into one storage array. However, JBOD offers none of the fault tolerance advantages of RAID.
K	Key exchange protocol	A protocol used to exchange secret keys for the facilitation of encrypted communication. Diffie Hellman is an example of a key exchange protocol
	Kilo lines of code (KLOC)	A software metric used to determine the cost of software development based solely on the length of code.
L	Latency	The delay a packet incurs in traveling from one node to another.
	Lattice-based access control (LBAC)	A security model that deals with confidentiality and integrity and places upper and lower bounds on subjects and objects.
	Log	A system that automatically records significant events. The files that contain these records are called log files or simply logs; what is written on a log is a record
M	MAC filtering	A method of controlling access on a wired or wireless network by denying access to any device whose MAC address does not match an address from a pre-approved list.
	Man-in-the-middle attack	A type of attack in which the attacker can read, insert, and change information being passed between two parties without either party knowing that the information has been compromised.
	Mandatory access control (MAC)	A means of restricting access to objects based on the sensitivity (as represented by

		a label) of the information contained in the objects and the formal authorization (such as clearance) of subjects to access information of such sensitivity.
	MD5	A hashing algorithm that produces a 128-bit output.
	Media Access Control (MAC)	The hard-coded address of a physical layer device that is attached to a network. Every network interface controller must have a hard-coded and unique MAC address. The MAC address is 48 bits long
	Micro segmentation	The practice of splitting up a network into many isolated segments. This activity is used with software-defined networks to integrate access control lists and increased security.
	Middleware	Software that “glues together” two or more types of software (for example, two applications, their operating systems, and the network on which everything works) by translating information between them and exchanging this information over a network. The interacting applications are not aware of the middleware.
	Minimum acceptable level of risk	The stake that an organization defines for the seven areas of information security responsibility. Depending on the goals and objectives for maintaining confidentiality, integrity, and availability of the IT infrastructure and its assets, the minimum acceptable level of risk will dictate the

		amount of information security.
	Mobile site	A portable data-processing facility transported by trailers to be quickly moved to a business location. Typically used by insurance companies and the military, these information-processing facilities can contain servers, desktop computers, communications equipment, and even microwave and satellite data links.
	Multipartite virus	A virus that attempts to attack both the boot sector and executable files.
N	Network administrator	An individual responsible for the installation, management, and control of a network. When problems with the network arise, this is the person to call.
	NIST 800-42	A document that provides guidance on network security testing. It deals mainly with techniques and tools used to secure systems connected to the Internet.
	Non-attribution	The act of not providing a reference to a source of information.
	Non-repudiation	A system or method put in place to ensure that an individual or a system cannot deny his/her/its own actions
O	One-time pad	An encryption mechanism that can be used only once and that is, theoretically, unbreakable. One‐time pads function by combining plaintext with a random pad (secret key) that is the same length as the plaintext.
	Open Web Application Security Project (OWASP)	A nonprofit organization that is focused on improving application security.

P	Password Authentication Protocol (PAP)	An insecure, obsolete protocol for authentication in which cleartext usernames and passwords are used without encryption
	Password Authentication Protocol (PAP)	An insecure, obsolete protocol for authentication in which cleartext usernames and passwords are used without encryption.
	Pattern matching	A method used by IDSs to identify malicious traffic. It is also called signature matching and works by matching traffic against signatures stored in a database.
	Penetration test	A method of evaluating the security of a network or computer system by simulating an attack by a malicious hacker but without doing harm and with the owner’s consent.
	Phishing	The act of misleading or tricking an individual into providing personal and confidential information to an attacker masquerading as a legitimate individual or business.
	Phreaker	An individual who hacks phone systems or phone-related equipment. Phreakers predate computer hackers.
	Piggybacking	A method of gaining unauthorized access into a facility by following an authorized employee through a controlled access point or door.
	Post Office Protocol (POP)	A commonly implemented method of delivering email from an email server to a client machine. Other

		methods include IMAP and Microsoft Exchange
	Preventive controls	Controls that reduce risk and are used to prevent undesirable events from happening.
	Privacy impact analysis (PIA)	A review of the information held by a corporation and assessment of the damage that would result if sensitive or personal information were lost, stolen, or divulged.
	Procedure	A detailed, in-depth, step-by-step document that lays out exactly what is to be done and how it is to be accomplished.
	Public key encryption	An encryption scheme that uses two keys. In an email transaction, for example, the public key encrypts the data, and a corresponding private key decrypts the data. Because the private key is never transmitted or publicized, the encryption scheme is extremely secure. For digital signatures, the process is reversed
	Public key infrastructure (PKI)	Infrastructure used to facilitate e-commerce and build trust. PKI consists of hardware, software, people, policies, and procedures; it is used to create, manage, store, distribute, and revoke public key certificates. PKI is based on public key cryptography
Q	Qualitative analysis	A weighted factor or nonmonetary evaluation and analysis based on a weighting or criticality factor valuation.
	Qualitative risk assessment	A scenario-based assessment in which one scenario is examined and assessed for

		each critical or major threat to an IT asset
	Quantitative analysis	A numeric evaluation and analysis based on monetary valuation
	Quantitative risk assessment	A methodical, step-by-step calculation of asset valuation, exposure to threats, and the financial impact or loss that would occur if threats were realized.
R	Radio frequency identification (RFID)	A set of components that include a reader and a small device referred to as a tag. The tag can be used to hold information for inventory, management, tracking, or other purposes. RFID provides a method to transmit and receive data over a short range from one point to another.
	Recovery time objective (RTO)	During the execution of disaster recovery or business continuity plans, the time goal for the reestablishment and recovery of a business function or resource
	Registration authority (RA)	An entity responsible for the identification and authentication of a PKI certificate. The RA is not responsible for signing or issuing certificates. The most common form of certificate is the X.509 standard
	Remote Authentication Dial‑In User Service (RADIUS	A client/server protocol and software that allows remote-access servers to communicate. Used in wireless systems such as 802.1x.
	Repository	A central place where data is stored and maintained. A repository can be a place where multiple databases or

		files are located for distribution over a network, or it can be a location that is directly accessible to users.
	Required vacations	A security control used to uncover misuse or illegal activity by requiring employees to use their vacation time.
S	Side Channel Attack	Side channel attack is a security exploit that gains information from the physical implementation of a computer system, rather than through software vulnerabilities. It involves analyzing indirect information such as power consumption, electromagnetic leaks, or even sound to uncover sensitive data like cryptographic keys or personal information
T	Trustzone	TrustZone is a technology that creates a secure area within a device's processor to provide a safe environment for sensitive operations.
U	Unclassified Information	Unclassified information is data that doesn’t require special handling or protection for security reasons and is accessible to the public. Controlled Unclassified Information (CUI) is a subset that, while not classified, still requires safeguarding according to legal standards.

V	Vulnerability	Vulnerability refers to the quality of being easily harmed, influenced, or attacked, whether physically or emotionally. It also denotes a specific weakness that can be exploited
Z	Zero Trust	Zero Trust is a security framework that operates on the principle of "never trust, always verify," requiring strict identity verification for every person and device trying to access resources on a private network. It eliminates implicit trust and continuously authenticates and authorizes based on the premise that threats can exist both inside and outside traditional network boundaries.