simplilearn
your pace, your place

CISSP—Glossary

802.11	IEEE 802.11 defines the mechanical process of WLAN implementation for vendors to create compatible products. WLAN standards include 802.11a, 802.11b, 802.11g, and 802.11n.
802.3	IEEE 802.3 defines the physical and data link layer implementation of wired Ethernet. 802.3 is a technology that supports IEEE 802.1 network architecture.
Abstraction	Suppresses unnecessary details and lets people focus on what they are trying to accomplish
Access	Access is the transfer of data between subjects and objects. E.g.: Accessing Web Server.
Access Control	Access control is that security feature which controls how a user and or system interact and communicate with other systems and resources.
Access Control List (ACL)	It specifies which subjects are granted access and what operations are allowed on objects.
Access Point	In wireless, an access point provides network connectivity for end devices such as PCs.
Accountability	Accountability is a system's capability to determine an individual's behavior and actions in a system and also to identify any particular individual.
Accreditation	It relates to the management's evaluation of the capability of a system in meeting the company's needs.
Acquisition	An acquisition is the buying of one business or company by another organization or business entity.
Address Resolution Protocol (ARP)	It is a protocol to resolve IP address to a Media Access Control (MAC) address.
Algorithm	The process of encryption or decryption uses a mathematical function that is also known as algorithm.
Applet	Applets, also known as mobile codes, are a small executable code that is placed in other software like web browser.
Asset	Asset is any information, software, hardware, or equipment that is utilized for, and critical to, business objectives, service delivery, and financial success.
Assurance	The amount of confidence in security methods and their capability to consistently perform
Attribute	A column in a two-dimensional database
Audit	Auditing means validating compliance to a security control framework, standard, or published specification.
Authentication	Authentication is the process of verification of the identity of a subject.
Authorization	Authorization is giving access to a data or object once the subject has been accurately identified and authenticated.
Availability	Availability is ensuring that information or a computer system is available to authorized entities as needed.

Avalanche Effect	A feature that denotes that a significant amount of change in ciphertext occurs because of a minor change in a key or plaintext.
Backdoor	Backdoor is any malicious program which permits log in by bypassing security protocols and checks.
Baselines	It refers to a state or data that is used as a control for comparison with future changes.
Bastian host	A bastion host is a hardened host that is fully exposed to attacks due to being on the demilitarized zone's public side, without protection from a firewall or filtering router.
Behavior	The end result exhibited or shown by an object in response to a message
Blackout	A total loss of power
Block Cipher	Operates on a fixed-length block or chunk of plaintext to a ciphertext block of the same length
Bollard	Bollard is a strong post designed to stop vehicles.
Broadcast	Transmission of a packet from a source to all of the nodes in a network or segment of a network
Brownout	A prolonged reduction in voltage below the normal minimum specification
Business Impact Analysis (BIA)	It is the formal method for determining how a disruption to an organization's IT system(s) will affect its functions and processes.
Cell	Row and column's intersection
CER	Crossover Error Rate (CER) is the point where the false rejection rate becomes equal to the false acceptance rate.
Certification	Evaluation or testing of a system's architecture, design, and controls, as per the standardized evaluation criteria
Change Management	The change management process involves documenting and tracking all planned changes, formally approving the substantial changes, and documentation.
Ciphertext	Also *cryptogram*. Message after alteration, now unreadable to the attacker but readable to intended recipient.
Class	It describes one or more objects or a group of common objects.
Cloud Computing	It is a type of computing that depends on sharing computing resources over the Internet instead of having personal device or local servers handle applications.
Clustering	A group of two or more servers that operate functionally as a single logical server
Collision	For different inputs, a hash function generates the same output. This is known as collision.
Confidentiality	Confidentiality refers to preventing unauthorized access of information within systems.
Common Criteria (CC)	It is an international set of specifications and guidelines developed for evaluation of information security products, especially to ensure that the agreed-upon security standards for government deployments are met.
Compilers	Compilers take source codes, and convert them into machine code that is

	saved in executable format.
Control	Countermeasure or Control is used to mitigate the potential risk.
Control Framework	Control framework is the structure of an organization's security solutions, designed to maximize business value and minimize risk.
Covert Channel	Covert channel is violation of security policy by any communication.
Crippleware	It is a software in which important functions are disabled; it is a partially functioning software.
Cryptanalysis	Techniques for deciphering encrypted communications without having the proper keys
Cryptology	Study and practice of techniques of hidden, disguised, and encrypted communications
Cryptosystem	Encompasses the entire cryptographic operation; Includes key + algorithm + key management functions
Database	A collection of structured set of data
DBMS	Database Management System (DBMS) is used for managing and controlling the database.
Data Dictionary	Data elements and their relationships stored in a central repository
Data Diddler	Trojan that deliberately corrupts data in the system
Data Mining	It is a tool that uses structured queries along with an inference engine to extract information from databases or data warehouses to match complex or relational information searches.
Data Remanence	After erasing data from the media, some data is left on it.
Data-Scavenging	The technique in which the information found in bits of data is pieced together
Data Warehouse	It is a storage facility comprising data from several databases or pre-computed data to be used by users through query and analysis tools.
Deadlocking	Two users denied access to a file when they both simultaneously try to access it.
Decoding	Opposite of encoding process; used to get plaintext from encoded format.
Decryption	Also *decipher*. The reverse of encryption, i.e., converting ciphertext into plaintext
Demilitarized zone (DMZ)	A buffer zone between an unprotected network and a protected network that allows for the monitoring and regulation of traffic between the two.
DIAMETER	An open protocol standard that authenticates and authorizes dial-up users and provides a centralized access control mechanism. It overcomes some of RADIUS's deficiencies and is more secure.
Diffusion	Dispersing the order of the plaintext throughout the ciphertext. Transposition allows first character of the plaintext to change several times during encryption and makes cryptanalysis much more difficult.
Divestiture	Divestment or divestiture is the decrease of some kind of asset either for ethical or financial objectives or for the sale of an existing business by a firm
Dropout	Also called Fault, it is total loss of power for a very short time period (milliseconds to a few seconds).
Due Care	Due care shows that the organization is using reasonable care to protect its activities, resources, and employees from all possible threats.

Due Diligence	Due diligence is the act of understanding and investigating the risks a company faces.
Encapsulation	Direct access for interacting or viewing the contents of the object is denied, and thus, the object is protected.
Encryption	Also *enciphering*. Converting plaintext message to ciphertext message.
Evaluation Assurance Level (EAL)	Degree or score of evaluation of a tested system or product
Event	An occurrence happening in an information system, which can be verified, analyzed, and documented
Expert System	It uses information from a knowledge expert to make decisions similar to that of a human.
Exposure	Exposure is the incident of being exposed and vulnerable to losses due to a threat agent.
Extensible Markup Language (XML)	Data is structured in a text file and is a World Wide Web Consortium (W3C) standard
Fail Safe	A failure mode that ensures that if software or system failure is detected for any reason, the system is protected from vulnerability.
False Acceptance Rate (FAR)	When an impostor who should be rejected is accepted in the system, it is false acceptance rate or called a Type II error
False Rejection Rate (FRR)	False rejection rate or Type I error is the rate at which authorized individuals are rejected by the biometric system.
File	A group of the similar kinds of records
Firmware	Software instructions that have been written into read-only memory (ROM) or a programmable ROM (PROM) chip
Foreign Key	When the primary key of one table has values matching an attribute of another table, the attribute is known as a foreign key.
Frame Relay	Frame relay is a WAN protocol that uses packet-switching technology and operates at the OSI model's data link layer.
Functionality	Functionality ensures the entity does what it says.
Goal	Goals are high-level and specific milestones that lend an overall context for what the organization hopes to accomplish.
Guidelines	Recommended operational guides or actions to users, operations staff, IT staff, and others
Honeypot	It is a system in which some services or ports are kept open to confuse the attacker in thinking that it is the production server and thereby study the techniques used by him to attack.
Hypervisor	Virtual machine monitor (VMM) or hypervisor is a software which is installed to virtualize a given computer.
Identification	Identification refers to a way of making sure that a subject is the same entity that it claims to be.
Identity Management	Identity management is a general term for the processes and procedures used to identify, authenticate, and authorize people in an organization.
Incident	An adverse event or series of events that negatively affects the company and/or affects its security posture.

Incident Response	It is a process of problem detection, determining what caused it, minimizing the damages due to it, problem resolution and documentation for future references.
Information Classification	Classification of information into different levels based on its sensitivity
Information Hiding	Components do not need to know how other components actually work
Information Risk Management (IRM)	The process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain it at that level
Information Security	Information security is the process of protecting data from unauthorized disclosure, access, use, destruction, deletion, modification, or disruption.
Information Security Governance	Information security governance is the set of practices and responsibilities implemented by the board and executive management with the aim of providing strategic direction.
Information Security Management	Information security management includes information security policies, standards, procedures, guidelines, baselines, information classification, risk management, security education, etc.
Inheritance	Subclass inherits method and class from the parent class
Initialization Vector	Also known as Nonce, it is an arbitrary number which is used with a secret key for encrypting the data and thus increasing the security.
Inrush	The instantaneous drawing of current by a device when it is first switched on
Integrity	Integrity refers to protecting the information system or processes from unintentional or intentional unauthorized changes.
Internet Protocol Security (IPSec)	Internet Protocol Security (IPsec) is a protocol suite used for securing Internet Protocol (IP) communications.
Interpreter	It is a computer program that directly executes, i.e., executes instructions written in a programming language.
Intrusion Detection System (IDS)	IDS is used to detect any malicious traffic or activity that tries to gain access to the target.
Intrusion Prevention System (IPS)	IPS is used to detect and prevent any malicious traffic or activity from gaining access to the target.
ISO 27001	Provides a framework for an “Information Security Management System” for designing, implementing, managing, maintaining IS processes entirely in an organization.
ISO 27034	International standard that provides guidelines to organizations on integrating security in software processes and is applicable to in-house developed or acquired software.
ITIL (IT Infrastructure Library)	Framework for identifying, planning, delivering, and supporting IT services to business.
Kernel	The core of an operating system, a kernel manages the machine’s hardware resources (including the processor and the memory), and provides and controls the way any other software component accesses these resources.
Key	Also *cryptovariable*. Sequence that controls the operation of the cryptographic algorithm
Key Clustering	Using the same transformation algorithm but with different keys or

	cryptovariables, a plaintext message generates identical cipher text messages.
Key Space	The set of all possible values that can be used to generate a key in a cryptographic algorithm
Liability	Refers to someone responsible for something. Civil and criminal penalties can be the punishment as a sanction for a legally liable person.
Logic Bomb	When a condition is met, this malicious program is activated.
Malicious code (Malware)	Malicious code (Malware) is designed to attack any application or program.
Maintenance hook	Maintenance hook is a type of backdoor or shortcut into an application which allows developers or programmers to directly enter an application during development, bypassing normal system checks.
Maximum Tolerable Downtime (MTD)	It is the maximum period of time for which the organization's key processes and functions are unavailable, after which the organization would suffer significant losses.
Message	Communication received by an object to carry out some operation
Metadata	Data about data – Describes resources and improves retrieval of information
Method	The actions of an object in response to a message it receives is defined by a code known as the method.
Mission	Mission or 'Mission statement' is a statement of the purpose of an organization, company or person and its reason for existence.
Multicast	Transmission of packet from a source to specific multiple destinations on the network
Multiprocessing	Servers or powerful computers having many processors handling different tasks, with one main processor and supplementary processors
Multitasking	Multitasking switches from one process to another to speed up processing.
Multithreading	The Operating System runs multiple threads simultaneously one after another by time slicing the threads and executing on the CPU.
Negligence	Not exercising due care like a prudent person is expected to exercise in a similar situation
Network Address Translation (NAT)	It converts a private IP address of the inside, trusted network to a registered "real" IP address seen by the outside, untrusted network.
Neural Network	It is a network with many simple processors built similar to the human brain
Noise	Random bursts of small changes in voltage
Nonrepudiation	Service by which sender and recipient cannot deny having participated in the communication
Object	A distinct entity that a programmer can create. Each object knows how to manipulate itself.
Object Reuse	To prevent unauthorized disclosure, the residual information on hard drive or tape should be cleared before it is allocated to another user.
Objective	A business objective is the map used to reach the goals of the organization.
Offshoring	It means outsourcing to another country.
One-way Hash	A hash function uses an algorithm without any key for encryption. This encryption cannot be reversed; hence, it is called "one way."
Open Web Application Security Project	A nonprofit organization focused on enhancing the application security

(OWASP)	
Outsourcing	Outsourcing is the subcontracting of a business process to a third-party company.
OTP	One-time password (OTP) or dynamic password will be valid for only one login session or transaction.
Passphrase	It is a password type in the form of a sequence of characters.
Patch Management	Patch management is the process of applying proper patches to the system at a specified time by using a strategy and plan.
Payment Card Industry Data Security Standard (PCI-DSS)	Payment Card Industry Security Standards Council (PCI-SSC) created PCI-DSS for the protection of an organization's customer account data in a proactive manner.
Pharming	Attack on DNS that redirects access to a legitimate, yet an imposter, site
Phishing	Emails luring users to fraudulent sites
Polymorphism	The ability of displaying different behavior depending on the receiver, with methods having the same names and parameter types.
Polyinstantiation	Developing a new version of an object by replacing the variables in one object by other values
Primary Key	Column that identify a row uniquely (Every row of a table must include a primary key.)
Privacy	Privacy is the safeguarding of the confidentiality of personal information. Ex: Bank account details
Procedure	Detailed or specific step-by-step tasks that should be performed to achieve a certain objective
Process	A process, also known as heavy-weight process (HWP) or task, is an executable program which loads its data and runs in memory.
Protection Profile (PP)	For a particular category of systems or products such as firewalls or IDS, PP is an independent set of security objectives and requirements.
Qualitative Analysis	Qualitative analysis is situation and scenario based, and does not use calculations.
Quantitative Analysis	Quantitative analysis uses risk calculations that attempt to predict the level of financial losses and the percentage of chance for each type of threat.
Record	A database entry with one or more values
Recovery point objective (RPO)	It is the amount of work/data loss or system inaccessibility (measured in time) that an organization can withstand in the event of a disaster or disruptive event.
Recovery time objective (RTO)	Also known as systems recovery time, which is the maximum allowed time for recovering IT or business systems
Reference Monitor	An access control mechanism that is auditable
Remote Authentication Dial-In User Service (RADIUS)	It is a security service that authenticates and authorizes dial-up users and is a centralized access control mechanism.
RAID	RAID is Redundant Array of Inexpensive Disks or Redundant Array of Independent Disks. It ensures availability of data by providing fault tolerance against hard disk failure in a file server.
Residual Risk	Residual risk is the risk remaining after risk treatment.

Risk	Risk is the likelihood of a threat agent taking advantage of a weakness or vulnerability and the resulting business impact.
Risk Analysis	Risk Analysis involves analyzing the likelihood and consequences of each identified risk.
Rootkit	Collection of tools (programs) that enable administrator-level access to a computer or computer network
SABSA	Sherwood Applied Business Security Architecture (SABSA) is the methodology and framework for Enterprise Security Architecture and service management
Sag	A short drop in voltage
Schema	Defines the structure of the database
Secure Socket Layer (SSL)	A protocol developed by Netscape for transmitting private documents via the Internet
Security Assertion Markup Language (SAML)	A format that uses XML to describe security information – primarily identity and authorization-related information
Security Policy	Security policy is an overall broad statement produced by senior management that dictates what role security plays within the organization.
Security Target (ST)	The document that describes the Target of Evaluation or TOE, which includes security requirements and operational environment.
Service bureaus	The BCP/DRP planning and/or implementation is outsourced by some organizations by paying another company to perform those services.
Service Oriented Architecture (SOA)	Provides standardized access to the most needed services for many different applications at one time
SLA	Service Level Agreement (SLA) is a formally defined level of service provided by an organization.
Smurf	A large number of forged ICMP echo requests. The packets are sent to a target network's broadcast address, which causes all systems on the network to respond.
Sniffers	It is a device that is used to intercept and log traffic over network.
SP-Network	Stands for substitution and permutation (transposition) (usually repeated); For increasing their strength, block ciphers use SP-Network. An SP-network breaks plaintext into a series of smaller S-boxes to handle computations.
Standard	Rules indicating how hardware and software should be implemented, used, and maintained. Standards provide a means to ensure that specific technologies or applications are used uniformly throughout an organization.
Steganography	Secret messages are hidden behind a picture file, audio file, etc.
Stream Cipher	A stream of ciphertext data is generated by combining the keystream (sequence of bits) with plaintext data bit-by-bit using XOR operations
Substitution	Exchange of one letter or byte for another. HIDE(Plaintext)-- shift alphabet 3 spaces—KLGH(Ciphertext)
Surge	A prolonged increase in voltage
SYN Flood	A large volume of TCP SYN packets consumes resources on target system and causes denial of service attack.
TACACS (Terminal access controller access	A client/server authentication protocol that authenticates and authorizes dial-up users and is used as a central access control mechanism mainly for

control system)	remote users
Target of Evaluation (ToE)	The target product or system whose evaluation has to be done
Teardrop Attack	An attacker sends mangled packet fragments with overlapping and oversized payloads to a target system
TEMPEST	A countermeasure for emanation security which limits signal emanations with shielding material
Threat	Threat is any potential danger to systems or information.
Threat Agent	Threat agent is any entity that takes advantage of vulnerability.
TOC/TOU	Time of Check/Time of Use, also called Race condition, is when an attacker tries to change a condition after the operating system checks it but before it is used
TOGAF	Enterprise architecture framework which provides a comprehensive approach for designing, planning, implementing, and governing an enterprise information architecture
Transient	A brief oscillation in voltage
Trusted computing base (TCB)	The totality of protection mechanisms within it, including hardware, firmware, and software, the combination of which is responsible for enforcing a computer security policy
Trusted Platform Module (TPM)	A dedicated chip that is installed for hardware authentication on the motherboard of a personal computer
Tuple	A row in a two-dimensional database
Unicast	Transmission of a packet from one source to one destination
View	A virtual relation defined in order to keep certain data hidden from subjects
Virtualization	Multiple operating systems can run simultaneously on a single processing hardware
Virtual LAN (VLAN)	A virtual local area network (VLAN) allows ports on the same or different switches to be grouped so that traffic is confined to members of that group.
Virtual Memory	It permits inactive portions of a program's memory to use secondary storage, which provides free primary memory that can be used by other processes.
Virtual Private Network (VPN)	A secure communication link between two nodes, emulating the properties of a point-to-point private link
Voice over IP (VoIP)	A category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP
Vulnerability	Vulnerability is any hardware, software, or procedural weakness that may give an attacker the open door for unauthorized access to resources.
Web Application Security Consortium (WASC)	A nonprofit organization that produces open source and best practices for World Wide Web. It is composed of an international group of experts, industry practitioners, and organizational representatives.
Work Factor	For breaking a protective system, the amount of time and effort required is known as the work factor.
Work recovery time (WRT)	For configuring the recovered system, the required time is called WRT.

simplilearn
your pace, your place

Zachman Framework	A comprehensive representation of an information technology enterprise represented by a logical structure

