CISSP-ANT 2021 glossary

Active Security Testing	Security testing that involves direct interaction with a target, such as sending packets to a target.
Banner Grabbing	The process of capturing banner information—such as application type and version—that is transmitted by a remote port when a connection is initiated.
Computer Security Log Management	Log management for computer security log data only.
Covert Testing	Testing performed using covert methods and without the knowledge of the organization's IT staff, but with full knowledge and permission of upper management.
Event	Something that occurs within a system or network.
Event Aggregation	The consolidation of similar log entries into a single entry containing a count of the number of occurrences of the event.
Event Correlation	Finding relationships between two or more log entries.
Event Filtering	The suppression of log entries from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.
Event Reduction	Removing unneeded data fields from all log entries to create a new log that is smaller.
External Security Testing	Security testing conducted from outside the organization's security perimeter.
Facility	The message type for a syslog message.
False Positive	An alert that incorrectly indicates that a vulnerability is present.
File Integrity Checking	Software that generates, stores, and compares message digests for files to detect changes made to the files.
Information Security Testing	The process of validating the effective implementation of security controls for information systems and networks, based on the organization's security requirements.
Internal Security Testing	Security testing conducted from inside the organization's security perimeter.
Log	A record of the events occurring within an organization's systems and networks.
Log Analysis	Studying log entries to identify events of interest or suppress log entries for insignificant events.
Log Archival	Retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server.
Log Clearing	Removing all entries from a log that precede a certain date

	and time.
Log Compression	Storing a log file in a way that reduces the amount of storage space needed for the file without altering the meaning of its contents.
Log Conversion	Parsing a log in one format and storing its entries in a second format.
Log Entry	An individual record within a log.
Log File Integrity Checking	Comparing the current message digest for a log file to the original message digest to determine if the log file has been modified.
Log Management	The process for generating, transmitting, storing, analyzing, and disposing of log data.
Log Management Infrastructure	The hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data.
Log Normalization	Converting each log data field to a particular data representation and categorizing it consistently.
Log Parsing	Extracting data from a log so that the parsed values can be used as input for another logging process.
Log Preservation	Keeping logs that normally would be discarded, because they contain records of activity of particular interest.
Log Reduction	Removing unneeded entries from a log to create a new log that is smaller.
Log Reporting	Displaying the results of log analysis.
Log Retention	Archiving logs on a regular basis as part of standard operational activities.
Log Rotation	Closing a log file and opening a new log file when the first log file is considered to be complete.
Log Viewing	Displaying log entries in a human-readable format.
Message Digest	A digital signature that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated.
Network Discovery	The process of discovering active and responding hosts on a network, identifying weaknesses, and learning how the network operates.
Network Sniffing	A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.
Operating System Fingerprinting	Analyzing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system in use on the target.
Overt Testing	Security testing performed with the knowledge and consent

	of the organization's IT staff.
Passive Security Testing	Security testing that does not involve any direct interaction with the targets, such as sending packets to a target.
Password Cracking	The process of recovering secret passwords stored in a computer system or transmitted over a network.
Penetration Testing	Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.
Phishing	A digital form of social engineering that uses authentic-looking—but bogus—e-mails to request information from users or direct them to a fake Web site that requests information.
Plan of Actions and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for meeting the tasks, and scheduled milestone completion dates.
Port Scanner	A program that can remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).
Review Techniques	Passive information security testing techniques, generally conducted manually, that are used to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities. They include documentation, log, ruleset, and system configuration review; network sniffing; and file integrity checking.
Rogue Device	An unauthorized node on a network.
Rule-Based Event Correlation	Correlating events by matching multiple log entries from a single source or multiple sources based on logged values, such as timestamps, IP addresses, and event types.
Rules of Engagement	Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions.
Ruleset	A collection of rules or signatures that network traffic or system activity is compared against to determine an action

	to take—such as forwarding or rejecting a packet, creating an alert, or allowing a system event.
Security Information and Event Management Software	A program that provides centralized logging capabilities for a variety of log types.
Social Engineering	The process of attempting to trick someone into revealing information (e.g., a password).
Syslog	A protocol that specifies a general log entry format and a log entry transport mechanism.
Target Identification and Analysis Techniques	Information security testing techniques, mostly active and generally conducted using automated tools, that are used to identify systems, ports, services, and potential vulnerabilities. Target identification and analysis techniques include network discovery, network port and service identification, vulnerability scanning, wireless scanning, and application security testing.
Target Vulnerability Validation Techniques	Active information security testing techniques that corroborate the existence of vulnerabilities. They include password cracking, remote access testing, penetration testing, social engineering, and physical security testing.
Version Scanning	The process of identifying the service application and application version currently in use.
Virtual Machine	Software that allows a single host to run one or more guest operating systems.
Vulnerability	Weakness in an information system, or in system security procedures, internal controls, or implementation, that could be exploited or triggered by a threat source.
Vulnerability Scanning	A technique used to identify hosts/host attributes and associated vulnerabilities.

CISSP-DEV 2021 glossary

Application Programming Interface	a library of commands maintained by a system for other programs to use, provides consistency and integrity for the programs
Assembler	converts a high level language into machine language
Assembly Code	low-level programming language with a few simple operations this code is harder to maintain, less readable, and has the potential to be substantially longer.
Atomicity	indivisible, data field must contain only one value that either all transactions take place or none do
Big Endian	most significant byte is stored first. SPARC uses a this architecture.
Botnet	organized group of compromised computers
Buffer	an area of memory allocated with a fixed size. It is commonly used as a temporary holding zone when data is transferred between two devices that are not operating at the same speed or workload.
Buffer Overflow	occurs when an area that has been allocated a specific storage space has more data copied to it than it can handle two classes include heap and stack overflows.
Byte Code	program code that is in between the highlevel language code understood by humans and machine code read by computers.
Checkpoint	part of a transaction control for a database which informs the database of the last recorded transaction
Class	OOP concept of a template that consist of attributes and behaviors
Compiler	converts source code to an executable
Consistency	property that data is represented in the same manner at all times
Cross-site scripting	malware that uses the trust on a website to redirect users to untrusted websites which captures data or installs more

	malware
Dangling Pointer	false memory reference
Data dictionary	a description of a database
Data diddler	malware that makes small random changes to many data points
Data Hiding	a feature of object-oriented programming languages. Classes and variables may be marked private, which restricts outside access to the internal workings of a class.
Data marts	small data warehouse
Data Type	specifies the way a variable will be stored in memory
Data warehouse	a copy of transaction data, designed for querying and reporting
Databases	a collection of information designed to reduce duplication and increase integrity
Deadlock	a condition in which neither party is willing to stop their activity for the other to complete
Denial of Service	an availability attack, to consume resources to the point of exhaustion
Disassembler	software tool is used to convert compiled programs in machine code to assembly code
Distributed Denial of Service	an availability attack, to consume resources to the point of exhaustion from multiple vectors
Durability	what is will remain, persistence
Dynamic Link Library	a programming component that runs on Win32 systems and contains functionality that is used by many other programs
Encapsulation	a feature of object-oriented programming, provides a logical structure to a program and allows for easy methods of inheritance.
Exploit	causes a software vulnerability to be triggered and leveraged by the attacker.
Function	a miniature program.
Heap	an area of memory utilized by an application and is allocated dynamically at runtime. Static variables are stored

	on the stack along with data allocated using the malloc interface.
HTTP Response Splitting	uncheck data input which results in redirection
Inference	to jump to a conclusion
Inheritance	Object-oriented organization and encapsulation allow programmers to easily reuse previously written code. it saves time since programmers do not have to recode previously implemented functionality.
Instance	OOP concept of an object at runtime
Integer Wrapping	In the case of unsigned values,this occurs when an overly large unsigned value is sent to an application that “passes” the integer back to zero or a small number.
Interpreter	line by line translation from a high level language to machine code
Isolation	another subject cannot see an ongoing or pending update until it is complete
Java	modern, object-oriented programming language, It combines a similar syntax to C and C++ with features such as platform independence and automatic garbage collection.
Little Endian	the least significant byte is stored first
Logic bomb	a program that waits for a condition or time to occur that executes an inappropriate activity
MAC	The hardware address of a particular computer system.
Machine language	program instructions based upon the CPU's specific architecture
Malformed input	inappropriate data
Malloc	a function call dynamically allocates n number of bytes on the heap. Many vulnerabilities are associated with the way this data is handled.
Memset	a function call is used to fill a heap buffer with a specified number of bytes of a certain character.

Metadata	information about data or records
Method	another name for a function in languages such as Java and C# it may be thought of as a miniature program.
NULL	A term used to describe a programming variable which has not had a value set, this value is not necessarily the same as a value of “” or 0.
Object Oriented Programming	design philosophy and a type of programming language, which breaks a program into smaller units. Each unit has its own function.
Object reuse	uncleared buffers or media
Object-oriented	programs are organized into classes. Instances of classes contain data and methods which perform actions on that data
Off-by-One	a bug is present when a buffer is set up with size n and somewhere in the application a function attempts to write n+1 bytes to the buffer.This often occurs with static buffers
Patch Management	business and technical process of applying security software updates in a regulated periodic way
Payload	final purpose or result
Platform Independence	idea that program code can run on different systems without modification or recompilation
Polymorphism	objects or programming that looks the different but act same
Printf	LIBC function for outputting data to a command-line interface
Procedural Language Programs	may be viewed as a sequence of instructions, where data at certain memory locations are modified at each step
Program	collection of commands that are understood by a computer system and may be written in a high-level language, such as Java or C, or in low-level assembly language.
Race condition	a state where two subjects can access the same object without proper mediation
Register	an area on the processor used to store information. Intel

	architecture: eax, ebx, ecx, edx, esi, and edi
Remote Access Trojan	a Trojan horse with the express underlying purpose of controlling host from a distance
Rollback	transaction controls for a database, a return to a previous state
Rootkit	malware that subverts the detective controls of an operating system
Salami	malware that makes many small changes over time to a single data point or system
Sandbox	a construct used to control code execution. Code executed cannot affect outside systems.This is particularly useful for security when a user needs to run mobile code, such as Java applets.
Service Provider Interface	used by devices to communicate with software it is normally written by the manufacturer of a hardware device to communicate with the operating system.
Shellcode	byte code that executes a shell or the code that is executed when an exploit is successful
Slack space	unused storage capacity
Spiral	a design methodology which addresses risk early and often
Spyware	program that inappropriately collects private data or activity
SQL injection	a type of malformed input that takes advantage of an appropriate true conditional logic statement adding a request for data that is against the security policy
Stack	an area of memory used to hold temporary data. It grows and shrinks throughout the duration of a program's runtime
Stack Overflow	occurs when a buffer has been overrun in the stack space. When this happens, the return address is overwritten, allowing for arbitrary code to be executed.
strcpy	LIBC function call is more commonly misimplemented because it copies data from one buffer to another without any size limitation

System Life Cycle	project management process with following phases: design and development, production, distribution, operation, maintenance, retirement, and disposal
Time of Check/Time of Use	a race condition where the security changes during the object's access
Trapdoors	(Backdoors) (maintenance hooks) a programming device use in development to circumvent controls
Trojan horse	a program with an inappropriate second purpose
Virtual Machine	a software simulation of a platform that can execute code it allows code to execute without being tailored to the specific hardware processor
Virus	independent malware that requires user interaction to execute
Vulnerability	an exposure that has the potential to be exploited most are specific software bugs or logic errors
Waterfall	a design methodology which executes in a linear one way fashion
Worm	autonomous malware that requires a flaw in a service
x86	a family of computer architectures commonly associated with Intel

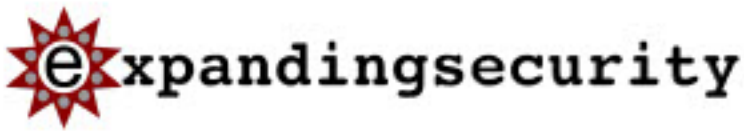
expandingsecurity

CISSP-CNS 2021 glossary

Access point	The connection between a wireless and wired network.
Bridge	A layer 2 device that used to connect two network segments and regulate traffic.
Brouter	A device that provides the functions of both a bridge and a router.
Coaxial cable	A cable consisting of a core, inner conductor that is surrounding by an insulator, an outer cylindrical conductor
Codec	Used to code/decode a digital data stream.
Concentrator	Layer 1 network device that is used to connect network segments together, but provides no traffic control
Demon Dialer	a technique by which a computer is used to repeatedly dial a number (usually to a crowded modem pool) in an attempt to gain access immediately after another user had hung up.
Digital signature	An asymmetric cryptography mechanism that provides authentication.
Eavesdropping	A passive network attack involving monitoring of traffic.
E-Mail spoofing	Forgery of the sender's email address in an email header.
Emanations	Potentially compromising leakage of electrical or acoustical signals.
Faraday Cage/ Shield	A shield against leakage of electromagnetic signals.
Fiber optics	Bundles of long strands of pure glass that efficiently transmit light pulses over long distances. Interception without detection is difficult.
Firewalls	A system that enforces an access control policy between two networks.
Fraggle	A Denial of Service attack initiated by sending spoofed UDP echo request to IP broadcast addresses.
Gateway	A secure connection to another network.
Hijacking	Interception and take over of a communication session by an attacker.

Hub	Layer 1 network device that is used to connect network segments together, but provides no traffic control
Injection	An attack technique that exploits systems that do not perform input validation by embedding partial SQL queries inside input.
Interception	Unauthorized access of information (e.g. tapping, sniffing, unsecured wireless communication, emanations)
IP address spoofing	Forging of an IP address.
IP Fragmentation	An attack that breaks up malicious code into fragments, in an attempt to elude detection.
Microwave	High frequency, highly directional radio signals. Attackers target interception attempts at transmission and relay stations.
Modems	A device that converts between digital and analog representation of data.
Modification	A type of attack involving attempted insertion, deletion or altering of data.
Multiplexers	A device that sequentially switches multiple analog inputs to the output.
Open mail relay servers	A mail server that improperly allows inbound SMTP connections for domains it does not serve.
Overlapping fragment attack	A Denial of Service attack that exploits packet filter firewalls that only inspect the initial fragment of a fragmented packet.
Packet filtering	A basic level of network access control that is based upon information contained in the IP packet header.
Patch panels	Provides a physical cross connect point for devices.
PBX	A Private Branch Exchange is a telephone exchange for a specific office or business.
Phishing	A social engineering attack that uses spoofed email or websites to persuade people to divulge information.
Physical tampering	Unauthorized access of network devices.
Proxies	Mediates communication between un-trusted hosts on

	behalf of the hosts that it protects.
Repeaters	Layer 1 network device that is used to connect network segments together, but provides no traffic control (a concentrator).
Rogue access points	Unauthorized wireless network access device.
Routers	A layer 3 device that used to connect two or more network segments and regulate traffic.
Satellite	A specialized wireless receiver/ transmitter placed in orbit that facilitates long distance communication.
Sequence Attacks	An attack involving the hijacking of a TCP session by predicting a sequence number.
Shielding	Enclosure of electronic communication devices to prevent leakage of electromagnetic signals.
Smurf	A Denial of Service attack initiated by sending spoofed ICMP echo request to IP broadcast addresses.
Sniffing	Eavesdropping on network communications by a third party.
Source routing exploitation	A vulnerability in IP that allows an attacker to dictate the path of a communication and thereby access an internal network.
Spam	Unsolicited commercial email
Switches	A layer 2 device that used to connect two or more network segments and regulate traffic.
SYN flooding	A Denial of Service attack that floods the target system with connection requests that are not finalized.
Tapping	Eavesdropping on network communications by a third party.
Tar Pits	Mitigation of spamming and other attacks by delaying incoming connections as long as possible.
Teardrop	A Denial of Service attack that exploits systems that are not able to handle malicious, overlapping and oversized IP fragments.



TEMPEST	A codename that refers to the study and mitigation of information disclosure via electromagnetic emanations from electronic equipment.
Twisted pair	A simple, inexpensive cabling technology consisting of two conductors that are wound together to decrease interference.
Voice over IP	Voice over Internet Protocol (VoIP) – a protocol for the efficient transmission of voice over the Internet
War dialing	Reconnaissance technique, involving automated, brute force identification of potentially vulnerable modems.
War Driving	Searching for wireless networks in a moving car.
Wi-Fi	wireless local area network technology specified in the 802.11 sub group A,B,G, or N
WI-MAX	“Worldwide Interoperability for Microwave Access” (IEEE 802.16) is a specification for wireless Metropolitan Area Networks that provides an alternative to the use of cable and DSL for last mile delivery.
Zero Trust	organizations should not automatically trust anything inside or outside its perimeters and instead must authenticate and verify all subjects, objects, and actions before granting access

CISSP-SRM 2021 glossary

27001	specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organization's overall business risks.
27002	A standard that defines information's confidentiality, integrity and availability controls in a comprehensive information security management system
Acceptable use policy	A policy that establishes an agreement between users and the organization and defines for all parties the ranges of use that are approved before gaining access to a network or the Internet
Access rights	Permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system as defined by rules established by data owners and the information security policy
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Accountability	The ability to map a given activity or event back to the responsible party
Administrative controls	The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies
Application controls	Manual or programmed activities intended to ensure the completeness and accuracy of records and the validity of entries made. The objectives of application controls are to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from

	manual and programmed processing.
Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass.
Audit trail	A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source
Availability	The security goal that generates the requirement for protection against— • Intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data • Unauthorized use of system resources.
Chief information security officer	An executive position charged with responsibility for managing and protecting information assets
Confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.
Control Objectives for Information and related Technology	A complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business goals and related IT goals by providing a comprehensive IT governance, management, control and assurance model. COBIT describes IT processes and associated control objectives, management guidelines (activities, accountabilities, responsibilities and performance metrics) and maturity models. COBIT supports enterprise management in the development, implementation, continuous improvement and monitoring of good IT-related practices.

Corporate governance	The system by which organizations are directed and controlled. Boards of directors are responsible for the governance of their organizations. It consists of the leadership and organizational structures and processes that ensure the organization sustains and extends strategies and objectives.
Corporate strategy	The pattern of decisions in a company that determines and reveals its objectives, purposes or goals; produces the principal policies and plans for achieving those goals; and defines the range of business the company is to pursue, the kind of economic and human organization it is or intends to be, and the nature of the economic and non-economic contribution it intends to make to its shareholders, employees, customers and communities
Countermeasure	a control after attack
Cross training	to know more than one job
Custodian	the guardian of asset(s), a maintenance activity
Data classification	The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the organization.
Decentralization	The process of distributing computer processing to different locations within an organization
Denial of Service	The prevention of authorized access to resources or the delaying of time critical operations.
Dual control	A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource such that no single entity acting alone can access that resource

Due Care	Managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. Integrity The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
Education	long term knowledge building
Ethics	the principles a person sets for themselves to follow
Exposure	An opportunity for a threat to cause loss. (terminology that encompasses many recent risk terms)
Governance	Executive responsibilities of goal setting, delegation, and verification, based upon the mission.
Guidelines	written suggestions that direct choice to a few alternatives
Information owner	the one person responsible for data, its classification and control setting
Information security governance	The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly
Information security program	The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis

IT-Related Risk	The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to these 4 items: 1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information 2. Unintentional errors and omissions 3. IT disruptions due to natural or man-made disasters 4. Failure to exercise due care and diligence in the implementation and operation of the IT system.
Job rotation	to move from location to location, keeping the same function
Job training	employment education done once per position or at significant change of function
Mandatory access control	A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users' programs acting on their behalf
Mandatory vacations	requirement to take time off
Mitigate	a choice in risk management, to implement a control that limits or lessens negative effects
Monitoring policy	The rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured
Objects	Data or systems, passive
Operational	intermediate level, pertaining to planning
Policy	written core statements that rarely change
Privacy	Freedom from unauthorized intrusion or disclosure of information about individuals
Private / privacy	Individual owned or ownership
Procedure	written step-by-step actions
Procedures	The portion of a security policy that states the general

	process that will be performed to accomplish a security goal
Qualitative	a risk assessment method, intrinsic value
Quantitative	a risk assessment method, measurable real money cost
Residual risk	quantity of risk remaining after a control is applied
Risk	the chance that something negative will occur
Risk assessment	the collection and summation of risk data relating to a particular asset and controls for that asset
Risk Management	The total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.
Safeguard	a control before attack
Security clearance	the level and label given to an individual for the purpose of compartmentalization
Security Goals	The five security goals are integrity, availability, confidentiality, accountability, and assurance.
Security metrics	Any form of measurement used to determine any aspect of the operation of any security-related activity
Separation of Duties	to break a business process into separate functions and assign to different people
Standard	written internalized or nationalized norms that are internal to an organization
Steering committee	A management committee assembled to sponsor and manage various projects, such as an information security program
Strategic	high level, pertaining to planning
Subjects	people or groups, Active
Tactical	low level, pertaining to planning
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat Agent	those who initiate the attack
Threat Analysis	The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
Threats	vehicle or tool that exploits a weakness
Threat-source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.
Total Risk	calculation encompassing threats, vulnerabilities and assets
Transfer	a choice in risk management, to convince another to assume risk, typically by payment
User	people who interact with assets
Vulnerability	weakness or flaw in an asset