Cybersecurity Fundamentals Glossary

Term	Definition
Acceptable interruption window	The maximum period of time that a system can be unavailable before compromising the achievement of the enterprise's business objectives
Acceptable use policy	A policy that establishes an agreement between users and the enterprise and defines for all parties' the ranges of use that are approved before gaining access to a network or the Internet
Access control list (ACL)	An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals Scope Note: Also referred to as access control tables
Access path	The logical route that an end user takes to access computerized information Scope Note: Typically includes a route through the operating system, telecommunications software, selected application software and the access control system
Access rights	The 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 ability to map a given activity or event back to the responsible party
Advanced Encryption Standard (AES)	A public algorithm that supports keys from 128 bits to 256 bits in size
Advanced persistent threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives using multiple attack vectors (NIST SP800-61) Scope Note: The APT: 1. pursues its objectives repeatedly over an extended period of time 2. adapts to defenders' efforts to resist it 3. is determined to maintain the level of interaction needed to execute its objectives

Term	Definition
Adversary	A threat agent
Adware	A software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used Scope Note: In most cases, this is done without any notification to the user or without the user's consent. The term adware may also refer to software that displays advertisements, whether or not it does so with the user's consent; such programs display advertisements as an alternative to shareware registration fees. These are classified as adware in the sense of advertising supported software, but not as spyware. Adware in this form does not operate surreptitiously or mislead the user, and it provides the user with a specific service.
Alert situation	The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The enterprise entering into an alert situation initiates a series of escalation steps.
Alternate facilities	Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed Scope Note: Includes other buildings, offices or data processing centers
Alternate process	Automatic or manual process designed and established to continue critical business processes from point-of-failure to return-to-normal
Analog	A transmission signal that varies continuously in amplitude and time and is generated in wave formation Scope Note: Analog signals are used in telecommunications
Anti-malware	A technology widely used to prevent, detect and remove many categories of malware, including computer viruses, worms, Trojans, keyloggers, malicious browser plug-ins, adware and spyware
Antivirus software	An application software deployed at multiple points in an IT architecture It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected

Term	Definition
Application layer	In the Open Systems Interconnection (OSI) communications model, the application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. Scope Note: The application layer is not the application that is doing the communication; a service layer that provides these services.
Architecture	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation
Asymmetric key (public key)	A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message Scope Note: See Public key encryption.
Attack	An actual occurrence of an adverse event
Attack mechanism	A method used to deliver the exploit. Unless the attacker is personally performing the attack, an attack mechanism may involve a payload, or container, that delivers the exploit to the target.
Attack vector	A path or route used by the adversary to gain access to the target (asset) Scope Note: There are two types of attack vectors: ingress and egress (also known as data exfiltration)
Attenuation	Reduction of signal strength during transmission
Audit trail	A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source
Authentication	1. The act of verifying identity (i.e., user, system) Scope Note: Risk: Can also refer to the verification of the correctness of a piece of data 2. The act of verifying the identity of a user and the user's eligibility to access computerized information Scope Note: Assurance: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.

Term	Definition
Authenticity	Undisputed authorship
Availability	Ensuring timely and reliable access to and use of information
Back door	A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions
Bandwidth	The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity of an electronic line and is expressed in bytes per second or Hertz (cycles per second).
Bastion	System heavily fortified against attacks
Biometrics	A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint
Block cipher	A public algorithm that operates on plaintext in blocks (strings or groups) of bits
Botnet	A term derived from "robot network;" is a large automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as a denial-of-service attack on selected victims
Boundary	Logical and physical controls to define a perimeter between the organization and the outside world
Bridge	Data link layer device developed in the early 1980s to connect local area networks (LANs) or create two separate LAN or wide area network (WAN) network segments from a single segment to reduce collision domains Scope Note: A bridge acts as a store-and-forward device in moving frames toward their destination. This is achieved by analyzing the MAC header of a data packet, which represents the hardware address of an NIC.
Bring your own device (BYOD)	An enterprise policy used to permit partial or full integration of user-owned mobile devices for business purposes
Broadcast	A method to distribute information to multiple recipients simultaneously
Brute force	A class of algorithms that repeatedly try all possible combinations until a solution is found
Brute force attack	Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found

Term	Definition
Buffer overflow	Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold Scope Note: Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
Business continuity plan (BCP)	A plan used by an enterprise to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems
Business impact analysis/assessment (BIA)	Evaluating the criticality and sensitivity of information assets An exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and the supporting system Scope Note: This process also includes addressing: -Income loss -Unexpected expense -Legal issues (regulatory compliance or contractual) -Interdependent processes -Loss of public reputation or public confidence
Certificate (Certification) authority (CA)	A trusted third party that serves authentication infrastructures or enterprises and registers entities and issues them certificates

Term	Definition
Certificate revocation list (CRL)	An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility Scope Note: The CRL details digital certificates that are no longer valid. The time gap between two updates is very critical and is also a risk in digital certificates verification.
Chain of custody	A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. Scope Note: Includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.
Checksum	A mathematical value that is assigned to a file and used to “test” the file at a later date to verify that the data contained in the file has not been maliciously changed Scope Note: A cryptographic checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as the checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum. Cryptographic checksums are used in data transmission and data storage. Cryptographic checksums are also known as message authentication codes, integrity check-values, modification detection codes or message integrity codes.
Chief Information Security Officer (CISO)	The person in charge of information security within the enterprise
Chief Security Officer (CSO)	The person usually responsible for all security matters both physical and digital in an enterprise
Cipher	An algorithm to perform encryption
Ciphertext	Information generated by an encryption algorithm to protect the plaintext and that is unintelligible to the unauthorized reader.

Term	Definition
Cleartext	Data that is not encrypted. Also known as plaintext.
Cloud computing	Convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction
Collision	The situation that occurs when two or more demands are made simultaneously on equipment that can handle only one at any given instant (Federal Standard 1037C)
Common Attack Pattern Enumeration and Classification (CAPEC)	A catalogue of attack patterns as “an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed” published by the MITRE Corporation
Compartmentalization	A process for protecting very-high value assets or in environments where trust is an issue. Access to an asset requires two or more processes, controls or individuals.
Compliance	Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies
Compliance documents	Policies, standard and procedures that document the actions that are required or prohibited. Violations may be subject to disciplinary actions.
Computer emergency response team (CERT)	A group of people integrated at the enterprise with clear lines of reporting and responsibilities for standby support in case of an information systems emergency This group will act as an efficient corrective control, and should also act as a single point of contact for all incidents and issues related to information systems.
Computer forensics	The application of the scientific method to digital media to establish factual information for judicial review Scope Note: This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities. As a discipline, it combines elements of law and computer science to collect and analyze data from information systems (e.g., personal computers, networks, wireless communication and digital storage devices) in a way that is admissible as evidence in a court of law.
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information
Configuration management	The control of changes to a set of configuration items over a system life cycle

Term	Definition
Consumerization	A new model in which emerging technologies are first embraced by the consumer market and later spread to the business
Containment	Actions taken to limit exposure after an incident has been identified and confirmed
Content filtering	Controlling access to a network by analyzing the contents of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules Scope Note: Differs from packet filtering in that it is the data in the packet that are analyzed instead of the attributes of the packet itself (e.g., source/target IP address, transmission control protocol [TCP] flags)
Control	The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature. Scope Note: Also used as a synonym for safeguard or countermeasure. See also Internal control.
Countermeasure	Any process that directly reduces a threat or vulnerability
Critical infrastructure	Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation.
Criticality	The importance of a particular asset or function to the enterprise, and the impact if that asset or function is not available
Criticality analysis	An analysis to evaluate resources or business functions to identify their importance to the enterprise, and the impact if a function cannot be completed or a resource is not available
Cross-site scripting (XSS)	A type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites Scope Note: Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. (OWASP)
Cryptography	The art of designing, analyzing and attacking cryptographic schemes
Cryptosystem	A pair of algorithms that take a key and convert plaintext to ciphertext and back
Cybercop	An investigator of activities related to computer crime
Cyberespionage	Activities conducted in the name of security, business, politics or technology to find information that ought to remain secret. It is not inherently military.

Term	Definition
Cybersecurity	The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems
Cybersecurity architecture	Describes the structure, components and topology (connections and layout) of security controls within an enterprise's IT infrastructure Scope Note: The security architecture shows how defense-in-depth is implemented and how layers of control are linked and is essential to designing and implementing security controls in any complex environment.
Cyberwarfare	Activities supported by military organizations with the purpose to threat the survival and well-being of society/foreign entity
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 enterprise.
Data custodian	The individual(s) and department(s) responsible for the storage and safeguarding of computerized data
Data Encryption Standard (DES)	An algorithm for encoding binary data Scope Note: It is a secret key cryptosystem published by the National Bureau of Standards (NBS), the predecessor of the US National Institute of Standards and Technology (NIST). DES and its variants has been replaced by the Advanced Encryption Standard (AES)
Data leakage	Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes
Data owner	The individual(s), normally a manager or director, who has responsibility for the integrity, accurate reporting and use of computerized data
Data retention	Refers to the policies that govern data and records management for meeting internal, legal and regulatory data archival requirements
Database	A stored collection of related data needed by enterprises and individuals to meet their information processing and retrieval requirements
Decentralization	The process of distributing computer processing to different locations within an enterprise

Term	Definition
Decryption	A technique used to recover the original plaintext from the ciphertext so that it is intelligible to the reader The decryption is a reverse process of the encryption.
Decryption key	A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption
Defense in depth	The practice of layering defenses to provide added protection Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.
Demilitarized zone (DMZ)	A screened (firewalled) network segment that acts as a buffer zone between a trusted and untrusted network Scope Note: A DMZ is typically used to house systems such as web servers that must be accessible from both internal networks and the Internet.
Denial-of-service attack (DoS)	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate
Digital certificate	A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender’s private key or applying a one-way hash function.
Digital forensics	The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings
Digital signature	A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation A digital signature is generated using the sender’s private key or applying a one-way hash function.
Disaster	1. A sudden, unplanned calamitous event causing great damage or loss. Any event that creates an inability on an enterprise's part to provide critical business functions for some predetermined period of time. Similar terms are business interruption, outage and catastrophe. 2. The period when enterprise management decides to divert from normal production responses and exercises its disaster recovery plan (DRP). It typically signifies the beginning of a move from a primary location to an alternate location.

Term	Definition
Disaster recovery plan (DRP)	A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster
Discretionary access control (DAC)	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong Scope Note: The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
Domain name system (DNS)	A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers
Domain name system (DNS) exfiltration	Tunneling over DNS to gain network access. Lower-level attack vector for simple to complex data transmission, slow but difficult to detect.
Due care	The level of care expected from a reasonable person of similar competency under similar conditions
Due diligence	The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis
Dynamic ports	Dynamic and/or private ports--49152 through 65535: Not listed by IANA because of their dynamic nature.
Eavesdropping	Listening a private communication without permission
E-commerce	The processes by which enterprises conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology Scope Note: E-commerce encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models, but does not include existing non-Internet e-commerce methods based on private networks such as electronic data interchange (EDI) and Society for Worldwide Interbank Financial Telecommunication (SWIFT).
Egress	Network communications going out
Elliptical curve cryptography (ECC)	An algorithm that combines plane geometry with algebra to achieve stronger authentication with smaller keys compared to traditional methods, such as RSA, which primarily use algebraic factoring. Scope Note: Smaller keys are more suitable to mobile devices.

Term	Definition
Encapsulation security payload (ESP)	Protocol, which is designed to provide a mix of security services in IPv4 and IPv6. ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. (RFC 4303) Scope Note: The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode).
Encryption	The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext)
Encryption algorithm	A mathematically based function or calculation that encrypts/decrypts data
Encryption key	A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext
Eradication	When containment measures have been deployed after an incident occurs, the root cause of the incident must be identified and removed from the network. Scope Note: Eradication methods include: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause.
Ethernet	A popular network protocol and cabling scheme that uses a bus topology and carrier sense multiple access/collision detection (CSMA/CD) to prevent network failures or collisions when two devices try to access the network at the same time
Event	Something that happens at a specific place and/or time
Evidence	1. Information that proves or disproves a stated issue 2. Information that an auditor gathers in the course of performing an IS audit; relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support Scope Note: Audit perspective
Exploit	Full use of a vulnerability for the benefit of an attacker
File Transfer Protocol (FTP)	A protocol used to transfer files over a Transmission Control Protocol/Internet Protocol (TCP/IP) network (Internet, UNIX, etc.)
Firewall	A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet

Term	Definition
Forensic examination	The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise
Freeware	Software available free of charge
Gateway	A device (router, firewall) on a network that serves as an entrance to another network
Governance	Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives Scope Note: Conditions can include the cost of capital, foreign exchange rates, etc. Options can include shifting manufacturing to other locations, sub-contracting portions of the enterprise to third-parties, selecting a product mix from many available choices, etc.
Governance, Risk Management and Compliance (GRC)	A business term used to group the three close-related disciplines responsible for the protection of assets, and operations
Guideline	A description of a particular way of accomplishing something that is less prescriptive than a procedure
Hacker	An individual who attempts to gain unauthorized access to a computer system
Hash function	An algorithm that maps or translates one set of bits into another (generally smaller) so that a message yields the same result every time the algorithm is executed using the same message as input Scope Note: It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm or to find two different messages that produce the same hash result using the same algorithm.
Hash total	The total of any numeric data field in a document or computer file This total is checked against a control total of the same field to facilitate accuracy of processing.
Hashing	Using a hash function (algorithm) to create hash valued or checksums that validate message integrity
Hijacking	An exploitation of a valid network session for unauthorized purposes
Honeypot	A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems Scope Note: Also known as "decoy server"

Term	Definition
Horizontal defense-in depth	Controls are placed in various places in the path to access an asset (this is functionally equivalent to concentric ring model above).
Hub	A common connection point for devices in a network, hubs are used to connect segments of a local area network (LAN) Scope Note: A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
Human firewall	A person prepared to act as a network layer of defense through education and awareness
Hypertext Transfer Protocol Secure (HTTPS)	A protocol for accessing a secure web server, whereby all data transferred are encrypted.
Hypertext Transfer Protocol (HTTP)	A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit hypertext markup language (HTML), extensible markup language (XML) or other pages to client browsers
IEEE (Institute of Electrical and Electronics Engineers)	Pronounced I-triple-E; IEEE is an organization composed of engineers, scientists and students Scope Note: Best known for developing standards for the computer and electronics industry
IEEE 802.11	A family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area network (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.
Imaging	A process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed. Scope Note: The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.
Impact	Magnitude of loss resulting from a threat exploiting a vulnerability
Impact analysis	A study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events In an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.

Term	Definition
Incident	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service
Incident response	The response of an enterprise to a disaster or other significant event that may significantly affect the enterprise, its people, or its ability to function productively An incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing damage assessment, and any other measures necessary to bring an enterprise to a more stable status.
Incident response plan	The operational component of incident management Scope Note: The plan includes documented procedures and guidelines for defining the criticality of incidents, reporting and escalation process, and recovery procedures.
Information security	Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)
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
Information systems (IS)	The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies Scope Note: Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.
Infrastructure as a Service (IaaS)	Offers the capability to provision processing, storage, networks and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, which can include operating systems (OSs) and applications
Ingestion	A process to convert information extracted to a format that can be understood by investigators. Scope Note: See also Normalization.
Ingress	Network communications coming in
Inherent risk	The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)
Injection	A general term for attack types which consist of injecting code that is then interpreted/executed by the application. (OWASP)

Term	Definition
Intangible asset	An asset that is not physical in nature Scope Note: Examples include: intellectual property (patents, trademarks, copyrights, processes), goodwill, and brand recognition
Integrity	The guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
Intellectual property	Intangible assets that belong to an enterprise for its exclusive use Scope Note: Examples include: patents, copyrights, trademarks, ideas, and trade secrets.
International Standards Organization (ISO)	The world's largest developer of voluntary International Standards
Internet Assigned Numbers Authority (IANA)	Responsible for the global coordination of the DNS root, IP addressing, and other Internet protocol resources
Internet Control Message Protocol (ICMP)	A set of protocols that allow systems to communicate information about the state of services on other systems Scope Note: For example, ICMP is used in determining whether systems are up, maximum packet sizes on links, whether a destination host/network/port is available. Hackers typically use (abuse) ICMP to determine information about the remote site.
Internet protocol (IP)	Specifies the format of packets and the addressing scheme
Internet Protocol (IP) packet spoofing	An attack using packets with the spoofed source Internet packet (IP) addresses. Scope Note: This technique exploits applications that use authentication based on IP addresses. This technique also may enable an unauthorized user to gain root access on the target system.
Internet service provider (ISP)	A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services
Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)	IPX is layer 3 of the open systems interconnect (OSI) model network protocol; SPX is layer 4 transport protocol. The SPX layer sits on top of the IPX layer and provides connection-oriented services between two nodes on the network.
Interrogation	Used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data

Term	Definition
Intruder	Individual or group gaining access to the network and it's resources without permission
Intrusion detection	The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack
Intrusion detection system (IDS)	Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack
Intrusion prevention	A preemptive approach to network security used to identify potential threats and respond to them to stop, or at least limit, damage or disruption
Intrusion prevention system (IPS)	A system designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks
Investigation	The collection and analysis of evidence with the goal to identifying the perpetrator of an attack or unauthorized use or access
IP address	A unique binary number used to identify devices on a TCP/IP network
IP Authentication Header (AH)	Protocol used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "integrity") and to provide protection against replays. (RFC 4302). Scope Note: AH ensures data integrity with a checksum that a message authentication code, such as MD5, generates. To ensure data origin authentication, AH includes a secret shared key in the algorithm that it uses for authentication. To ensure replay protection, AH uses a sequence number field within the IP authentication header.
IP Security (IPSec)	A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets
IT governance	The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives
Kernel mode	Used for execution of privileged instructions for the internal operation of the system. In kernel mode, there are no protections from errors or malicious activity and all parts of the system and memory are accessible.
Key length	The size of the encryption key measured in bits
Key risk indicator (KRI)	A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk Scope Note: See also Risk Indicator.
Keylogger	Software used to record all keystrokes on a computer

Term	Definition
Latency	The time it takes a system and network delay to respond Scope Note: More specifically, system latency is the time that a system takes to retrieve data. Network latency is the time it takes for a packet to travel from the source to the final destination.
Layer 2 switches	Data link level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks
Layer 3 and 4 switches	Switches with operating capabilities at layer 3 and layer 4 of the open systems interconnect (OSI) model. These switches look at the incoming packet's networking protocol, e.g., IP, and then compare the destination IP address to the list of addresses in their tables, to actively calculate the best way to send a packet to its destination.
Layer 4-7 switches	Used for load balancing among groups of servers Scope Note: Also known as content-switches, content services switches, web-switches or application-switches.
Legacy system	Outdated computer systems
Likelihood	The probability of something happening
Local area network (LAN)	Communication network that serves several users within a specified geographic area Scope Note: A personal computer LAN functions as a distributed processing system in which each computer in the network does its own processing and manages some of its data. Shared data are stored in a file server that acts as a remote disk drive for all users in the network.
Log	To record details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred
Logical access	Ability to interact with computer resources granted using identification, authentication and authorization.
Logical access controls	The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files
MAC header	Represents the hardware address of an network interface controller (NIC) inside a data packet
Mail relay server	An electronic mail (e-mail) server that relays messages so that neither the sender nor the recipient is a local user
Mainframe	A large high-speed computer, especially one supporting numerous workstations or peripherals

Term	Definition
Malware	Short for malicious software Designed to infiltrate, damage or obtain information from a computer system without the owner's consent Scope Note: Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes.
Mandatory access control (MAC)	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 or programs acting on their behalf
Man-in-the-middle attack	An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication
Masking	A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report
Media access control (MAC) address	A unique identifier assigned to network interfaces for communications on the physical network segment
Message authentication code	An American National Standards Institute (ANSI) standard checksum that is computed using Data Encryption Standard (DES)
Message digest	A smaller extrapolated version of the original message created using a message digest algorithm
Message digest algorithm	Message digest algorithms are SHA1, MD2, MD4 and MD5. These algorithms are one-way functions unlike private and public key encryption algorithms. Scope Note: All digest algorithms take a message of arbitrary length and produce a 128-bit message digest.
Metropolitan area network (MAN)	A data network intended to serve an area the size of a large city
Miniature fragment attack	Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall, in the hope that only the first of the sequence of fragmented packets would be examined and the others would pass without review.

Term	Definition
Mirrored site	An alternate site that contains the same information as the original Scope Note: Mirrored sites are set up for backup and disaster recovery and to balance the traffic load for numerous download requests. Such download mirrors are often placed in different locations throughout the Internet.
Mobile device	A small, handheld computing devices, typically having a display screen with touch input and/or a miniature keyboard and weighing less than two pounds
Mobile site	The use of a mobile/temporary facility to serve as a business resumption location The facility can usually be delivered to any site and can house information technology and staff.
Monitoring policy	Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted
Multifactor authentication	A combination of more than one authentication method, such as token and password (or personal identification number [PIN] or token and biometric device).
National Institute for Standards and Technology (NIST)	Develops tests, test methods, reference data, proof-of concept implementations, and technical analyses to advance the development and productive use of information technology Scope Note: NIST is a US government entity that creates mandatory standards that are followed by federal agencies and those doing business with them.
Network address translation (NAT)	A methodology of modifying network address information in IP datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another
Network basic input/output system (NetBIOS)	A program that allows applications on different computers to communicate within a local area network (LAN).
Network interface card (NIC)	A communication card that when inserted into a computer, allows it to communicate with other computers on a network Scope Note: Most NICs are designed for a particular type of network or protocol.
Network news transfer protocol (NNTP)	Used for the distribution, inquiry, retrieval, and posting of Netnews articles using a reliable stream-based mechanism. For news-reading clients, NNTP enables retrieval of news articles that are stored in a central database, giving subscribers the ability to select only those articles they wish to read. (RFC 3977)

Term	Definition
Network segmentation	A common technique to implement network security is to segment an organization's network into separate zones that can be separately controlled, monitored and protected.
Network traffic analysis	Identifies patterns in network communications Scope Note: Traffic analysis does not need to have the actual content of the communication but analyzes where traffic is taking place, when and for how long communications occur and the size of information transferred.
Nonintrusive monitoring	The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities
Nonrepudiation	The assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data and that can be verified by a third party Scope Note: A digital signature can provide non-repudiation.
Normalization	The elimination of redundant data
Obfuscation	The deliberate act of creating source or machine code that is difficult for humans to understand
Open Systems Interconnect (OSI) model	A model for the design of a network. The open systems interconnect (OSI) model defines groups of functionality required to network computers into layers. Each layer implements a standard protocol to implement its functionality. There are seven layers in the OSI model.
Open Web Application Security Project (OWASP)	An open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted
Operating system (OS)	A master control program that runs the computer and acts as a scheduler and traffic controller Scope Note: The operating system is the first program copied into the computer's memory after the computer is turned on; it must reside in memory at all times. It is the software that interfaces between the computer hardware (disk, keyboard, mouse, network, modem, printer) and the application software (word processor, spreadsheet, e-mail), which also controls access to the devices and is partially responsible for security components and sets the standards for the application programs that run in it.

Term	Definition
Outcome measure	Represents the consequences of actions previously taken; often referred to as a lag indicator Scope Note: Outcome measure frequently focuses on results at the end of a time period and characterize historic performance. They are also referred to as a key goal indicator (KGI) and used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called "lag indicators."
Outsourcing	A formal agreement with a third party to perform IS or other business functions for an enterprise
Packet	Data unit that is routed from source to destination in a packet-switched network Scope Note: A packet contains both routing information and data. Transmission Control Protocol/Internet Protocol (TCP/IP) is such a packet-switched network.
Packet filtering	Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules
Packet switching	The process of transmitting messages in convenient pieces that can be reassembled at the destination
Passive response	A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action
Password	A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system
Password cracker	A tool that tests the strength of user passwords by searching for passwords that are easy to guess It repeatedly tries words from specially crafted dictionaries and often also generates thousands (and in some cases, even millions) of permutations of characters, numbers and symbols.
Patch	Fixes to software programming errors and vulnerabilities

Term	Definition
Patch management	An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk Scope Note: Patch management tasks include the following: maintaining current knowledge of available patches; deciding what patches are appropriate for particular systems; ensuring that patches are installed properly; testing systems after installation; and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks. Patches are sometimes ineffective and can sometimes cause more problems than they fix. Patch management experts suggest that system administrators take simple steps to avoid problems, such as performing backups and testing patches on non-critical systems prior to installations. Patch management can be viewed as part of change management.
Payload	The section of fundamental data in a transmission. In malicious software this refers to the section containing the harmful data/code.
Penetration testing	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers
Personal identification number (PIN)	A type of password (i.e., a secret number assigned to an individual) that, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual Scope Note: PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer (EFT) system.
Phishing	This is a type of electronic mail (e-mail) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering Scope Note: Phishing attacks may take the form of masquerading as a lottery organization advising the recipient or the user's bank of a large win; in either case, the intent is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.
Plain old telephone service (POTS)	A wired telecommunications system.
Platform as a Service (PaaS)	Offers the capability to deploy onto the cloud infrastructure customer-created or -acquired applications that are created using programming languages and tools supported by the provider

Term	Definition
Policy	1. Generally, a document that records a high-level principle or course of action that has been decided on The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams. Scope Note: In addition to policy content, policies need to describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured. 2. Overall intention and direction as formally expressed by management Scope Note: COBIT 5 perspective
Port (Port number)	A process or application-specific software element serving as a communication endpoint for the Transport Layer IP protocols (UDP and TCP)
Port scanning	The act of probing a system to identify open ports
Prime number	A natural number greater than 1 that can only be divided by 1 and itself.
Principle of least privilege/access	Controls used to allow the least privilege access needed to complete a task
Privacy	Freedom from unauthorized intrusion or disclosure of information about an individual
Probe	Inspect a network or system to find weak spots
Procedure	A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.
Protocol	The rules by which a network operates and controls the flow and priority of transmissions
Proxy server	A server that acts on behalf of a user Scope Note: Typical proxies accept a connection from a user, make a decision as to whether the user or client IP address is permitted to use the proxy, perhaps perform additional authentication, and complete a connection to a remote destination on behalf of the user.

Term	Definition
Public key encryption	A cryptographic system that uses two keys: one is a public key, which is known to everyone, and the second is a private or secret key, which is only known to the recipient of the message See also Asymmetric Key.
Public key infrastructure (PKI)	A series of processes and technologies for the association of cryptographic keys with the entity to whom those keys were issued
Public switched telephone network (PSTN)	A communications system that sets up a dedicated channel (or circuit) between two points for the duration of the transmission.
Reciprocal agreement	Emergency processing agreement between two or more enterprises with similar equipment or applications Scope Note: Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises.
Recovery	The phase in the incident response plan that ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDOs) or business continuity plan (BCP)
Recovery action	Execution of a response or task according to a written procedure
Recovery point objective (RPO)	Determined based on the acceptable data loss in case of a disruption of operations It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.
Recovery time objective (RTO)	The amount of time allowed for the recovery of a business function or resource after a disaster occurs
Redundant site	A recovery strategy involving the duplication of key IT components, including data or other key business processes, whereby fast recovery can take place
Registered ports	Registered ports--1024 through 49151: Listed by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users
Registration authority (RA)	The individual institution that validates an entity's proof of identity and ownership of a key pair
Regulation	Rules or laws defined and enforced by an authority to regulate conduct
Regulatory requirements	Rules or laws that regulate conduct and that the enterprise must obey to become compliant

Term	Definition
Remediation	After vulnerabilities are identified and assessed, appropriate remediation can take place to mitigate or eliminate the vulnerability
Remote access service (RAS)	Refers to any combination of hardware and software to enable the remote access to tools or information that typically reside on a network of IT devices Scope Note: Originally coined by Microsoft when referring to their built-in NT remote access tools, RAS was a service provided by Windows NT which allowed most of the services that would be available on a network to be accessed over a modem link. Over the years, many vendors have provided both hardware and software solutions to gain remote access to various types of networked information. In fact, most modern routers include a basic RAS capability that can be enabled for any dial-up interface.
Removable media	Any type of storage device that can be removed from the system while is running
Repeaters	A physical layer device that regenerates and propagates electrical signals between two network segments Scope Note: Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) distorted by transmission loss due to reduction of signal strength during transmission (i.e., attenuation)
Replay	The ability to copy a message or stream of messages between two parties and replay (retransmit) them to one or more of the parties
Residual risk	The remaining risk after management has implemented a risk response
Resilience	The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect
Return on investment (ROI)	A measure of operating performance and efficiency, computed in its simplest form by dividing net income by the total investment over the period being considered
Return-oriented attacks	An exploit technique in which the attacker uses control of the call stack to indirectly execute cherry-picked machine instructions immediately prior to the return instruction in subroutines within the existing program code
Risk	The combination of the probability of an event and its consequence. (ISO/IEC 73)
Risk acceptance	If the risk is within the enterprise's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, the enterprise can assume the risk and absorb any losses

Term	Definition
Risk assessment	A process used to identify and evaluate risk and its potential effects Scope Note: Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan. Risk assessments are also used to manage the project delivery and project benefit risk.
Risk avoidance	The process for systematically avoiding risk, constituting one approach to managing risk
Risk management	1. The coordinated activities to direct and control an enterprise with regard to risk Scope Note: In the International Standard, the term "control" is used as a synonym for "measure." (ISO/IEC Guide 73:2002) 2. One of the governance objectives. Entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the enterprise's risk appetite. Scope Note: COBIT 5 perspective
Risk mitigation	The management of risk through the use of countermeasures and controls
Risk reduction	The implementation of controls or countermeasures to reduce the likelihood or impact of a risk to a level within the organization's risk tolerance.
Risk tolerance	The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives
Risk transfer	The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service
Risk treatment	The process of selection and implementation of measures to modify risk (ISO/IEC Guide 73:2002)
Root cause analysis	A process of diagnosis to establish the origins of events, which can be used for learning from consequences, typically from errors and problems
Rootkit	A software suite designed to aid an intruder in gaining unauthorized administrative access to a computer system

Term	Definition
Router	A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the open systems interconnection (OSI) model Scope Note: Networks connected by routers can use different or similar networking protocols. Routers usually are capable of filtering packets based on parameters, such as source addresses, destination addresses, protocol and network applications (ports).
RSA	A public key cryptosystem developed by R. Rivest, A. Shamir and L. Adleman used for both encryption and digital signatures Scope Note: The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the number of the decryption key bits should be greater than 512 bits.
Safeguard	A practice, procedure or mechanism that reduces risk
Secure Electronic Transaction (SET)	A standard that will ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet.
Secure Multipurpose Internet Mail Extensions (S/MIME)	Provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption) to provide a consistent way to send and receive MIME data. (RFC 2311)
Secure Shell (SSH)	Network protocol that uses cryptography to secure communication, remote command line login and remote command execution between two networked computers
Secure Sockets Layer (SSL)	A protocol that is used to transmit private documents through the Internet Scope Note: The SSL protocol uses a private key to encrypt the data that are to be transferred through the SSL connection.
Security as a Service (SecaaS)	The next generation of managed security services dedicated to the delivery, over the Internet, of specialized information-security services.
Security metrics	A standard of measurement used in management of security-related activities
Security perimeter	The boundary that defines the area of security concern and security policy coverage

Term	Definition
Segregation/separation of duties (SoD)	A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets Scope Note: Segregation/separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.
Sensitivity	A measure of the impact that improper disclosure of information may have on an enterprise
Service delivery objective (SDO)	Directly related to the business needs, SDO is the level of services to be reached during the alternate process mode until the normal situation is restored
Service level agreement (SLA)	An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured
Simple Mail Transfer Protocol (SMTP)	The standard electronic mail (e-mail) protocol on the Internet
Single factor authentication (SFA)	Authentication process that requires only the user ID and password to grant access
Smart card	A small electronic device that contains electronic memory, and possibly an embedded integrated circuit Scope Note: Smart cards can be used for a number of purposes including the storage of digital certificates or digital cash, or they can be used as a token to authenticate users.
Sniffing	The process by which data traversing a network are captured or monitored
Social engineering	An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information
Software as a service (SaaS)	Offers the capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).
Source routing specification	A transmission technique where the sender of a packet can specify the route that packet should follow through the network
Spam	Computer-generated messages sent as unsolicited advertising
Spear phishing	An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim
Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system

Term	Definition
Spyware	Software whose purpose is to monitor a computer user's actions (e.g., web sites visited) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user Scope Note: A particularly malicious form of spyware is software that monitors keystrokes to obtain passwords or otherwise gathers sensitive information such as credit card numbers, which it then transmits to a malicious third party. The term has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.
SQL injection	Results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. (MITRE)
Stateful inspection	A firewall architecture that tracks each connection traversing all interfaces of the firewall and makes sure they are valid.
Statutory requirements	Laws created by government institutions
Supervisory control and data acquisition (SCADA)	Systems used to control and monitor industrial and manufacturing processes, and utility facilities
Switches	Typically associated as a data link layer device, switches enable local area network (LAN) segments to be created and interconnected, which has the added benefit of reducing collision domains in Ethernet-based networks.
Symmetric key encryption	System in which a different key (or set of keys) is used by each pair of trading partners to ensure that no one else can read their messages The same key is used for encryption and decryption. See also Private Key Cryptosystem.
System development life cycle (SDLC)	The phases deployed in the development or acquisition of a software system Scope Note: SDLC is an approach used to plan, design, develop, test and implement an application system or a major modification to an application system. Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review, but not the service delivery or benefits realization activities.
System hardening	A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system

Term	Definition
Tangible asset	Any assets that has physical form
Target	Person or asset selected as the aim of an attack
Telnet	Network protocol used to enable remote access to a server computer Scope Note: Commands typed are run on the remote server.
Threat	Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm Scope Note: A potential cause of an unwanted incident (ISO/IEC 13335)
Threat agent	Methods and things used to exploit a vulnerability Scope Note: Examples include determination, capability, motive and resources.
Threat analysis	An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against enterprise assets Scope Note: The threat analysis usually defines the level of threat and the likelihood of it materializing.
Threat event	Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm
Threat vector	The path or route used by the adversary to gain access to the target
Timelines	Chronological graphs where events related to an incident can be mapped to look for relationships in complex cases Scope Note: Timelines can provide simplified visualization for presentation to management and other non-technical audiences.
Token	A device that is used to authenticate a user, typically in addition to a username and password Scope Note: A token is usually a device the size of a credit card that displays a pseudo random number that changes every few minutes.
Topology	The physical layout of how computers are linked together Scope Note: Examples of topology include ring, star and bus.

Term	Definition
Total cost of ownership (TCO)	Includes the original cost of the computer plus the cost of: software, hardware and software upgrades, maintenance, technical support, training, and certain activities performed by users
Transmission Control Protocol (TCP)	A connection-based Internet protocol that supports reliable data transfer connections Scope Note: Packet data are verified using checksums and retransmitted if they are missing or corrupted. The application plays no part in validating the transfer.
Transmission Control Protocol/Internet Protocol (TCP/IP)	Provides the basis for the Internet; a set of communication protocols that encompass media access, packet transport, session communication, file transfer, electronic mail (e-mail), terminal emulation, remote file access and network management
Transport Layer Security (TLS)	A protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. (RFC 2246) Scope Note: Transport Layer Security (TLS) is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.
Triple DES (3DES)	A block cipher created from the Data Encryption Standard (DES) cipher by using it three times
Trojan horse	Purposefully hidden malicious or damaging code within an authorized computer program Scope Note: Unlike viruses, they do not replicate themselves, but they can be just as destructive to a single computer.
Tunnel	The paths that the encapsulated packets follow in an Internet virtual private network (VPN)
Tunnel mode	Used to protect traffic between different networks when traffic must travel through intermediate or untrusted networks. Tunnel mode encapsulates the entire IP packet with and AH or ESP header and an additional IP header.
Two-factor authentication	The use of two independent mechanisms for authentication, (e.g., requiring a smart card and a password) typically the combination of something you know, are or have
Uncertainty	The difficulty of predicting an outcome due to limited knowledge of all components
Uniform resource locator (URL)	The string of characters that form a web address

Term	Definition
User Datagram Protocol (UDP)	A connectionless Internet protocol that is designed for network efficiency and speed at the expense of reliability Scope Note: A data request by the client is served by sending packets without testing to verify whether they actually arrive at the destination, not whether they were corrupted in transit. It is up to the application to determine these factors and request retransmissions.
User interface impersonation	Can be a pop-up ad that impersonates a system dialog, an ad that impersonates a system warning, or an ad that impersonates an application user interface in a mobile device.
User mode	Used for the execution of normal system activities
User provisioning	A process to create, modify, disable and delete user accounts and their profiles across IT infrastructure and business applications
Value	The relative worth or importance of an investment for an enterprise, as perceived by its key stakeholders, expressed as total life cycle benefits net of related costs, adjusted for risk and (in the case of financial value) the time value of money
Vertical defense-in depth	Controls are placed at different system layers – hardware, operating system, application, database or user levels
Virtual local area network (VLAN)	Logical segmentation of a LAN into different broadcast domains Scope Note: A VLAN is set up by configuring ports on a switch, so devices attached to these ports may communicate as if they were attached to the same physical network segment, although the devices are located on different LAN segments. A VLAN is based on logical rather than physical connections.
Virtual private network (VPN)	A secure private network that uses the public telecommunications infrastructure to transmit data Scope Note: In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.
Virtual private network (VPN) concentrator	A system used to establish VPN tunnels and handle large numbers of simultaneous connections. This system provides authentication, authorization and accounting services.
Virtualization	The process of adding a "guest application" and data onto a "virtual server," recognizing that the guest application will ultimately part company from this physical server

Term	Definition
Virus	A program with the ability to reproduce by modifying other programs to include a copy of itself Scope Note: A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network.
Virus signature file	The file of virus patterns that are compared with existing files to determine whether they are infected with a virus or worm
Voice-over Internet Protocol (VoIP)	Also called IP Telephony, Internet Telephony and Broadband Phone, a technology that makes it possible to have a voice conversation over the Internet or over any dedicated Internet Protocol (IP) network instead of over dedicated voice transmission lines
Volatile data	Data that changes frequently and can be lost when the system's power is shut down
Vulnerability	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events
Vulnerability analysis	A process of identifying and classifying vulnerabilities
Vulnerability scanning	An automated process to proactively identify security weaknesses in a network or individual system
Warm site	Similar to a hot site but not fully equipped with all of the necessary hardware needed for recovery
Web hosting	The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites Scope Note: Most hosting is "shared," which means that web sites of multiple companies are on the same server to share/reduce costs.
Web server	Using the client-server model and the World Wide Web's HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.
Well-know ports	Well-known ports--0 through 1023: Controlled and assigned by the Internet Assigned Numbers Authority (IANA), and on most systems can be used only by system (or root) processes or by programs executed by privileged users. The assigned ports use the first portion of the possible port numbers. Initially, these assigned ports were in the range 0-255. Currently, the range for assigned ports managed by the IANA has been expanded to the range 0-1023.
Wide area network (WAN)	A computer network connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmissions that encompass a large region or several countries

Term	Definition
Wi-Fi protected access (WAP)	A class of systems used to secure wireless (Wi-Fi) computer networks. Scope Note: WPA was created in response to several serious weaknesses that researchers found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security with two significant issues. First, either WPA or WPA2 must be enabled and chosen in preference to WEP; WEP is usually presented as the first security choice in most installation instructions. Second, in the "personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical six to eight character passwords users are taught to employ.
Wi-Fi protected access II (WPA2)	Wireless security protocol that supports 802.11i encryption standards to provide greater security. This protocol uses Advanced Encryption Standards (AES) and Temporal Key Integrity Protocol (TKIP) for stronger encryption.
Wired Equivalent Privacy (WEP)	A scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks) Scope Note: Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network (in particular, it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping.
Wireless local area network (WLAN)	Two or more systems networked using a wireless distribution method
Worm	A programmed network attack in which a self-replicating program does not attach itself to programs, but rather spreads independently of users' action
Write blocker	A devices that allows the acquisition of information on a drive without creating the possibility of accidentally damaging the drive
Write protect	The use of hardware or software to prevent data to be overwritten or deleted
Zero-day-exploit	A vulnerability that is exploited before the software creator/vendor is even aware of it's existence