802.1X A standard that defines a framework for centralized port-based authentication.

802.11a A WLAN standard that operates in the 5 GHz frequency band and, by using OFDM, supports speeds up to 54 Mbps.

802.11b A WLAN standard that operates in the 2.4 GHz frequency band and supports speeds up to 11 Mbps.

802.11f A WLAN standard amendment that addressed problems introduced when wireless clients roam from one AP to another.

802.11g A WLAN standard that operates in the 2.4 GHz frequency band and, by using OFDM, supports speeds up to 54 Mbps.

802.11n A WLAN standard that uses several newer concepts to achieve up to 650 Mbps. It does this using channels that are 40 MHz wide, using multiple antennas that allow for up to four spatial streams at a time (a feature called multiple input, multiple output [MIMO]). It can be used in both the 2.4 GHz and 5.0 GHz bands.

802.11ac A WLAN standard operating in the 5.0 GHz band that has multi-station throughput of at least 1 Gbps and single-link throughput of at least 500 Mbps.

802.11ax A WLAN standard that operates in license-exempt bands between 1 and 7.125 GHz, including the 2.4 and 5 GHz bands already in common use as well as the much wider 6 GHz band (5.925–7.125 GHz in the United States).

A record A host record that represents the mapping of a single device to an IPv4 address.

AAAA record A host record that represents the mapping of a single device to an IPv6 address.

accept A risk strategy that involves understanding and accepting the level of risk as well as the cost of damages that can occur.

acceptability The likelihood that users will accept and follow the system.

acceptance testing A type of software testing which ensures that a system will be accepted by the end users.

access control list (ACL) A rule set that can be implemented on a firewall, switch, or other infrastructure device to control access.

access control matrix A table that consists of a list of subjects, a list of objects, and a list of the actions that a subject can take on each object.

access point (AP) A wireless transmitter and receiver that hooks into the wired portion of a network and provides an access point to that network for wireless devices.

accountability The ability to identify entities that have access to or control of cryptographic keys throughout their life cycles.

accuracy The most important characteristic of biometric systems, which indicates how correct the overall readings will be.

active scanner A scanner that can take action to block attacks, such as blocking dangerous IP addresses.

active state A state in which a key may be used to cryptographically protect information (for example, encrypt plaintext or generate a digital signature), to cryptographically process previously protected information (for example, decrypt ciphertext or verify a digital signature), or both.

ActiveX A deprecated server-side Microsoft technology that uses object-oriented programming (OOP) and is based on the Component Object Model (COM) and the Distributed Component Object Model (DCOM).

Ad Hoc mode A WLAN mode in which there is no AP, and the stations communicate directly with one another.

address space layout randomization (ASLR) A technique that can be used to prevent memory attacks.

Advanced Encryption Standard (AES) A symmetric algorithm adopted by the U.S. government as the replacement algorithm for 3DES.

advanced persistent threat (APT)/nation-state A hacking process that targets a specific entity and is carried out over a long period of time. The attacker is usually a group of organized individuals often funded and supported by a nation-state to gain illicit access to another government's information.

Agile A software development approach that is iterative and incremental and in which developers work on small modules.

air gap A form of security created by disconnecting a device from all networks.

Aircrack-ng A set of command-line tools you can use to sniff wireless networks, among other things.

Airplane mode A setting on a mobile device that disables all wireless network connections.

alert fatigue The effect on a security team that occurs when too many false positives (alerts that do not represent threats) are received.

annualized loss expectancy (ALE) The expected risk cost of an annual threat event.

annualized rate of occurrence (ARO) An estimate of how often a given threat might occur annually.

API gateway A device that receives requests from internal and external sources, called "API calls," routes them to the appropriate API or APIs, and receives and delivers the responses to the user or device that made the request.

application allow list A list of allowed applications (with all others excluded).

application block list A list of prohibited applications (with all others allowed).

application programming interface (API) A software interface that handles interactions between multiple software applications or mixed hardware/software intermediaries.

application-specific integrated circuit (ASIC) A circuit that is designed specifically for an application and thus is not a general-purpose chip.

artificial intelligence (AI) The ability of a machine or computer to learn and adapt.

assessment A step in risk management that involves performing either a quantitative or qualitative risk assessment process.

Asset Reporting Format (ARF) A data model that is used to express the transport format of information about assets and the relationships between assets and reports.

asymmetric algorithm An algorithm that uses both a public key and a private, or secret, key. The public key is known by all parties, and the private key is known only by its owner.

Asynchronous JavaScript and XML (AJAX) A group of interrelated web development techniques used on the client side to create asynchronous web applications.

atomicity A characteristic of an online processing system such as a database in which all operations are complete, or the database changes are rolled back.

attack simulator A device or software that automates common attacks and tests network defenses.

attestation A process that allows changes to a user's computer to be detected by authorized parties.

attestation identity key (AIK) Versatile memory that ensures the integrity of an EK.

attribute-based access control (ABAC) An access control system that takes multiple factors or attributes into consideration before authenticating and authorizing an entity.

augmented reality (AR) A program that overlays virtual objects on the real-world environment.

authentication server The centralized device that performs authentication in 802.1X.

authenticator The device through which the supplicant is attempting to access the network in 802.1X.

author identification The process of attempting to determine the author of a piece of software.

autoscaling A technique used in a virtual environment, such as a cloud scenario, in which compute resources can be added and subtracted automatically based on the workloads at hand.

availability The amount or percentage of time a computer system is available for use.

availability zone A unique physical location within a cloud vendor region.

avoid A risk strategy that involves terminating an activity that causes a risk or choosing an alternative that is not as risky.

baseline A reference point that is defined and captured to be used as a future reference.

Bash A shell used to manage Linux/UNIX systems that has been used as the default login shell for most Linux distributions.

Bcrypt A password-hashing function designed based on the Blowfish cipher.

benchmark A reference point that is compared to the baseline to determine whether any security or performance issues exist.

BGP route hijacking An attack in which mechanisms that are used to prevent the routing of traffic through a private network are also used to manipulate the routing in such a way that traffic is directed where the hacker intends.

big data A term for sets of data so large or complex that they cannot be analyzed by using traditional data processing applications.

binding The process of attaching a hard drive through encryption to a particular computer.

Binwalk A tool for searching a given binary image for embedded files and executable code.

biometric device A device that uses physical characteristics to identify a user.

biometric impersonation The process of capturing biometric data and using it to impersonate an individual.

bit splitting A process that involves encrypting data, separating it into pieces, and distributing the pieces across several storage areas.

blob storage A storage model that uses three components: a storage account, a container, and a blob.

block storage A storage model in which data is stored in pieces called blocks and as separate entities. Each block is given a unique identifier, which allows the system to select a block of data wherever it is most convenient.

blockchain A continuously growing list of records, called blocks, that are linked and secured using cryptography.

Bluejacking An attack in which an unsolicited message is sent to a Bluetooth-enabled device, often for the purpose of adding a business card to the victim's contact list.

Bluesnarfing An attack that involves unauthorized access to a device using a Bluetooth connection.

Bluetooth A wireless technology that is used to create personal area networks (PANs), which are short-range connections between devices and peripherals, such as headphones.

bootstrapping The process of bringing an operating system to life; it occurs when the bootstrap code locates and loads the operating system files.

browser extension A small program or script that increases the functionality of a website.

buffer A portion of system memory that is used to store information.

buffer overflow An attack that occurs when the amount of data that is submitted is larger than the buffer can handle.

Building Automation and Control Network (BACnet) An application, network, and media access control (MAC) layer communications service that can operate over a number of layer 2 protocols, including Ethernet.

business continuity plan (BCP) A process that focuses on sustaining an organization's mission/business processes during and after a disruption.

business impact analysis (BIA) The process of identifying mission critical systems and identifying measures to provide fault tolerance and high availability.

bytecode Code generated by compiling source code which can be executed by a virtual machine.

caching Storing information that is frequently used by systems for future use.

Capability Maturity Model Integration (CMMI) A process improvement approach.

certificate authority (CA) An entity that creates and signs digital certificates, maintains the certificates, and revokes them when necessary.

certificate revocation list (CRL) A list of digital certificates that a CA has revoked.

certificate signing request (CSR) A request that a self-generated certificate be validated and signed by a CA.

ChaCha A modification of Salsa20 published in 2008 that avoids the possibility of timing attacks in software implementations.

chain of custody Documentation that shows who controlled the evidence, who secured the evidence, and who obtained the evidence.

change management The process used to vet and approve all suggested changes.

character class One of four types of characters: numbers, nonnumeric characters, uppercase, and lowercase.

checklist test A test in which managers of each department or functional area review the BCP and make note of any modifications to the plan.

Children's Online Privacy Protection Act (COPPA) A law that addresses abuse of children on the Internet.

choose your own device (CYOD) A strategy in which organization users choose their own devices from a list of options but the devices are purchased, owned, and managed by the organization.

cipher block chaining (CBC) A DES mode in which 64-bit blocks are chained together and each resultant 64-bit ciphertext block is applied to the next block.

Class 1 certificate A certificate used for individuals and intended for email.

Class 2 certificate A certificate used by organizations that must provide proof of identity.

Class 3 certificate A certificate used by servers and software signing in which independent verification and identity and authority checking is done by the issuing CA.

Class 4 certificate A certificate used for online business transactions between companies.

Class 5 certificate A certificate used by private organizations or for government security.

clearing A removal technique which ensures that the data cannot be reconstructed using normal file recovery techniques and tools.

click-jacking An attack in which a transparent page or frame is crafted over a legitimate-looking page that entices the user to click something. When he does, he is really clicking on a different URL.

client-based application virtualization (application streaming) Virtualization in which the target application is packaged and streamed to the client PC.

clone An exact bit-for-bit copy of everything on a hard drive.

cloud backup An increasingly popular backup method that involves backing up data to a cloud location.

clustering The use of hardware and software to provide load balancing services.

CNAME record An alias record that represents an additional hostname mapped to an IPv4 address that already has an A record mapped.

code signing The process of digitally signing executables and scripts so that the user installing the code can be assured that it comes from the verified author.

cognitive password A password that is a piece of information that can be used to verify an individual's identity. The user provides this information to the system by answering a series of questions based on her life, such as favorite color, pet's name, mother's maiden name, and so on.

cold site A leased facility that contains only electrical and communications wiring, air conditioning, plumbing, and raised flooring.

combination password A password, also called a composition password, that uses a mix of dictionary words—usually two that are unrelated.

command injection An attempt to execute an operating system command.

commodity malware Malware that is widely available either for purchase or as a free download.

Common Configuration Enumeration (CCE) A set of best practice statements maintained by the National Institute of Standards and Technology (NIST).

Common Criteria (CC) A standardized rating system that assess security of products.

Common Industrial Protocol (CIP) A suite of messages and services for the collection of manufacturing automation applications.

Common Name (CN) The entity name protected by an SSL/TLS certificate, which is technically represented by the Common Name field in the X.509 certificate specification.

Common Platform Enumeration (CPE) A naming scheme for describing and classifying operating systems, applications, and hardware devices used by SCAP.

Common Vulnerabilities and Exposures (CVE) A free MITRE database that lists vulnerabilities in published operating systems and application software as identified by Common Platform Enumeration (CPE).

Common Vulnerability Scoring System (CVSS) A system of ranking vulnerabilities that are discovered based on predefined metrics.

communications analysis The process of analyzing communication over a network by capturing all or part of the communication and searching for particular types of activity.

community cloud A cloud computing model in which the cloud infrastructure is shared among several organizations from a specific group with common computing needs.

compensative control A control that is in place to substitute for a primary access control and mainly help mitigate risks.

complex password A password that includes a mixture of upper- and lowercase letters, numbers, and special characters.

compromised state A state in which keys are released to or determined compromised by an unauthorized entity.

confidentiality Assurance that data is protected from unauthorized access.

configuration identification The process of breaking down an operation into individual configuration items (CIs).

configuration item (CI) A uniquely identifiable subset of a system that represents the smallest portion to be subject to an independent configuration control procedure.

configuration lockdown A setting that prevents any changes to the configuration, even by users who formerly had the right to configure the device.

configuration management A process that focuses on bringing order out of the chaos that can occur when multiple engineers and technicians have administrative access to the computers and devices that make a network function.

configuration management database (CMDB) A database that keeps track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships between such assets.

conntrack A set of free software tools for GNU/Linux that allows system administrators to interact, from user space, with the in-kernel Connection Tracking.

container A virtualization technique in which the kernel allows for multiple isolated user space instances. The instances are known as containers, virtual private servers, or virtual environments.

containerization Server virtualization in which the kernel allows for multiple isolated user space instances. The instances are known as containers, virtual private servers, or virtual environments. Also a feature of most mobile device management (MDM) software that creates an encrypted "container" to hold and quarantine corporate data separately from that of the users.

containment The process of performing countermeasures to stop a data breach in its tracks.

content analysis The process of analyzing the contents of a drive and giving a report detailing the types of data, by percentage, or analyzing the content of software, particularly malware, to determine the purpose for which the software was created.

content delivery network (CDN) A set of geographically dispersed servers that serve content to users based on their location, so that users get content from the physically nearest server.

Content Security Policy (CSP) header An HTTP header that enables precise control of content sources.

context analysis The process of analyzing the environment that software was found in to discover clues related to determining risk.

continuity of operations plan (COOP) A plan that focuses on restoring an organization's mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations.

continuity planning Planning that deals with identifying the impact of any disaster and ensuring that a viable recovery plan for each function and system is implemented.

continuous delivery (CD) The ability to make software features, configuration changes, bug fixes, and experiments available to users safely and quickly and in a sustainable way.

continuous delivery pipeline (CDP) The workflows needed to introduce new functionality to software, from ideation to an on-demand release of value to the end user.

continuous integration (CI) The practice of merging all software developer working copies into a shared main line several times a day.

continuous lighting An array of lights that provide an even amount of illumination across an area.

control A measure or technique that reduces either the likelihood or the impact of a security issue.

control plane The part of a network that carries signaling traffic originating from or destined for a router or switch.

Controller Area Network (CAN) bus A newer standard for vehicle-to-vehicle and vehicle-to-road communication.

copyright A mark which ensures that a work that is authored is protected from any form of reproduction or use without the consent of the copyright holder.

corporate-owned, personally enabled (COPE) A strategy in which an organization purchases mobile devices, and users manage those devices.

corrective control A control that is in place to reduce the effect of an attack or another undesirable event.

COSOs Enterprise Risk Management (ERM) Integrated Framework An ERM framework presented in the form of a three-dimensional matrix.

counter (CTR) A DES mode that uses an incrementing IV counter to ensure that each block is encrypted with a unique keystream.

credentialed scan A scan that is performed by someone with administrative rights to the host being scanned.

Crime Prevention Through Environmental Design (CPTED) A multi-disciplinary approach to security that involves designing a facility from the ground up to support security.

crisis communications plan A plan that documents standard procedures for internal and external communications in the event of a disruption.

critical infrastructure protection (CIP) plan A set of policies and procedures that serve to protect and recover these assets and mitigate risks and vulnerabilities.

cross-certification The process of establishing trust relationships between certification authorities (CAs) so that the participating CAs can rely on the other participants' digital certificates and public keys.

cross-certification model A federation model in which each organization certifies that every other organization is trusted. This trust is established when the organizations review each other's standards.

cross-site request forgery (CSRF) An attack that causes an end user to execute unwanted actions on a web application in which he or she is currently authenticated.

cross-site scripting (XSS) An attack in which an attacker locates a website vulnerability and injects malicious code into the web application.

crossover error rate (CER) The point at which FRR equals FAR.

cryptanalysis The study of encryption algorithms with the intent of discovering how the algorithm may be attacked or compromised.

crypto shredding A method of making encrypted data permanently unavailable by deleting or overwriting the key used to decrypt it.

cryptographic service provider (CSP) A software library that implements the Microsoft CryptoAPI (CAPI) in Windows.

customer relationship management (CRM) Software that identifies customers and stores customer-related data, particularly contact information and data on any direct contacts with customers.

cyber incident response plan A plan that establishes procedures to address cyber attacks against an organization's information system(s).

Cyber Kill Chain A cyber intrusion identification and prevention model developed by Lockheed Martin that describes the stages of an intrusion.

data anonymization The process of deleting or masking personal identifiers, such as personal names from a set of data.

data at rest Refers to data that is stored physically in any digital form that is not active.

data custodian A person who implements information classification and controls after they are determined by the data owner.

data dispersion A technique that is commonly used to improve data security—but without encryption. It involves rearranging data across multiple disks, much as RAID does, but in a way that enhances security.

Data Distribution Service Middleware that operates between an operating system and applications. It is an API standard for data-centric connectivity from the Object Management Group, and it addresses applications that require real-time data exchange.

data exfiltration The inadvertent or purposeful escape of sensitive data from a network.

data haven A country that fails to legally protect personal data.

data in process/data in use Data that is being accessed or manipulated in some way.

data in transit Refers to data that is transmitted over the Internet or another network.

data inventory and mapping A process typically using software tools to enumerate all the data, regardless of where it might be stored or which department uses it.

data loss prevention (DLP) Software that uses ingress and egress filters to identify sensitive data that is leaving the organization and can prevent such leakage.

data masking Altering data from its original state to protect it.

data owner A person whose main responsibility is to determine the classification level of information and the control applied.

data plane Also known as the forwarding plane, the part of a network that carries user traffic.

data processing pipeline An operation performed on a piece of data.

data remnants Data that is left behind on a computer or another resource when that resource is no longer used.

data sovereignty The idea that information that has been converted and stored in binary digital form is subject to the laws of the country in which it is located.

data zone A segmentation technique used in big data architectures.

database activity monitoring (DAM) The use of tools to monitor transactions and the activity of database services.

database storage A storage model in which data is typically stored in a server as ordered and unordered flat files, ISAM, heaps, hash buckets, or B+ trees.

dd A UNIX/Linux command that is used to convert and copy files.

de facto standard A standard that is widely accepted but not formally adopted.

de jure standard A standard that is based on law or regulation and that is adopted by international standards organizations.

deactivated state A state in which keys in the deactivated state are not used to apply cryptographic protection, but in some cases, they may be used to process cryptographically protected information.

decoy file A file that triggers an alert when accessed.

deep fake Synthetic media that impersonates a real person’s appearance and speech.

deep learning A form of machine learning that uses artificial neural networks and representational learning.

deep packet inspection The process used to identify data types that should not be on a network as well as data types that should not be leaving the network.

deep web Parts of the internet that can only be located and accessed via a direct URL or IP address.

dependency A relationship that exists between code in different software libraries.

dependency management The process of identifying all dependencies of code from a library.

deprovisioning The process of removing a resource from a network.

destroyed phase A stage in the key life cycle in which keys are no longer available.

destroyed state A state in which a key has been destroyed as specified in the destroyed phase.

destruction A removal technique that involves destroying the media on which data resides.

detective control A control that is in place to detect an attack while it is occurring and alert appropriate personnel.

deterrent control A control that is in place to deter or discourage an attacker.

DevOps A software development method that aims at shorter development cycles, increased deployment frequency, and more dependable releases, in close alignment with business objectives.

DevSecOps A development approach that involves representatives from development, operations, and security to create a shared sense of responsibility with regard to security.

Diameter A protocol that might be considered an upgrade to RADIUS. It adds additional commands that support EAP and operates at the application layer.

Diamond Model of Intrusion Analysis A model that emphasizes the relationships between and characteristics of four basic components: the adversary, capabilities, infrastructure, and victims.

differential backup A backup in which all files that have been changed since the last full backup are backed up.

Diffie-Hellman A widely used key agreement process.

dig A Linux command that is used to troubleshoot DNS.

digital rights management (DRM) Technology used by hardware manufacturers, publishers, copyright holders, and individuals to control the use of digital content.

digital signature A hash value encrypted with the sender's private key. A digital signature provides authentication, non-repudiation, and integrity.

Digital Signature Standard (DSS) A U.S. federal digital security standard that governs the Digital Security Algorithm (DSA).

digital watermarking Embedding a logo or trademark in documents, pictures, or other objects. The watermark deters people from using the materials in an unauthorized manner.

directory service A service that stores, organizes, and provides access to information in a computer operating system's directory.

directory traversal The process of breaking out of the web root folder in order to access restricted directories and execute commands outside of the web server's root directory.

disaster recovery plan (DRP) An information system–focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency.

discretionary access control (DAC) An access control system in which the owner of an object specifies which subjects can access the resource.

disk imaging The process of creating an exact image of the contents of a hard drive.

distributed consensus The process whereby distributed nodes reach agreement or consensus on the validity of transactions.

distributed DoS (DDoS) attack A DoS attack that is carried out from multiple attack locations.

Distributed Network Protocol 3 (DNP3) A primary/secondary protocol that uses port 19999 when using Transport Layer Security (TLS) and port 20000 when not using TLS. Its main use is in utilities such as electric and water companies.

diversity Use of multiple types and models of security appliances, security protocols, encryption algorithms, and operating systems. Also called heterogeneity.

DNS harvesting A process that involves acquiring the DNS records of an organization to use in mapping the network.

DNS over HTTPS (DoH) A method of transmitting DNS traffic to remote DNS servers using the Secure HTTPS protocol.

Domain Name System (DNS) A database that provides a hierarchical naming system for computers, services, and any resources connected to the Internet or a private network.

Domain Name System Security Extensions (DNSSEC) A secure form of DNS which ensures that a DNS server is authenticated before the transfer of DNS information begins between the DNS server and the client.

downgrade attack An attack in which the attacker convinces the system to use an older, lower-quality mode of operation (for example, plaintext) that is typically provided for backward compatibility with older systems.

due care A process an organization goes through to prevent security issues or to mitigate damage if security breaches occur.

due diligence A process an organization takes to understand the security risks it faces.

Dumpster diving An attack that involves examining the contents of physical garbage cans or recycling bins to obtain confidential information, including personnel information, account login information, network diagrams, and organizational financial data.

dynamic analysis The process of testing software while it is running.

dynamic application security testing (DAST) A form of testing that is automated.

dynamic network configurations tool A tool that uses preconfigured configurations to constantly affirm the secure configuration of devices.

Dynamic Trunking Protocol (DTP) A protocol that enables two switches to form a trunk link automatically, based on their configuration.

e-discovery The exchange of evidence recovered from electronic devices.

eFuse A tool used to help secure a stolen device.

electronic codebook (ECB) The easiest and fastest DES mode to use. It has security issues because every 64-bit block is encrypted with the same key.

electronic vaulting A backup method that involves copying files as modifications occur in real time.

elliptic-curve cryptography (ECC) An approach to public key cryptography that is based on the algebraic structure of elliptic curves over finite fields.

Elliptic-Curve Diffie-Hellman (ECDH) A key agreement protocol that uses an elliptic-curve public/private key pair to establish a symmetric key over an insecure channel.

Elliptic-Curve Digital Signature Algorithm (ECDSA) An algorithm that provides elliptical-curve-based key exchange.

email code review A type of code review in which code is emailed around to colleagues for them to review when time permits.

email spoofing The process of sending an email that appears to come from one source when it really comes from another.

embedded system A piece of software that is built into a larger piece of software and is in charge of performing some specific function on behalf of the larger system.

emergency lighting Lighting systems with their own power source to use when power is out.

emulator Software that changes the CPU instructions required for the architecture and executes them on another architecture successfully. Also a code processor that enables a host system to run software or use peripheral devices designed for the guest system in a virtual environment.

end-of-life A software or hardware product that is deemed by its creator to be no longer for sale.

end-of-support A software or hardware product that is no longer supported by its creator.

endorsement key (EK) Persistent memory installed by a manufacturer that contains a public/private key pair.

endpoint detection and response (EDR) A proactive endpoint security approach that is designed to supplement existing defenses.

enrollment time The process of obtaining a sample that is used by a biometric system.

enterprise resource planning (ERP) A process that involves collecting, storing, managing, and interpreting data from product planning, product cost, manufacturing or service delivery, marketing/sales, inventory management, shipping, payment, and any other business processes.

enterprise service bus (ESB) A software platform used to facilitate communication between mutually interacting software applications in an SOA.

erasure coding The process of breaking data into fragments and expanding and encoding the fragments with a configurable number of redundant pieces of data and storing them across different locations, allowing for the failure of two or more elements of a storage array.

ExifTool Open-source software that can be used to read and edit file metadata.

exploit framework A tool that provides a consistent environment to create and run exploit code against a target.

export control A rule and regulation governing the shipment or transmission of items from one country to another.

exposure factor (EF) The percentage value or functionality of an asset that will be lost when a threat event occurs.

Extended Validation (EV) certificate A certificate that requires verification of the requesting entity's legal identity before the certificate can be issued.

Extensible Access Control Markup Language (XACML) A standard for an access control policy language using XML. Its goal is to create an attribute-based access control (ABAC) system that decouples the access decision from the application or the local machine.

Extensible Authentication Protocol (EAP) A framework for port-based access control that uses the same three components that are used in RADIUS.

Extensible Configuration Checklist Description Format (XCCDF) A specification language for writing security checklists, benchmarks, and related kinds of documents that is used by Security Content Automation Protocol.

Extensible Markup Language (XML) A markup language that is often used in web deployments.

extension The designation at the end of a file that describes the purpose of the certificate.

facial scan A biometric scan that records facial characteristics, including bone structure, eye width, and forehead size.

false acceptance rate (FAR) A measurement of the percentage of invalid users that will be falsely accepted by the system.

false negative A test result that incorrectly indicates that a vulnerability does not exist. False means the scanner is wrong, and negative means it did not find a vulnerability.

false positive A test result that incorrectly identifies a vulnerability that does not exist. False means the scanner was incorrect, and positive means it identified a vulnerability.

false rejection rate (FRR) A measurement of valid users that will be falsely rejected by the system.

fault tolerance The ability of a system to continue operating properly when components within the system fail.

feature extraction An approach to obtaining biometric information from a collected sample of a user's physiological or behavioral characteristics.

federated identity A portable identity that can be used across businesses and domains.

Federation of European Risk Management Associations (FERMA) Risk Management Standard An organization that provides guidelines for managing risk in an organization.

field-programmable gate array (FPGA) A type of programmable logic device (PLD) that is programmed by blowing fuse connections on the chip or using an antifuse that makes a connection when a high voltage is applied to the junction.

fielding The process of making software available for sale or use.

file-based storage A storage model in which files are stored in folders or directories

file carving The process of reassembling computer files from fragments in the absence of file system metadata.

file integrity monitoring (FIM) Methods of ensuring that files have not been altered by an unauthorized person or application.

finger scan A type of scan that extracts only certain features from a fingerprint.

fingerprint scan A type of scan that usually examines the ridges of a finger for a match.

firmware A type of instruction stored in non-volatile memory devices such as read-only memory (ROM), electrically erasable programmable read-only memory (EPROM), or Flash memory.

first-in, first-out (FIFO) A tape rotation scheme in which the newest backup is saved to the oldest media

foremost A command that recovers files for Linux systems.

Forensic Toolkit (FTK) Imager A tool for taking images of forensic data, without making changes to the original evidence.

formal methods Methods of software engineering that use mathematical models.

formal review An extremely thorough, line-by-line inspection, usually performed by multiple participants using multiple phases.

full backup A backup in which all data is backed up.

full interruption test A test that involves shutting down the primary facility and bringing up the alternate facility to full operation.

function as a service (FaaS) An extension of PaaS that completely abstracts the virtual server from the developer.

fuzz testing The process of injecting invalid or unexpected input (sometimes called faults) into an application to test how the application reacts.

Galois/Counter Mode (GCM) A DES mode in which blocks are numbered sequentially, and then a block number is combined with an initialization vector (IV) and encrypted with a block cipher, usually AES.

General Data Protection Regulation (GDPR) Regulatory guidelines required by the European Union.

generation-based fuzzing A type of fuzzing that involves generating inputs from scratch, based on the specification/format.

geofencing The application of geographic limits to where a device can be used.

geotagging The process of adding geographic metadata (a form of geospatial metadata) to various media, including photographs, videos, websites, SMS messages, or RSS feeds.

Ghidra A software reverse engineering (SRE) suite of tools developed by the NSA's Research Directorate.

GNU Privacy Guard (GPG) A rewrite or upgrade of PGP that uses AES.

GNU Project debugger (GDB) A tool that allows visibility into a program while it executes or determines what the program was doing at the moment it crashed.

grandfather/father/son (GFS) A tape rotation scheme in which three sets of backups are defined. Most often these three definitions are daily, weekly, and monthly. The daily backups are the sons, the weekly backups are the fathers, and the monthly backups are the grandfathers. Each week, one son advances to the father set

graphical password A password that uses graphics as part of the authentication mechanism. Also called a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) password.

guest environment Resources provided to a virtual machine by a virtualization hypervisor.

hacktivist An activist for a cause, perhaps for animal rights, who uses hacking as a means to get their message out and affect the businesses that they feel are detrimental to their cause.

hand geometry scan A type of scan that usually obtains size, shape, or other layout attributes of a user's hand but can also measure bone length or finger length.

hand topography scan A type of scan that records the peaks and valleys of the hand and its shape.

hardware password manager A small physical device that stores a password file offline so it is not on the hard drive.

hardware security module (HSM) An appliance that safeguards and manages digital keys used with strong authentication and provides crypto processing.

hash-based message authentication code (HMAC) A keyed-hash MAC that involves a hash function with a symmetric key. HMAC provides data integrity and authentication.

hashing Running data through a cryptographic function to produce a one-way message digest. Because the message digest is unique, it can be used to check data integrity.

hexdump A Linux utility that is a filter which displays the specified files, or standard input if no files are specified, in a user-specified format.

hierarchical storage management (HSM) A backup method that involves storing frequently accessed data on faster media and less frequently accessed data on slower media.

historian server A server that receives, parses, and saves data and commands transmitted across programmable logic controllers (PLCs), sensors, and actuators.

history A policy that specifies the amount of time that must elapse before an expired password can be reused.

homomorphic encryption A form of encryption that is unique in that it allows computation on ciphertexts, generating an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

honeypot A system that is configured with reduced security to entice attackers so that administrators can learn about attack techniques.

horizontal privilege escalation A form of privilege escalation in which a normal user accesses functions or content reserved for other normal users.

hot site A leased facility that contains all the resources needed for full operation.

HMAC-based one-time password (HOTP) An algorithm that computes a password from a shared secret that is used one time only. It uses an incrementing counter that is synchronized on the client and the server to do this.

HTTP interceptor A device or software that intercepts and examines web traffic between a browser and a website.

HTTP Strict Transport Security (HSTS) A policy mechanism that informs web browsers (or other user agents) that they should automatically interact with it using only HTTPS connections.

HTTP Strict Transport Security (HSTS) header An HTTP header that enforces the use of encrypted HTTPS connections instead of plaintext HTTP communication.

human intelligence (HUMINT) Any information gathered via person-to-person contact.

hunt teaming A relatively new approach to security that is offensive in nature rather than defensive.

hybrid cloud A cloud computing model in which an organization provides and manages some resources in-house and has others provided externally via a public cloud.

hybrid SDN A combination of both traditional networking and SDN protocols operating in the same environment.

Hypertext Markup Language 5 (HTML5) The latest version of Hypertext Markup Language (HTML), a standardized system for tagging text files to apply web formatting.

hypervisor Software that manages the distribution of resources (CPU, memory, and disk) to the virtual machines in a virtual environment.

identify A step in risk management that involves identifying assets, the value of assets, and vulnerabilities.

identity proofing An additional step in the identification portion of authentication. Also called two-step verification.

identity theft An attack in which someone obtains personal information—such as driver's license number, bank account number, or Social Security number—and uses that information to assume the identity of the individual whose information was stolen.

immutable system A system that is never updated but that is completely replaced with a new server built from a common image when the appropriate changes are provisioned to replace the old one.

impact A measurement of the damage a particular risk event will cause an organization.

in-band Describes a direct connection to the network.

incident response The process of detecting and reacting to security events.

incident response plan A plan created to identify and respond to security incidents.

incremental backup A backup in which up all files that have been changed since the last full or incremental backup.

indicator of compromise (IoC) Any activity, artifact, or log entry that is typically associated with an attack of some sort.

industrial control system (ICS) A general term that encompasses several types of control systems used in industrial production.

information security gap analysis An audit that compares an organization's security program to overall best security practices.

Information Sharing and Analysis Centers (ISACs) Nonprofit organizations that host security information sharing systems.

information system contingency plan (ISCP) A plan that provides established procedures for the assessment and recovery of a system following a system disruption.

infrastructure as a service (IaaS) A cloud service model in which the vendor provides the hardware platform or data center, and the company installs and manages its own operating systems and application systems.

Infrastructure mode A WLAN mode in which all transmissions between stations go through the AP, and no direct communication occurs between stations.

inherent risk The level of risk before mitigation factors or treatments are applied.

input validation The process of checking all input for things such as proper format and proper length.

insider threat Someone who has knowledge of and access to systems that outsiders do not have and who therefore has a much easier avenue for carrying out or participating in an attack. An organization should implement the appropriate event collection and log review policies to provide the means to detect insider threats as they occur.

integer overflow An attack in which math operations try to create a numeric value that is too large for the available space.

integration testing A type of software testing that assesses the way in which the modules work together and determines whether functional and security specifications have been met.

integrity Assurance that data is protected from unauthorized modification or data corruption.

intellectual property A tangible or intangible asset to which an owner has exclusive rights.

intelligence feed An RSS feed dedicated to the sharing of information about the latest vulnerabilities.

interactive application security testing (IAST) A form of testing in which the tester interacts with the system.

interconnection security agreement (ISA) An agreement between two organizations that own and operate connected IT systems to document the technical requirements of the interconnection.

interface testing A type of testing that evaluates whether an application's systems or components correctly pass data and control to one another.

Internet Message Access Protocol (IMAP) An application layer protocol used on a client to retrieve email from a server.

Internet Protocol Security (IPsec) A suite of protocols that establishes a secure channel between two devices.

Internet of Things (IoT) A system of interrelated computing devices, mechanical and digital machines, and objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

interpretation A code processing method that involves analyzing a source instruction, performing the required operation, and moving to the next source instruction.

intrusion detection system (IDS) A system responsible for detecting unauthorized access or attacks against systems and networks.

intrusion prevention systems (IPS) A system that is responsible for preventing attacks.

iptables A common host-based firewall on Linux-based systems.

iris scan A biometric scan that records the colored portion of the eye, including all rifts, coronas, and furrows.

ISO/IEC 27000 A security program development standard on how to develop and maintain an information security management system (ISMS).

jailbreaking The process of removing the security restrictions on an iPhone or iPad.

job rotation An administrative control in which multiple users are trained to perform the duties of a position to help prevent fraud by any individual employee.

JSON Web Token (JWT) A proposed Internet standard that uses signed tokens to communicate with previously established authentication information in an SSO environment.

jump box A server that is used to access devices that have been placed in a secure network zone such as a screened subnet (DMZ).

Kerberos The authentication and authorization system used in UNIX and Windows AD.

key agreement A type of algorithm that negotiates the creation of a shared symmetric key for encryption.

key escrow The process of storing keys with a third party to ensure that decryption can occur.

key management The process of ensuring that keys are protected during creation, distribution, transmission, and storage.

key performance indicator (KPI) A metric that is created, collected, and analyzed to assess performance.

key recovery The process whereby a key is archived in a safe place

key risk indicator (KRI) A metric that is created, collected, and analyzed to assess risk.

key stretching A cryptographic technique, also referred to as key strengthening, that involves making a weak key stronger by increasing the time it takes to test each possible key.

key-value pair A pair of related values that are used in the search process to locate data as an alternative to rows and tables in a database.

keystroke dynamics A system that measures the typing pattern a user uses when inputting a password or other predetermined phrase.

ladder logic A type of programming language for PLCs that is more visual than many other programming languages.

Layer 2 Tunneling Protocol (L2TP) A newer protocol that operates at layer 2 of the OSI model. Like PPTP, L2TP can use various authentication mechanisms; however, L2TP does not provide any encryption. It is typically used with Internet Protocol Security (IPsec), which is a very strong encryption mechanism.

LDAP injection A situation in which queries made to locate an item are constructed from untrusted input without prior validation or sanitization.

ldd A utility that prints the shared libraries required by each program or shared library specified on the command line.

legal hold The requirement that an organization maintain archived data for longer periods.

Lightweight Directory Access Protocol (LDAP) A common directory services standard.

lightweight review A type of code review that is much more cursory than a formal review.

likelihood A measurement of the chance that a particular risk event will impact an organization.

load balancer A hardware or software product that provides load-balancing services.

local area network (LAN) A network that comprises a set of devices that reside in the same IP subnet.

log analysis The process of analyzing network traffic logs.

lsof A command that lists all open files.

MAC filter A filter that allows and disallows devices based on their MAC addresses.

machine code Code written in machine language or binary that can be directly executed by a CPU.

machine learning (ML) The use of generated training data to build a model that makes predictions and decisions without being explicitly programmed to do so.

managed security service provider (MSSP) A provider that offers the option to fully outsource all information assurance to a third party.

management plane The part of a network that administers a router or switch.

mandatory access control (MAC) An access control system in which subject authorization is based on security labels.

mandatory vacations A policy that requires all personnel to take time off, allowing other personnel to fill their positions while gone. This detective administrative control enhances the opportunity to discover unusual activity.

master service agreement (MSA) A contract between two parties in which both parties agree to most of the terms that will govern future transactions or future agreements.

mean time between failures (MTBF) The estimated amount of time a device will operate before a failure occurs.

mean time to recovery (MTTR) The average time required to repair a single resource or function when a disaster or disruption occurs.

measured boot A boot process in which software and platform components have been identified, or "measured," using cryptographic techniques.

memorandum of understanding (MOU) An agreement between two or more organizations that details a common line of action.

memory card A swipe card that is issued to a valid user. The card contains user authentication information.

memory snapshot A copy of the contents of RAM.

message digest (MD) A family of hashing algorithms.

metadata Information about a piece of data. This information can be assigned as a key word or term and stored in a tag.

microsegmentation A method of creating zones in data centers and cloud environments to isolate workloads from one another and secure them individually.

middleware A layer of software that acts as a bridge between an operating system and a database or an application.

mission critical Describes functions that, if missing, will impact the organizations' ability to do business.

misuse case testing A type of application testing which ensures that the application can handle invalid input or unexpected behavior.

mitigate A risk strategy that involves defining the acceptable risk level an organization can tolerate and reducing the risk to that level.

MITRE Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) A knowledge base of adversarial tactics and techniques based on real-world observations.

MITRE ATT&CK for Industrial Control Systems (ICS) A MITRE knowledge base that focuses specifically on industrial control systems (ICSs).

mobile site A recovery site located in a truck or trailer that can be moved where it is needed and provides its own power, Internet connection, and cell tower.

Modbus A protocol used in industrial control systems that was created by Modicon (now Schneider Electric) to be used by its PLCs.

movable lighting Lighting that can be repositioned as needed.

multidomain certificate A certificate that can represent multiple domains with a single certificate.

multifactor authentication (MFA) Authentication in which authentication factors from at least two different factor categories are used—for example, a PIN (knowledge factor), a retina scan (characteristic factor), and signature dynamics (behavioral factor).

Multipurpose Internet Mail Extensions (MIME) An Internet standard that allows email to include non-text attachments, non-ASCII character sets, multiple-part message bodies, and non-ASCII header information.

multitenancy model A cloud computing model in which multiple organizations share the resources.

mutation fuzzing A type of fuzzing that involves changing the existing input values (blindly).

MX record A mail exchanger record that represents an email server mapped to an IPv4 address.

nano technology The use of matter on atomic, molecular, and supramolecular scales for industrial purposes.

natural access control A concept that applies to the entrances of a facility that encourages the idea of creating security zones in the building.

natural surveillance The use of physical environmental features to promote visibility in all areas and thus discourage crime in those areas.

natural territorial reinforcement A design principle whose goal is to create a feeling of community in the area.

nc (netcat) A command-line utility that can be used for many investigative operations, including port scanning, file transfers, and port listening.

near-field communication (NFC) A set of communication protocols that allow two electronic devices, one of which is usually a mobile device, to establish communication when they are within 2 inches of each other.

net present value (NPV) A function that considers the fact that money spent today is worth more than savings realized tomorrow.

NetFlow Cisco software that captures network flows (that is, conversations or sessions that share certain characteristics) between two devices.

netstat (network status) A command that is used to see what ports are listening on a TCP/IP-based system.

network access control (NAC) A service that goes beyond authentication of the user and includes examination of the state of the computer the user is introducing to the network when making a remote access or VPN connection to the network.

network address translation (NAT) A service that can be supplied by a router or by a server that translates public IP addresses to private IP addresses and vice versa.

network enumerator A device that scans a network and gathers information about users, groups, shares, and services that are visible, in a process sometimes referred to as device fingerprinting.

network IDS (NIDS) An IDS that monitors network traffic on a local network segment.

network IPS (NIPS) An IPS that scans traffic on a network for signs of malicious activity and takes some action to prevent it.

network tap A network monitoring device that is directly attached to a network that all traffic flows through.

next-generation firewall (NGFW) A type of firewall that attempts to address the traffic inspection and application-awareness shortcomings of a traditional stateful firewall—without hampering performance.

NIST 800 series A set of documents that describe U.S. federal government computer security policies, procedures, and guidelines.

NIST Framework for Improving Critical Infrastructure Cybersecurity A NIST cybersecurity risk framework.

NIST SP 800-37 Rev. 1 A NIST publication that defines the tasks that should be carried out in each step of the risk management framework.

NIST SP 800-39 A NIST publication that provides guidance for an integrated organizationwide program for managing information security risk to organizational operations.

NIST SP 800-53 Rev. 4 A security control development framework developed by the U.S. NIST.

NIST SP 800-160 A NIST publication that defines the systems security engineering framework.

non-credentialed scan A scan that is performed by someone without administrative rights to the host being scanned.

non-disclosure agreement (NDA) An agreement between two parties that defines what information is considered confidential and cannot be shared outside the two parties.

non-persistent agent An agent that is installed and run as needed on an endpoint.

non-repudiation Assurance that a sender cannot deny an action.

NS record A name server record that represents a DNS server mapped to an IPv4 address.

nslookup A command-line administrative tool for testing and troubleshooting DNS servers.

numeric password A password that includes only numbers.

NX (no-execute) bit Technology used in CPUs to segregate areas of memory for use by either storage of processor instructions (code) or storage of data.

obfuscation The process of making something obscure, unclear, or unintelligible. When we use that term with respect to sensitive or private information, it refers to changing the information in some way to make it unreadable to unauthorized individuals.

objdump A command-line program for displaying information about object files on UNIX-like operating systems.

object storage A storage model that uses a flat structure in which files are broken into parts and spread out among hardware.

occupant emergency plan A plan that outlines first-response procedures for occupants of a facility in the event of a threat or an incident to the health and safety of personnel, the environment, or property.

OCSP stapling An alternative to using OCSP.

OllyDbg A 32-bit, assembler-level analyzing debugger for Microsoft Windows.

one-time password (OTP) A password that is used only once to log in to the access control system. This password type provides the highest level of security because it is discarded after it is used once. Also called a dynamic password.

Online Certificate Status Protocol (OCSP) An Internet protocol that obtains the revocation status of an X.509 digital certificate by using the serial number.

Open Authorization (OAuth) A standard for authorization that allows users to share private resources on one site to another site without using credentials.

open SDN A decentralized, IT community-based approach to SDN.

open-source intelligence (OSINT) Data collected from publicly available sources.

Open Source Security Testing Methodology Manual (OSSTMM) A manual that covers different kinds of security tests of physical, human (processes), and communication systems.

Open System Authentication (OSA) The default authentication used in 802.11 networks using WEP. The authentication request contains only the station ID and authentication response.

Open Vulnerability and Assessment Language (OVAL) A standardized method used to transfer security information across the entire spectrum of security tools and services.

Open Web Application Security Project (OWASP) A group that monitors web attacks.

OpenID An open standard and decentralized protocol from the nonprofit OpenID Foundation that allows users to be authenticated by certain cooperating sites.

operational intelligence Intelligence that is gathered to develop a response. It is less passive than strategic intelligence and involves more effort on the part of the organization but yields better information.

operational-level agreement (OLA) An internal organizational document that details the relationships that exist between departments to support business activities.

operational phase A stage in the key life cycle in which the keying material is available and in normal use. Keys are in the active or suspended state.

optical jukebox A backup method that involves storing data on optical discs and using robotics to load and unload the optical discs as needed. This method is ideal when 24/7 availability is required

order of volatility The order in which evidence should be collected, starting with the most volatile evidence.

organized crime Groups that primarily threaten the financial services sector and are expanding the scope of their attacks. They perpetrate well-funded attacks.

out-of-band Describes a connection to a device that does not use the network.

output feedback (OFB) A DES mode that uses a previous keystream with a key to create the next keystream.

over-the-air update An update that occurs over a wireless connection.

over-the-shoulder A type of code review in which coworkers review the code, and the author explains his or her reasoning.

overflow A condition in which an area where something is stored gets full and additional information leaks over to another area.

packet capture The process of using capture tools to collect raw packets from a network.

packet-filtering firewall A firewall that inspects only the header of a packet for allowed IP addresses or port numbers.

pair programming A type of code review in which two coders work side-by-side, checking one another’s work as they go.

palm or hand scan A type of scan that combines fingerprint and hand geometry technologies. It records fingerprint information from every finger as well as hand geometry information.

parallel test A test that involves bringing the recovery site to a state of operational readiness but maintaining operations at the primary site.

passive scanner A scanner that can only gather information.

passphrase password A password that uses a long phrase. Because of the password's length, it is easier to remember but much harder to attack, both of which are definite advantages.

Password-Based Key Derivation Function 2 (PBKDF2) An encryption mechanism that basically uses a password and manipulates it to generate a strong key that can be used for encryption and subsequently decryption.

password cracker A program that attempts to identify passwords.

password repository application A tool that secures the location of passwords and helps in their management.

passwordless authentication An authentication method that does not rely on the use of passwords.

patent Protection granted to an individual or a company for an invention.

path tracing Tracing the path of a particular traffic packet or traffic type to discover the route used by the attacker.

payback A simple calculation that compares ALE against the expected savings resulting from an investment.

Payment Card Industry Data Security Standard (PCI DSS) A security standard that enumerates requirements that payment card industry players should meet to secure and monitor their networks, protect cardholder data, manage vulnerabilities, implement strong access controls, and maintain security policies.

peer-to-peer network A network in which each device is an autonomous security entity; the devices have no domain or network association with one another.

peering A voluntary interconnection of two separate networks for the purpose of exchanging traffic directly between the users of the networks.

perfect forward secrecy (PFS) A process which ensures that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.

persistent agent An agent that is installed on an endpoint and waits to be called into action.

personally identifiable information (PII) A piece of data that can be used alone or with other information to identify a particular person.

pharming An attack that involves polluting the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site.

phishing A social engineering attack in which attackers try to learn personal information, including credit card information and financial data.

pivoting A technique used by hackers and pen testers to advance from an initially compromised host to other hosts on the same network.

platform as a service (PaaS) A cloud service model in which the vendor provides the hardware platform or data center and the software running on the platform, including the operating systems and infrastructure software. The company is still involved in managing the system.

platform configuration register (PCR) hash Versatile memory that stores data hashes for the sealing function.

Point-to-Point Tunneling Protocol (PPTP) A Microsoft protocol based on PPP that uses built-in Microsoft Point-to-Point encryption and can use a number of authentication methods, including CHAP, MS-CHAP, and EAP-TLS.

Poly1305 A cryptographic message authentication code (MAC) that can verify the data integrity and the authenticity of a message.

port mirroring The process of capturing and duplicating the stream of packets traversing one port to another port.

port scanner A device or software used to scan a network for open ports.

Post Office Protocol (POP) An application layer email retrieval protocol.

post-operational phase A stage in the key life cycle in which the keying material is no longer in normal use, but access to the keying material is possible, and the keying material may be used for processing only in certain circumstances.

PowerShell A powerful tool built into all Windows systems that can automate tasks and can be used to script configuration changes.

pre-activation state A state in which a key has been generated but has not been authorized for use.

preescalation tasks Tasks that should precede the escalation of a security event.

preferred roaming list (PRL) A list of radio frequencies that resides in the memory of some kinds of digital phones.

pre-operational phase A stage in the key life cycle in which the keying material is not yet available for normal cryptographic operations.

preserved The process of ensuring that evidence is not subject to damage or destruction.

Pretty Good Privacy (PGP) An encryption system that provides email encryption over the Internet can provide confidentiality, integrity, and authentication, depending on the encryption methods used.

principle of least privilege A policy that requires a user or process to be given only the minimum access privilege needed to perform a particular task.

privacy impact assessment A process that identifies all data types that require privacy protections (PII, PHI, work records, medical records) and attempts to assess the impact of a breach involving those data types.

privacy-level agreement (PLA) A document that sets out in contractual terms how a third-party provider will ensure that the information it hosts will not be seen by the wrong sets of eyes.

private cloud A cloud computing model in which a private organization implements a cloud in its internal enterprise.

private function evaluation (PFE) The process of evaluating one party's private data using a private function owned by another party.

private information retrieval (PIR) A type of protocol that can retrieve information from a server without revealing which item is retrieved.

privilege escalation The process of exploiting a bug or weakness in an operating system to allow a user to receive privileges to which she is not entitled.

Process Explorer A tool in Sysinternals that enables you to look at the graph that appears in Task Manager and identify what caused spikes in the past. This is not possible with Task Manager alone.

process injection A method of executing arbitrary code in the address space of a separate live process.

processing pipeline A discrete step that can represent an algorithm, a software tool, or a file format manipulation. Pipelines use the output of one element as the input of the next one.

product release information (PRI) A connection between a mobile device and a radio.

programmable logic device (PLD) An integrated circuit with connections or internal logic gates that can be changed through a programming process.

protective control A control that is designed to protect an asset or prevent an issue from occurring.

protocol analyzer A device that can capture raw data frames from a network. Also called a sniffer.

provisioning The process of adding a resource to a network.

proxy firewall A firewall that stands between the internal and external sides of an internal-to-external connection and makes the connection on behalf of the endpoints

ps A Linux command for viewing the processes running on a system.

public cloud The standard cloud computing model, in which a service provider makes resources available to the public over the Internet.

public key infrastructure (PKI) The set of systems, software, and communication protocols that distribute, manage, and control public key cryptography.

public key pinning A security mechanism delivered via an HTTP header that allows HTTPS websites to resist impersonation by attackers using mis-issued or otherwise fraudulent certificates.

purging A removal technique that involves making data unreadable even with advanced forensic techniques.

Python A scripting language whose design philosophy emphasizes code readability. Python code, which is written and stored as scripts with the file extension.py, can be executed to perform a task.

qualitative risk analysis Risk analysis that does not assign monetary and numeric values to all facets of the risk analysis process.

quantitative risk analysis Risk analysis that assigns monetary and numeric values to all facets of the risk analysis process, including asset value, threat frequency, vulnerability severity, impact, and safeguard costs.

quantum computing The use of quantum states, such as superposition and entanglement, to perform computation.

race condition An attack in which the hacker inserts himself between instructions, introduces changes, and alters the order of execution of the instructions, thereby altering the outcome.

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) A hashing algorithm that produces a 160-bit hash value after performing 160 rounds of computations on 512-bit blocks.

RAID A hard drive technology in which data is written across multiple disks in such a way that a disk can fail, and the data can be quickly made available by remaking disks in the array without resorting to a backup tape.

RAID 0 Also called disk striping, a RAID method that writes the data across multiple drives. While it improves performance, it does not provide fault tolerance.

RAID 1 Also called disk mirroring, a RAID method that uses two disks and writes a copy of the data to both disks, providing fault tolerance in the event of a single drive failure.

RAID 3 A RAID method that requires at least three drives, writes the data across all drives, and then writes parity information to a single dedicated drive. The parity information is used to regenerate the data in the event of a single drive failure.

RAID 5 A RAID method that requires at least three drives, writes the data across all drives, and then writes parity information across all drives as well. The parity information is used in the same way as in RAID 3, but it is not stored on a single drive, so there is no single point of failure for the parity data.

RAID 7 A proprietary RAID implementation that incorporates the same principles as RAID 5 but enables the drive array to continue to operate if any disk or any path to any disk fails. The multiple disks in the array operate as a single virtual disk.

RAID 10 A RAID method that combines RAID 1 and RAID 0 and requires a minimum of four disks. However, most implementations of RAID 10 involve four or more drives. A RAID 10 deployment contains a striped disk that is mirrored on a separate striped disk.

ransomware Malware that prevents or limits users from accessing their systems. The attackers force victims to pay a ransom using certain online payment methods if they want to be given access to their systems again or get their data back.

readelf A command in the GNU Binary Utilities, a set of programming tools for creating and managing binary programs. As the name implies, it is used to read elf files.

real user monitoring (RUM) A monitoring method that captures and analyzes every transaction of every application or website user.

recovery control A control that is in place to recover a system or device after an attack has occurred.

recovery service level A level of service that an organization strives to provide after an outage.

region A segmentation method used by a cloud provider to organize the physical locations of the various data centers where customer data resides.

registration authority (RA) A server that verifies a requester's identity and registers the requester.

regression A situation in which a software change by developers reduces either the security or the functionality of the software.

regression testing A type of software testing which catches bugs that may have been accidentally introduced into the new build or release candidate.

regular expression A sequence of characters that specifies a search pattern. Characters can be one of two types: special characters that are not to be taken literally but have special meaning or function (that is, metacharacters) and special characters that are taken literally.

regulatory requirement Any requirement that must be documented and followed based on laws and regulations.

relevant In the context of evidence, the quality of proving a material fact related to a crime by showing that a crime has been committed, providing information describing the crime, providing information regarding the perpetuator's motives, or verifying what occurred.

reliable In the context of evidence, the quality of ensuring freedom from tampering or modification.

reliability The ability of a control to perform as expected on a constant basis.

Remote Authentication Dial-in User Service (RADIUS) A networking protocol that provides centralized authentication and authorization.

Remote Desktop Protocol (RDP) A proprietary protocol developed by Microsoft that provides a graphical interface to connect to another computer over a network connection.

remote terminal unit (RTU) A device in an ICS that connects to sensors and converts sensor data to digital data, including telemetry hardware.

remote journaling A backup method that involves copying the journal or transaction log offsite on a regular schedule, in batches.

remote wipe An instruction sent remotely to a mobile device to erase all the data, typically used when a device is lost or stolen.

replication The process of copying data from one storage location to another.

representational state transfer (REST) A client/server model for interacting with content on remote systems, typically using HTTP.

residual risk The level of risk that remains after safeguards or controls have been implemented.

resiliency The ability of a system or group of systems to continue to operate at an acceptable level when system faults or failures occur or when the workload soars.

retina scan A type of scan that examines the retina's blood vessel pattern.

return on investment (ROI) The money gained or lost after an organization makes an investment.

reverse engineering Using tools to break down hardware or software to understand its purpose and how to defeat it. Also the process of retrieving the source code of a program to study how the program performs certain operations.

reverse proxy A type of proxy server that retrieves resources on behalf of external clients from one or more internal servers.

reversible encryption Encryption of passwords that can be reversed. It is required by some applications but is not secure.

review A step in risk management that involves a follow-up review to ensure that all security gaps have at least been narrowed if not eliminated.

risk appetite The level of exposure or risk that an organization views as acceptable.

risk assessment A tool used in risk management to identify vulnerabilities and threats, assess the impact of those vulnerabilities and threats, and determine which controls to implement.

risk management life cycle Best practice steps involved in risk management.

risk register A document or piece of software that is used to record assets, vulnerabilities, efforts to address vulnerabilities, and the result of such efforts.

risk tolerance The degree of variance from an organization's risk appetite that the organization is willing to tolerate.

Rivest, Shamir, and Adleman (RSA) The most popular asymmetric algorithm.

role-based access control (RBAC) An access control system in which each subject is assigned to one or more roles. Roles are hierarchical, and access control is defined based on the roles.

root of trust The foundation of assurance of the trustworthiness of a device.

rooting The process of removing security restrictions on an Android device.

router A device that uses a routing table to determine in which direction to send traffic destined for a particular network.

runbook A manual list of steps to take to address a specific issue or vulnerability or an automated script or program that takes the same steps.

rule-based access control An access control system that facilitates frequent changes to data permissions. Using this method, a security policy is based on global rules imposed for all users.

safe harbor An entity that conforms to all the requirements of the EU Principles on Privacy.

safety instrumented system A system that has sensors, logic solvers, and final control elements for the single purpose of taking the process to a safe state when predetermined conditions are violated.

Salsa20 A stream cipher that avoids the possibility of timing attacks in software implementations.

sandbox detonation A preventive approach in which a security team intentionally sets of, or execution (that is, detonated) the payload of a malicious file to determine what it will do and how to address it.

sandbox escape A situation that occurs when a VM breaks out of a sandbox.

sandboxing Limiting the parts of the operating system and user an application is allowed to interact with.

scalability A characteristic of a device or security solution that describes its capability to cope and perform under an increased or expanding workload.

scaling horizontally Adding additional systems to process the workload. Also known as scaling out.

scaling vertically Increasing the capacity of a single machine by adding more resources, such as memory or CPU. Also known as scaling up.

scope of work A list of the exact tasks that testers will perform on a network.

screened subnet An architecture with a subnet between two firewalls that can act as a DMZ for resources from the outside world.

script kiddie A hacker who has relatively little knowledge of hacking and uses prepackaged tools or scripts created by others.

scrubbing A process used to maintain data quality and/or to remove private data. Also deleting incriminating data from an audit log.

SDN overlay A deployment method that involves running a logically separate network or network component on top of existing infrastructure. The SDN network overlay tunnels through the physical network.

sealing The process of locking the system state to a particular hardware and software configuration to prevent attackers from making any changes to the system.

secure boot One of several technologies that follow the Secure Boot standard. Its implementations include Windows Secure Boot, measured launch, and Integrity Measurement Architecture (IMA).

secure by default Secure without changes to any default settings.

secure by deployment Secure because the environment into which an application is introduced was considered from a security standpoint.

secure by design Secure because the design process was approached from a security standpoint.

secure coding standards Practices that, if followed throughout the software development life cycle, help reduce the attack surface of an application.

secure enclave A part of an operating system that cannot be compromised even when the operating system kernel is compromised because the enclave has its own CPU and is separated from the rest of the system.

secure function evaluation (SFE) The process in which multiple parties collectively compute a function and receive its output without learning the inputs from any other party.

Secure Hashing Algorithm (SHA) A family of four algorithms published by the U.S. NIST.

Secure MIME (S/MIME) A secure version of MIME that encrypts and digitally signs email messages and encrypts attachments.

Secure/Multipurpose Internet Mail Extensions (S/MIME) A protocol that allows MIME to encrypt and digitally sign email messages and encrypt attachments.

Secure Shell (SSH) A protocol created to provide an encrypted method of performing remote command-line operations.

Secure Sockets Layer (SSL) A protocol used to create secure connections to servers. It works at the application layer of the OSI model. It is used mainly to protect HTTP/HTTPS traffic or web servers.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) A protocol used for creating secure connections to servers. It can provide confidentiality authentication and integrity services.

Secured Memory A feature that allows for a partition to be designated as a security-sensitive or a non-security-sensitive partition.

Security Assertion Markup Language (SAML) A security attestation model built on XML and SOAP-based services that allows for the exchange of authentication and authorization data between systems and that supports federated identity management.

Security Content Automation Protocol (SCAP) A standard that the security automation community uses to enumerate software flaws and configuration issues.

Security-Enhanced Android (SEAndroid) An SELinux version that runs on Android devices.

Security-Enhanced Linux (SELinux) A Linux kernel security module that separates enforcement of security decisions from the security policy itself and streamlines the amount of software involved with security policy enforcement.

security information and event management (SIEM) A system that provides log centralization and an automated solution for analyzing events.

Security Orchestration, Automation, and Response (SOAR) The use of technologies used to accomplish automation and orchestration in performing mundane tasks that are crucial to identifying and responding to security issues.

security requirements traceability matrix (SRTM) A grid that documents the security requirements that a new asset must meet.

Security Trust Assurance and Risk (STAR) Registry A list of cloud providers that have met the requirements laid out by the Cloud Security Alliance (CSA).

segmentation A technique used to partition off sections of a network so that each section might be treated differently, and access control can be implemented to control cross-segment traffic.

self-encrypting drive A drive that encrypts itself without any user intervention.

self-healing hardware A system deployed with multiple instances of certain hardware components (power supplies, network cards, CPUs, etc.) and the ability to switch over to a backup component when a main component fails.

Sender Policy Framework (SPF) An email validation system that works by using Domain Name System (DNS) to determine whether an email sent by someone has been sent by a host sanctioned by that domain's administrator.

sensor A device that is designed to gather information of some sort and make it available to a larger system. Also a device in an ICS that has digital or analog I/O but not in a form that can be easily communicated over long distances.

separation of duties A policy that prevents fraud by distributing tasks and their associated rights and privileges among users.

server-based application virtualization (terminal services) Virtualization in which an application runs on servers. Users receive the application environment display through a remote client protocol.

service-level agreement (SLA) An agreement to respond to problems within a certain time frame while providing an agreed level of service.

service-oriented architecture (SOA) A style of software design that involves using software to provide application functionality as services to other applications.

service set identifier (SSID) A name or value assigned to identify a WLAN from other WLANs.

Sha256sum A tool that is designed to verify data integrity using SHA-256. SHA-256 hashes, when used properly, can confirm both file integrity and authenticity.

Shared Key Authentication (SKA) A verification process that uses WEP and a shared secret key for authentication. The challenge text is encrypted with WEP using the shared secret key.

shell restriction Access control via a software interface to an operating system that limits the system commands that are available.

Shibboleth An open-source project that provides single sign-on capabilities and allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

shoulder surfing An attack in which someone watches when a user enters login or other confidential data.

side-channel analysis Analysis that allows an attacker to infer information about a process by observing nonfunctional characteristics of a program, such as execution time or memory consumed.

side loading A method of installing applications on a mobile device from a computer rather than from an app store, such as Google Play or the Apple App Store.

signature dynamics A system that measures stroke speed, pen pressure, and acceleration and deceleration while the user writes his signature.

signature rule A rule used by antimalware and vulnerability scanning systems to locate and quarantine certain files, as identified by their signatures.

Simple Certificate Enrollment Protocol (SCEP) A protocol that is used in provisioning certificates to network devices, including mobile devices.

Simple Mail Transfer Protocol (SMTP) A standard application layer protocol that is used by clients to send email.

Simple Network Management Protocol (SNMP) An application layer protocol that is used to retrieve information from network devices and to send configuration changes to those devices.

Simple Object Access Protocol (SOAP) A protocol specification for exchanging structured information in the implementation of web services in computer networks.

simulation test A test in which the operations and support personnel execute the DRP in a role-playing scenario.

single loss expectancy (SLE) The monetary impact of a threat occurrence.

single sign-on (SSO) A service in which a single password yields access to all resources and systems.

single-tenancy model A cloud computing model in which a single tenant uses a resource.

slack space analysis The process of analyzing the slack (marked as empty or reusable) space on a drive to see whether any old (marked for deletion) data can be retrieved.

The Sleuth Kit A collection of command-line tools that are used in the digital forensics process.

smart card A card, often known as an integrated circuit card (ICC), that contains memory like a memory card and also contains an embedded chip like a debit or credit card.

SOA record A Start of Authority record that represents a DNS server that is authoritative for a DNS namespace.

social engineering An attack that involves gaining the trust of a user and in some way convincing him or her to reveal sensitive information such as a password or to commit other actions that reduce the security of the network.

software as a service (SaaS) A cloud service model in which the vendor provides the entire solution, including the operating system, the infrastructure software, and the application.

software composition analysis (SCA) The process of performing automated scans of an application’s code base, including related artifacts such as containers and registries, to identify

all open-source components, their license compliance data, and any security vulnerabilities and fix vulnerabilities through prioritization and auto remediation.

software-defined networking (SDN) The decoupling of the control plane and the data plane in networking.

software library A controlled area that is accessible only to approved users who are restricted to the use of an approved procedure.

spam Unsolicited emails.

spear phishing The process of carrying out a phishing attack on a specific person rather than on a random set of people. The attack may be made more convincing by using details about the person.

spiral model A software development approach which assumes that knowledge gained at each iteration is incorporated into the design as it evolves.

SQL injection An attack that inserts, or injects, a SQL query as the input data from the client to the application.

ssdeep A tool that performs fuzzy hashing, a form of hashing that is the key to finding new malware that looks like something that has been seen previously.

staging environment A production-like environment used to see how developed code will perform.

standard A suggested action or rule that is tactical in nature, meaning that it provides the steps necessary to achieve security.

standard software library A library that contains common objects and functions used by a language that developers can access and reuse.

standard word password A password that consists of a single word that often includes a mixture of upper- and lowercase letters.

standby lighting A type of system that illuminates only at certain times or on a schedule.

stateful firewall A firewall that is aware of the proper functioning of the TCP handshake, keeps track of the state of all connections with respect to this process, and can recognize when packets trying to enter the network don’t make sense in the context of the TCP handshake.

stateful NAT (SNAT) A service that implements two or more NAT devices to work together as a translation group. It is called stateful NAT because it maintains a table about the communication sessions between internal and external systems.

static analysis The process of testing or examining software when it is not running.

static application security testing (SAST) A form of testing that is performed with the application not running.

static password A password that is the same for each login. It provides a minimum level of security because the password never changes.

steganography analysis The process of analyzing the graphic files on a drive to see whether the files have been altered or to discover the encryption used on the files. Data can be hidden within graphic files or hidden by other means.

storage key Versatile memory that contains the keys used to encrypt a computer's storage, including hard drives, USB flash drives, and so on.

storage root key (SRK) Persistent memory that secures the keys stored in a TPM chip.

strace A system call tracer for Linux/UNIX that can be used to monitor and tamper with interactions between processes and the Linux kernel.

strategic intelligence Intelligence that is gathered on a global scale.

streaming pipeline A sequence of elements supporting sequential and parallel aggregate operation. Commonly used in Java.

Strings2 A Windows 32-bit and 64-bit command-line tool for extracting strings from binary data.

Subject Alternative Name (SAN) An extension to the X.509 specification that allows users to specify additional host names for a single SSL/TLS certificate.

subordinate or intermediate CA One of a number of servers that are spread out geographically to issue certificates cosigned by the root server.

supervisory control and data acquisition (SCADA) A system that operates with coded signals over communication channels to provide control of remote equipment.

supplicant The user or device requesting access to the network in 802.1X.

supply chain access A type of attack that takes advantage of the weakest cybersecurity link and often begins with an advanced persistent threat (APT) during the manufacturing process of an electronic product in order to ultimately cause harm to a target customer or company.

suspended state A state in which the use of a key or a key pair may be suspended for several possible reasons; in the case of asymmetric key pairs, both the public and private keys are suspended at the same time.

symmetric algorithm An algorithm that uses a private, or secret, key that must remain secret between the two parties. Each party pair requires a separate private key.

synthetic transaction monitoring A type of testing in which external agents run scripted transactions against an application.

system on a chip (SoC) Software contained on a chip such as a baseband processor in a network interface that manages radio functions.

System File Checker (SFC) A command-line utility that checks and verifies the versions of system files on a computer.

switched port analyzer (SPAN) port A port that has been configured to include mirrored traffic from other ports on a switch.

tabletop exercise An informal brainstorming session that works best with participation from business leaders and other key employees. The participants agree to a particular disaster scenario upon which they will focus.

tactical threat information Information on threats that can be considered local in nature.

tape vaulting A backup method that involves creating backups over a direct communication line on a backup system at an offsite facility.

targeted attack An attack that presents a threat to a single organization and typically involves preparation and direct involvement of the attacker.

Task Manager A tool used to determine what process is causing a bottleneck in performance .

tcpdump A command that captures packets on Linux and UNIX platforms.

telemetry system A system in an ICS that connects RTUs and PLCs to control centers and the enterprise.

template A collection of security settings used to standardize the settings across many systems.

Terminal Access Controller Access Control System (TACACS) A networking protocol that provides centralized authentication and authorization.

test coverage analysis A type of analysist that looks at the percentage of test cases that were run, that passed, and that failed.

tethering A process in which one mobile device is connected to another mobile device for the purpose of using the Internet connection.

threat emulation The process of simulating an attack to see how the security system in place reacts.

threat hunting A relatively active form of threat identification that involves meeting the attackers at the point of attack

throughput rate The rate at which a biometric system will be able to scan characteristics and complete the analysis to permit or deny access.

time-based one-time password (TOTP) An algorithm that computes a password from a shared secret and the current time. It is based on HOTP but turns the current time into an integer-based counter.

time of check to time of use An attack in which a system is changed between a condition check and the display of the check's results.

token device A handheld device that presents the authentication server with a one-time password (OTP).

tokenization A data obfuscation method that substitutes a sensitive value in the data with another value that is not sensitive.

tool-assisted A type of code review that uses automated testing tools and is perhaps the most efficient method.

total cost of ownership (TCO) A measure of the overall costs associated with running an organizational risk management process, including insurance premiums, finance costs, administrative costs, and any losses incurred.

TPM chip A security chip installed on a computer's motherboard that is responsible for protecting symmetric and asymmetric keys, hashes, and digital certificates. This chip provides services to protect passwords and encrypt drives and digital rights, making it much harder for attackers to gain access to the computers that have TPM chips enabled.

tracert A utility that traces the path of a packet from its source to its destination.

trade secret Intellectual property (for example, recipe, formula, ingredient listing) that gives an organization a competitive edge.

trademark A mark which ensures that a symbol, a sound, or an expression that identifies a product or an organization is protected from being used by another organization.

traffic mirroring The process of capturing and duplicating the stream of packets traversing an interface.

transfer A risk strategy that involves passing the risk on to a third party, such as an insurance company.

transitive trust A trust relationship in which if entity A trusts entity B, and entity B trusts entity C, then entity A trusts domain C.

triage event A security event that comprises gathering information about an event and using all available log files and alerts to determine as much as possible about the source of the event and its characteristics.

Triple Digital Encryption Standard (3DES) The replacement algorithm for DES.

true negative A test that correctly determines that a vulnerability does not exist. True means the scanner is correct, and negative means it did not identify a vulnerability.

true positive A test that correctly identifies a vulnerability. True means the scanner was correct, and positive means it identified a vulnerability.

trunk link A link between switches and between routers and switches that carry the traffic of multiple VLANs.

trust model A model that defines which entities are trusted in a federation.

trusted third-party (or bridge) model A federation model in which each organization subscribes to the standards of a third party. The third party manages verification, certification, and due diligence for all organizations.

tshark A command that captures packets on Linux and UNIX platforms, much as **tcpdump** does.

two-factor authentication (2FA) Authentication in which authentication factors from two different factor categories are used—for example, a password (knowledge factor) and an iris scan (characteristic factor).

Type 1 hypervisor A hypervisor installed on bare metal.

Type 2 hypervisor A hypervisor installed on top of an operating system.

Unified Extensible Firmware Interface (UEFI) An alternative to BIOS for interfacing between the software and the firmware of a system.

unified threat management (UTM) A solution in which devices perform multiple security functions. For example, antivirus, firewalling, and network access control may all be provided by a single device.

unit testing A type of software testing in which each module is tested separately.

usability The ease of using a security solution or device.

user acceptance testing A type of software testing which ensures that the customer (either internal or external) is satisfied with the functionality of the software.

user and entity behavior analytics (UEBA) A type of analysis that focuses on observing network behaviors for anomalies.

validation testing A type of software testing which ensures that a system meets the requirements defined by the client.

vascular scan A type of scan that examines the pattern of veins in the user's hand or face.

vendor lock-in A scenario in which an organization is unable to switch CSPs because the cost of doing so outweighs the benefits.

vendor lock-out A scenario in which an organization is unable to migrate to another cloud provider due to the complexity or cost of a migration.

versioning A numbering system which helps ensure that developers are working with the latest software versions and eventually that users are using the latest version.

vertical privilege escalation A form of privilege escalation in which a lower-privilege user or application accesses functions or content reserved for higher-privilege users or applications.

virtual desktop infrastructure (VDI) A server-based virtualization technology that hosts and manages virtual desktops. Functions include creating the desktop images, managing the desktops on the servers, and providing client network access for the desktop.

virtual local area network (VLAN) A separate network created on a switch.

virtual machine (VM) An instance of an operating system in a virtual environment.

virtual machine (VM) hopping The process of compromising one VM and then pivoting or moving laterally to attack another VM.

virtual private cloud (VPC) A cloud that is used for safe traffic analysis and that utilizes traffic mirroring in that process.

virtual private network (VPN) A connection that uses an untrusted carrier network but provides protection of the information through strong authentication protocols and encryption mechanisms.

virtual reality (VR) A program that immerses users in a fully artificial digital environment.

virtualization The act of creating a virtual device on a physical resource; a physical resource can hold more than one virtual device.

virtualization support A feature that can be enabled to provide many benefits, such as improved performance.

VLAN hopping An attack that enables a device in one VLAN to obtain traffic destined for another VLAN

VM escape An attack in which the attacker "breaks out" of a VM's normally isolated state and interacts directly with the hypervisor.

vmstat A built-in monitoring utility in Linux that is typically used to help identify performance bottlenecks and diagnose problems and that can also be used in the same way as the **ps** command to identify malicious processes.

voice pattern or print A system that measures the sound pattern of a user saying certain words.

Volatility A tool for collecting volatile data. It is free tool used to record information held in RAM.

VPC peering A connection created directly between two virtual private clouds that makes it possible to route traffic between the clouds using private IPv4 addresses or IPv6 addresses.

vulnerability An absence of a countermeasure or a weakness of a countermeasure that is in place.

vulnerability scanner A device or software that can probe for a variety of security weaknesses, including misconfigurations, out-of-date software, missing patches, and open ports.

walk-through test A test in which representatives of each department or functional area thoroughly review the BCP's accuracy.

Waterfall model A software development approach that breaks up the software development process into distinct phases. It is a somewhat rigid approach that sees the process as a sequential series of steps that are followed without going back to earlier steps.

Web Services Security (WSSecurity or WSS) An extension to SOAP that is used to apply security to web services.

warm site A leased facility that contains electrical and communications wiring, full utilities, and networking equipment.

whaling A spear phishing attack that targets a person who is of significance or importance, such as a CEO, COO, or CTO.

Wi-Fi Protected Access (WPA) An alternative security mechanism that is designed to improve on WEP.

Wi-Fi Protected Access 2 (WPA2) An improvement over WPA that uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) and is based on the Advanced Encryption Standard (AES), rather than TKIP.

wildcard certificate A public key certificate that can be used with multiple subdomains of a domain.

Wired Equivalent Privacy (WEP) The first security measure used with 802.11.

wireless intrusion detection system (WIDS) An IDS that operates on a WLAN rather than on a wired network.

Wireshark A widely used sniffer that captures raw packets from the interface on which it is configured and allows you to examine each packet.

WPA3 A WLAN standard that offers improved security over WPA2.

X-Frame-Options header An HTTP header that prevents the current page from being loaded into any iframes to prevent cross-site scripting attacks.

XML gateway An externally facing screened subnet (DMZ) tier of a web services platform that handles communication.

XN (execute never) bit A method for specifying areas of memory that cannot be used for execution.

Zigbee An IEEE 802.15.4-based specification that is used to create personal area networks (PANs) with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power, low-bandwidth needs.