Table des matières

An access control list (ACL)

1. **Recommended:** An access control list (ACL) contains rules that grant or deny access to certain digital environments. (Source)
2. Alternative 1: A setting in a network device that dictates where it's allowed to pass traffic to and from. (Source)
3. Alternative 2: An Access Control Lists "ACL is a function that watches incoming and outgoing traffic and compares it with a set of defined statements. (Source)

Access control mechanism

1. **Recommended:** Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. Source
2. Alternative 1: Security safeguards designed to detect and deny unauthorized access and permit authorized access to an information system. Source
3. Alternative 2: Implementations of formal AC policy such as AC model. Access control mechanisms can be designed to adhere to the properties of the model by machine implementation using protocols, architecture, or formal languages such as program code. Source

Access control

1. **Recommended:** Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources. Secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users Source
2. Alternative: Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources. Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data. Access control can also be applied to limit physical access to campuses, buildings, rooms, and datacenters Source

Access

1. **Recommended:** Ability to make use of any information system (IS) resource Source
2. Alternative 1: Access, in the context of security, is the privilege or assigned permission to use computer data or resources in some manner. For instance, a user may be allowed read access to a file, but will not be allowed to edit or delete it Source
3. Alternative 2: To make contact with one or more discrete functions of an online, digital service Source

Account Management

1. **Recommended:** A mechanism that implements access control for a system resource by

enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity Source

2. Alternative 1: Account management is one of the most important aspects of an organization’s security posture. Not only do the decisions affect how users interact with their network and systems, but account management embodies many key security principles. Therefore, understanding the range of account types as well as how to employ and manage each is a foundational skill of Security+ professionals Source
3. Alternative 2: The Account Management Standard provides requirements around creating and maintaining user and special accounts. The primary audience for the standard is account administrators. However, there are reporting requirements pertaining to personnel and roles and responsibility changes for managers as well Source

Accountability

1. **Recommended:** The principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information Source
2. Alternative 1: Being the one who has to get something done. The accountable person is where the buck stops in the event of failure. Only one person can be accountable for any one task or goal Source
3. Alternative 2: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action Source

Accreditation

1. **Recommended:** Formal recognition by an assessor that an individual or organisation has attained an agreed, recognised standard of qualification, behaviour or adherence to specific definitions and/or standards. As a verb, the action of the assessor awarding an accreditation. In the sense of the UK Cyber Security Council, a quality assurance process recognising the minimum standards required for the quality of an educational curriculum. Source
2. Alternative 1: Accreditation is the external recognition of your adherence to a set of standards to perform an activity or hold a certain status. Typically, accreditation is held by education institutions or organisations. However, schemes exist in a variety of industries. It can show that an organisation subscribes to certain quality standards or adheres to a voluntary self-regulatory code. Source
3. Alternative 2: Accreditation is a formal, independent verification that a program or institution meets established quality standards and is competent to carry out specific conformity assessment tasks. Conformity assessment tasks may include, but are not limited to, testing, inspection, or certification Source

Accredited

Recommended: Adjective describing an organisation that has been awarded an Accreditation. Also, an adjective for an entity (for example a programme, course or training scheme) that has been independently assessed as meeting published requirements such as learning outcomes or standards of competence or other. Source

Administrative Account

1. **Recommended:** A high-privilege login account that is able to do more than a normal user. System administrators use them to reconfigure systems, create and delete normal user accounts, and so on. Source
2. Alternative 1: Administrator accounts are used by users to carry out tasks that require special permissions, such as installing software or renaming a computer. These Administrator accounts should be regularly audited – this should include a password change, and confirmation of who has access to these accounts Source
3. Alternative 2: means the user account of the Customer, which can solely be accessed and used by the Administrator and through which the Administrator shall be able to (i) use the Tool, App and Services in accordance with Customer's order, (ii) change the configuration settings (including but not limited to adding additional Services or features) and (iii) creating additional accounts for Users Source

Advanced Encryption Standard

1. **Recommended:** A Cryptography algorithm based on a symmetric block cipher, that is generally regarded as one of the best you can use (though see also Elliptic Curve Algorithm) Source
2. Alternative 1: A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information Source
3. Alternative 2: "Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement Source

Advanced Persistent Threat

1. **Recommended:** An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives Source
2. Alternative 1: An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of

organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives Source

3. Alternative 2: Deliberate, considered attacks on your security by outsiders who are determined to get into your system and who will try any number of different attacks in order to get in. If you think you have an APT going on you should look into it, because unlike most attackers they will spend significant time and effort attempting to breach your defenses Source

Adversary

1. **Recommended:** Person, group, organization, or government that conducts or has the intent to conduct detrimental activities. Source
2. Alternative 1: someone or a group that intends to perform malicious actions against other cyber resources. Source
3. Alternative 2: An entity that is not authorized to access or modify information, or who works to defeat any protections afforded the information Source

Advisory

1. **Recommended:** Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. Rationale: General definition of a commonly understood term Source
2. Alternative: A notification put out by security consultancies, law enforcement agencies and the like to tell the world about a security problem they've come across which they think worthy of warning people about. It is wise to take the time to read them, as they're free information about attacks that may be beating on your door any time soon Source

Alert

1. **Recommended:** A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note Source
2. Alternative 1: A notification from your security systems that someone is trying to break in (or, perhaps, has already done so) Source
3. Alternative 2: Notification that a specific attack has been directed at an organization's information systems Source

Allow List

1. **Recommended:** A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system

Source

2. Alternative 1: The opposite of a Block List in which a system permits connections only from the remote systems that appear in a specific list or database. Much more reliable than a Block List for keeping out nefarious connections because it will deny access by default to attackers' machines, but more time-consuming to manage. Traditionally called a Whitelist Source
3. Alternative 2: An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments Source

Anti-Malware Software

1. **Recommended:** A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents Source
2. Alternative 1: Synonymous with **Anti-Virus Software**.
3. Alternative 2: Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more Source

Anti-Virus Software

1. **Recommended:** Software which scans the files going in and out of your computer systems and tries to spot hidden software that is designed to cause damage or theft of data Source
2. Alternative 1: A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents Source
3. Alternative 2: Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more Source

Application

1. **Recommended:** An application, also referred to as an application program or application software, is a computer software package that performs a specific function directly for an end user or, in some cases, for another application. An application can be self-contained or a group of programs Source
2. Alternative 1: A program that runs on a computer Source
3. Alternative 2: A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user’s identity so that the end user’s identifier can be used to facilitate the end user’s interaction with the system Source
4. Alternative 3: The system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications Source

Asset

1. **Recommended:** An item of value to achievement of organizational mission/business objectives. Note 1: Assets have interrelated characteristics that include value, criticality, and the degree to which they are relied upon to achieve organizational mission/business objectives. From these characteristics, appropriate protections are to be engineered into solutions employed by the organization. Note 2: An asset may be tangible (e.g., physical item such as hardware, software, firmware, computing platform, network device, or other technology components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, image, or reputation) Source
2. Alternative 1: Something you own, and hence something that could be compromised or simply stolen. Note that a piece of information can also be classed as an asset, in the same way as a physical object Source
3. Alternative 2: A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems Source
4. Alternative 3: An item of value to achievement of organizational mission/business objectives. Note 1: Assets have interrelated characteristics that include value, criticality, and the degree to which they are relied upon to achieve organizational mission/business objectives. From these characteristics, appropriate protections are to be engineered into solutions employed by the organization. Note 2: An asset may be tangible (e.g., physical item such as hardware, software, firmware, computing platform, network device, or other technology components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, image, or reputation) Source

Asymmetric Cryptography

1. **Recommended:** Cryptography that uses two separate keys to exchange data, one to encrypt or digitally sign the data and one for decrypting the data or verifying the digital signature. Also known as public key cryptography. Source
2. Alternative 1: Largely synonymous with Public Key Cryptography - where the key used to decrypt something is different from the one that was used to encrypt it Source
3. Alternative 2: Encryption system that uses a public-private key pair for encryption and/or digital signature Source

Attack Signature

1. **Recommended:** A specific sequence of events indicative of an unauthorized access attempt Source
2. Alternative: Alternative: The pattern of events that take place in order to perpetrate an attack on a computer system. Often, an intrusion involves several steps, and if one can establish out the sequence of steps then one can see whether two attacks are similar and hence may have been from the same source Source

Audit Log

1. **Recommended:** A system or application log that stores details of what people have been doing on the application/system it applies to, which is invaluable both for general monitoring and, in particular, for forensic analysis in the event of a problem Source
2. Alternative: A chronological record of system activities. Includes records of system accesses and operations performed in a given period Source

Audit Trail

1. **Recommended:** The next level up from an Audit Log: an audit trail is a chronology of events but is generally more human-readable than an Audit Log. The latter is system-generated and hence can be cryptic; the audit trail is built by a human being using sources such as the audit log and is written to be readable by non-technical people Source
2. Alternative 1: A record showing who has accessed an information technology (IT) system and what operations the user has performed during a given period Source
3. Alternative 2: A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result Source

Audit

1. **Recommended:** An assessment of an organisation's operation against one or more specified standards. Internal audits, often called first-party audits, are conducted as self-assessments by the organisation itself; external, or third-party audits, are conducted by an independent assessor from outside the organisation Source
2. Alternative 1: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures Source
3. Alternative 2: The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures and to recommend any indicated changes in controls, policy, or procedures Source

Authentication

1. **Recommended:** Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system Source
2. Alternative 1: Confirming the identify of an individual who is trying to connect to and use a computer system Source
3. Alternative 2: The process of establishing confidence of authenticity; in this case, the validity of a person’s identity and an authenticator (e.g., PIV Card or derived PIV credential) Source

Availability

1. **Recommended:** The property that data or information is accessible and usable upon demand by an authorized person Source
2. Alternative 1: One of the three pillars of security: CIA. It's all about ensuring that systems are up, running, accessible and not overloaded in order that the data and applications the users need are all usable. Denial of Service attacks are a common way of attempting to deny the availability of services Source
3. Alternative 2: Ensuring timely and reliable access to and use of information Source

Back Door

- **Recommended:** An undocumented way of gaining access to computer system. A backdoor is a potential security risk Source
- Alternative 1: An unofficial means to access a system or application - one that's not officially supported and doesn't form part of the accepted or tested design, but which was inserted by one or more of the developers to provide a means of side-stepping the formal security mechanisms Source
- Alternative 2: A malicious program that listens for commands on a certain Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port Source

Backup

1. **Recommended:** A copy of files and programs made to facilitate recovery if necessary Source
2. Alternative: A copy of part or all of the content of a system that is stored safely in order that should the system fail (or should the Integrity of the contents be compromised) the system can be restored to service by copying the content from the backup Source

Baselining

1. **Recommended:** Monitoring resources to determine typical utilization patterns so that significant deviations can be detected Source
2. Alternative 1: Monitoring your systems' behavior to establish what looks normal, so that your security systems can Alert you if they detect abnormal behavior Source
3. Alternative 2: The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system Source

Bastion Host

1. **Recommended:** A special purpose computer on a network where the computer is specifically designed and configured to withstand attacks Source
2. Alternative 1: A device in your network that you put in front of the Internet connection in order to fend off or absorb attacks Source

3. Alternative 2: A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration Source

Biometric

1. **Recommended:** Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics Source
2. Alternative 1: A characteristic of your body which, in the context of cybersecurity, can be used to identify you; examples are your irises and your fingerprints Source
3. Alternative 2: A physical or behavioral characteristic of a human being Source

Black Box Testing

1. **Recommended:** Security testing of a system where the tester has no information about the system's design, implementation or security mechanisms. The opposite of White Box Testing Source
2. Alternative 1: A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing Source
3. Alternative 2: A method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance Source

Blacklist

1. **Recommended:** Synonymous with Block List, the term “Blacklist” is widely falling into disuse following the growth of the Black Lives Matter movement Source
2. Alternative 1: A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity. Also known as dirty word list Source
3. Alternative 2: A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity Source

Block Cipher Algorithm

1. **Recommended:** An Encryption Algorithm (and an associated Decryption Algorithm) that operates on fixed-size chunks of data at a time Source
2. Alternative 1: An invertible symmetric-key cryptographic algorithm that operates on fixed-length blocks of input using a secret key and an unvarying transformation algorithm. The resulting output block is the same length as the input block Source
3. Alternative 2: A family of functions and their inverse functions that is parameterized by cryptographic keys; the functions map bit strings of a fixed length to bit strings of the same length Source

Block List

1. **Recommended:** A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity. Source
2. Alternative 1: A list or databases of users, systems, companies, etc. that are specifically prohibited from accessing a system (e.g. an email server would reject inbound email from any domain that was on the organisation's Block List). Source
3. Alternative 2: A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity. Also known as dirty word list Source

Blue Team

1. **Recommended:** A security testing team that focuses on analysing systems and designing new or improved security mechanisms to defend the systems from attack. See also Red Team Source
2. Alternative 1: The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the **Red Team**). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team) Source
3. Alternative 2: A group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cybersecurity readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the **Red Team** test the systems Source

Bot

1. **Recommended:** A computer connected to the Internet that has been compromised with malicious logic to undertake activities under the command and control of a remote administrator Source
2. Alternative 1: Cyber criminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all the infected machines into a network of "bots" that the criminal can remotely manage Source
3. Alternative 2: A bot is a software application that is programmed to do certain tasks. Bots are automated, which means they run according to their instructions without a human user needing to manually start them up every time. Bots often imitate or replace a human user's behavior. Typically they do repetitive tasks, and they can do them much faster than human

users could Source

Botnet

1. **Recommended:** A network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge Source
2. Alternative 1: The word "botnet" is formed from the words "robot" and "network." Cyber criminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all the infected machines into a network of "bots" that the criminal can remotely manage Source
3. Alternative 2: A bot is a software application that is programmed to do certain tasks. Bots are automated, which means they run according to their instructions without a human user needing to manually start them up every time. Bots often imitate or replace a human user's behavior. Typically they do repetitive tasks, and they can do them much faster than human users could Source

Boundary

1. **Recommended:** Physical or logical perimeter of a system Source
2. Alternative: The "edge" of a system or network, where it connects to another system or network. For example, the firewall providing connectivity between the Local Area Network and the internet is part of the Boundary Source

Breach

1. **Recommended:** Breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act Source
2. Alternative 1: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose Source
3. Alternative 2: A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms Source

Bring your own device

1. **Recommended:** Bring your own device (BYOD) is the practice of allowing staff to use their own devices in the workplace and to use those devices to securely access the organisation's systems, applications and information. This can mean using their own smartphones, tablets or laptops for work Source
2. Alternative 1: BYOD is the concept of employees using their personally owned device(s) for work purposes. Source
3. Alternative 2: Bring your own device (BYOD) refers to the trend of employees using

personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data. Personal devices could include smartphones, personal computers, tablets, or USB drives Source

Brute Force Attack

1. **Recommended:** A method of accessing an obstructed device [1] by attempting multiple combinations of numeric/alphanumeric passwords Source
2. Alternative 1: A means of trying to figure out the password of a particular login account for a system. It's the simplest cracking program to write because you just have to loop through every possible password or through every entry in an extensive list of potential passwords. Trouble is, trying every possible combination takes a long time. Brute Force attacks work best not by trying to log into a remote system bazillions of times (each connection can take several seconds - which adds up when trying several million passwords) but by breaking in and stealing the password file and running the cracker against it on a nice fast machine Source
3. Alternative 2: In cryptography, an attack that involves trying all possible combinations to find a match Source

Buffer Overflow

1. **Recommended:** A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system Source
2. Alternative: A technique for hacking systems that injects more characters into a request than should be permitted, either causing the system to crash or injecting code into the target system to change its behaviour. Buffer Overflow attacks are generally possible because of poor design and coding techniques when systems are built Source

Bug

1. **Recommended:** A bug refers to an error, fault or flaw in any computer program or a hardware system. A bug produces unexpected results or causes a system to behave unexpectedly. In short, it is any behavior or result that a program or system gets but it was not designed to do” Source
2. Alternative 1: A software bug is a problem causing a program to crash or produce invalid output. The problem is caused by insufficient or erroneous logic. A bug can be an error, mistake, defect or fault, which may cause failure or deviation from expected results Source
3. Alternative 2: Simply stated, a software bug is a defect in a computer program or system. This probably sounds pretty straightforward but unfortunately, these bugs are sometimes not very easy to find or detect. Especially with complex software applications made up of millions of lines of code. Some bugs cause minimal harm and can go unnoticed until the following update, but others can have more serious effects. For example, minor bugs can

[1] or a system

cause errors in navigation, system design or timings. These are usually observable bugs that can be easy to find by software developers. However, major bugs can cause systems to crash, close unexpectedly or affect other applications Source

Business Continuity Plan

1. **Recommended:** The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption Source
2. Alternative 1: A framework and procedure set that you build in order to maximise your chances of recovering from a business-impacting incident (which could include a security breach or some such) Source
3. Alternative 2: Business continuity planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster Source

Business Impact Analysis

1. **Recommended:** An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption Source
2. Alternative 1: An assessment of all of your systems to estimate the negative effect on the organisation of a system being compromised or disabled Source
3. Alternative 2: A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs) and recovery point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions and plans Source

Certificate Management

1. **Recommended:** Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed Source
2. Alternative 1: The regime of creating, storing and managing Source
3. Alternative 2: Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. (In the context of this practice guide, it also includes inventory, monitoring, enrolling, installing, and revoking) Source

Certificate Revocation List

1. **Recommended:** A list of revoked public key certificates created and digitally signed by a certification authority Source
2. Alternative 1: A list of digital certificates that have been revoked by their Certification Authority. It's particularly important for your software to check the CRL because it's there

precisely to tell you that a certificate is no longer acceptable - perhaps its host was compromised and the private key stolen, for instance Source

3. Alternative 2: These are digitally signed “blacklists” of revoked certificates. Certification authorities (CAs) periodically issue certificate revocation lists (CRLs), and users can retrieve them on demand via repositories Source

Certification Authority

1. **Recommended:** The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates and exacting compliance with a PKI policy Source
2. Alternative 1: A respected organisation that issues digital certificates, which you can attach to your Web servers in order to prove your organisation's identity Source
3. Alternative 2: The entity in a public key infrastructure (PKI) that is responsible for issuing certificates to certificate subjects and exacting compliance to a PKI policy Source

Chain of Evidence

1. **Recommended:** A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The “sequencing” of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner. Rationale: Sufficiently covered under chain of custody Source
2. Alternative: A definitive, provable sequence of events and/or actions that you use to demonstrate to a court or tribunal, or your HR department, that conclusively demonstrates what occurred in a security breach. It should be possible to step through your Chain of Evidence from beginning to end and demonstrate that none of the evidence could have been tampered with or illicitly seen at any stage Source

Challenge-Response

1. **Recommended:** Challenge Response Authentication Mechanism is also called CRAM. It refers to a set of protocols that helps validate actions to protect digital assets and services from unauthorized access. This protocol usually has two components – a question and a response – where a verifier presents a challenge to a user, who must provide a correct answer for authentication. Challenge-response protocols can be as simple as a password or a dynamically generated request Source
2. Alternative 1: A basic means of authentication, where a system requests action from the user, and the user responds - for example, a system requesting a user's password and the user entering it Source
3. Alternative 2: An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (often by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and

controls the secret Source

Checksum

1. **Recommended:** A value computed on data to detect error or manipulation Source
2. Alternative 1: A calculation that's used to confirm the Integrity of a collection of data: a calculation is performed on all the individual bytes of data and the result is the checksum. Checksums are good for checking for corruption but less so for ensuring that the data has not been tampered with, because it's often possible to change the data so that the checksum works out correctly; use a Hash Function instead in the latter case Source
3. Alternative 2: A value that (a) is computed by a function that is dependent on the contents of a data object and (b) is stored or transmitted together with the object, for detecting changes in the data Source

Cipher Text

1. **Recommended:** Data in its encrypted form Source
2. Alternative 1: The result of running Plain Text through a Cipher or Encryption Algorithm Source
3. Alternative 2: Ciphertext is what encryption algorithms, or ciphers, transform an original message into Source

Cipher

1. **Recommended:** Synonymous with **Encryption Algorithm**
2. Alternative 1: Series of transformations that converts plaintext to ciphertext using the Cipher Key Source
3. Alternative 2: Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both Source

Classified Information

1. **Recommended:** Highly confidential information that pertains to, for example, national security Source
2. Alternative 1: Classified information or classified national security information means information that has been determined pursuant to E. O.[2)] 12958 as amended by E.O. 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form Source
3. Alternative 2: Information that has been determined pursuant to Executive Order (E.O.) 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form Source

[2)] Executive Order

Clear Text

1. **Recommended:** Unencrypted information Source
2. Alternative 1: Intelligible data, the semantic content of which is available. Note: Clear text data is, by definition, not encrypted Source
3. Alternative 2: Intelligible data, the semantic content of which is available Source

Clearance

1. **Recommended:** Formal certification, generally from a government agency, that permits one to work with Classified Information. Required for many government-related jobs Source
2. Alternative: A formal security determination by an authorized adjudicative office that an individual is authorized access, on a need-to-know basis, to a specific level of classified information (TOP SECRET, SECRET, or CONFIDENTIAL) Source

Clickjacking

1. **Recommended:** Clickjacking is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. Its other name, user interface (UI) redressing, better describes what is going on Source
2. Alternative 1: A malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages Source
3. Alternative 2: Clickjacking, also known as a “UI redress attack”, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page. Thus, the attacker is “hijacking” clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both Source

Code of Conduct

1. **Recommended:** A code of conduct is the most common policy within an organization. This policy lays out the company's principles, standards, and the moral and ethical expectations that employees and third parties are held to as they interact with the organization Source
2. Alternative 1: A set of guidelines used by an organisation to regulate the behaviour of its members with a focus on compliance and rules. in the sense of the UK Cyber Security Council, each licensed body must have its own Code of Conduct Source
3. Alternative 2: A code of conduct serves not only as a set of internal guidelines for the employees to follow, but also as an external statement of corporate values and commitments Source

Code of Ethics

1. **Recommended:** A code of ethics is similar to a code of conduct in that it establishes behavior expectations that an organization has of its employees and third parties. However, it is slightly adjacent because a code of ethics dives deeper into the principles that should guide their actions and touches upon issues such as harassment, safety, and conflicts of interest. This code is often considered an ethical code of conduct Source
2. Alternative: A set of principles designed to help professionals and/or members of an organisation or professional body conduct business honestly, transparently and with integrity Source

Collision

1. **Recommended:** In a given context, the equality of two values, usually out of a large number of possible values Source
2. Alternative 1: An instance in which an encryption or Hash Function produces the same output for two or more given sets of input Source
3. Alternative 2: An event in which two different messages have the same message digest Source

Common Vulnerabilities and Exposures

1. **Recommended:** An identifier for a specific software flaw defined within the official CVE Dictionary and that conforms to the CVE specification Source
2. Alternative: A nomenclature and dictionary of security-related software flaws Source

Common Vulnerability Scoring System

1. **Recommended:** A system for measuring the relative severity of software flaw vulnerabilities Source
2. Alternative 1: An industry standard for assessing the severity of a Vulnerability on a computer system and representing it as a “score” between 0 (no risk) and 10 (severe risk) Source
3. Alternative 2: An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity Source

Compliance

1. **Recommended:** The level to which systems and security are operated in accordance with documented standards, policies and procedures Source
2. Alternative 1: Cybersecurity Compliance involves meeting various controls (usually enacted by a regulatory authority, law, or industry group) to protect the confidentiality, integrity, and availability of data Source
3. Alternative 2: Simply put, cybersecurity compliance is the organizational risk management method aligned with pre-defined security measures & controls on how data confidentiality

is ensured by its administrational procedures Source

Compromise

1. **Recommended:** See **Breach**
2. Alternative 1: A successful penetration into a system by a hacker despite the security mechanisms defending it Source
3. Alternative 2: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred Source
4. Alternative 3:
    a. (General) The disclosure of classified data to persons not authorized to receive that data.
    b. (Automated Information Systems) A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.
    c. Source

Computer Emergency Response Team

1. **Recommended:** Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team) Source
2. Alternative 1: A team that exists to provide response and recovery from a computer or cyber security incident. Because the abbreviation “CERT” is a registered trademark in the US, terms such as Computer Incident Response Team or Cyber Security Incident Response Team are often used instead Source
3. Alternative 2: Group of individuals usually consisting of security analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Cyber Incident Response Team, Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center or Computer Incident Response Capability) Source

Computer Incident Response Team

See **Computer Emergency Response Team**

Computer Network Defence

1. **Recommended:** Typically applied to military and government security, CND refers to the measures taken to protect information systems and networks against cyber attacks and intrusions Source
2. Alternative 1: Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern

analysis), and response and restoration activities [3] Source

3. Alternative 2: A set of processes and protective measures that use computer networks to detect, monitor, protect, analyze and defend against network infiltrations resulting in service/network denial, degradation and disruptions. CND enables a government or military institute/organization to defend and retaliate against network attacks perpetrated by malicious or adversarial computer systems or networks Source

Confidentiality

1. **Recommended:** The property that data or information is not made available or disclosed to unauthorized persons or processes Source
2. Alternative 1: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information Source
3. Alternative 2: The ability to protect data so that unauthorized parties cannot view the data Source

Configuration Management

1. **Recommended:** A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle Source
2. Alternative: A regime of recording, monitoring and regularly verifying the configuration of systems and applications to verify that changes that are made do not have unexpected security consequences Source

Continuous Monitoring

1. **Recommended:** A technology and process that IT organizations may implement to enable rapid detection of compliance issues and security risks within the IT infrastructure. Continuous monitoring is one of the most important tools available for enterprise IT organizations, empowering SecOps teams with real-time information from throughout public and hybrid cloud environments and supporting critical security processes like threat intelligence, forensics, root cause analysis, and incident response Source
2. Alternative 1: Maintaining ongoing awareness to support organizational risk decisions See information security continuous monitoring, risk monitoring, and status monitoring Source
3. Alternative 2: An automated process by which DevOps personnel can observe and detect compliance issues and security threats during each phase of the DevOps pipeline. Outside DevOps, the process may be expanded to do the same for any segment of the IT infrastructure in question. It helps teams or organizations monitor, detect, study key

[3] Note: Within DoD, term was approved for deletion from JP 1-02 (DoD Dictionary) by issuance of JP 3-13, “Information Operations”. This term has been replaced by the use of “cyberspace defense“ used in JP 3-12, “Cyberspace Operations.” Original source of term was JP 1-02 (DoD Dictionary)

relevant metrics, and find ways to resolve said issues in real-time Source

Cookie

1. **Recommended:** A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests Source
2. Alternative 1: A token embedded into Web pages that let the owner of the site you're connected to track your progress, remember who you're logged in as, and so on Source
3. Alternative 2: A cookie is a piece of data from a website that is stored within a web browser that the website can retrieve at a later time. Cookies are used to tell the server that users have returned to a particular website Source

Countermeasure(s)

1. **Recommended:** Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices Source
2. Alternative 1: An action, application or device that reduces a security threat in a system or application Source
3. Alternative 2: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system Source

Credentials

1. **Recommended:** The information used to authenticate a user’s identity – for example, password, token, certificate Source
2. Alternative: A piece of information that is sent from one computer to another to check that a user is who they claim to be or to allow someone to see information Source

Credit card fraud

1. **Recommended:** An inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services or to make payment to another account, which is controlled by a criminal Source
2. Alternative 1: It's when your credit card details are stolen by fraudsters, who either use them to make payments, or to sell them on to other criminals. This activity may even have an effect on your credit report, for example, if the fraudsters have exceeded your credit card limit Source
3. Alternative 2: Credit card fraud is any kind of theft or fraud that involves a credit card. The aim of credit card fraud is to purchase goods without paying, or to steal money from someone else’s credit account Source

Critical infrastructure Sector

1. **Recommended:** A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society Source
2. Alternative 1: Information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping Source
3. Alternative 2: Critical infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety Source

Critical infrastructure

1. **Recommended:** A public or private infrastructure or process whose destruction, standstill, illegitimate exploitation or disruption for a defined period of time will cause either loss of lives or significant loss to the economy or damage significantly the reputation of the State or its symbols of governance. In this definition, infrastructure includes the networks, systems and the physical or digital data essential for providing this service. This term may refer to a certain system or process whose functioning is critical within the organization Source
2. Alternative 1: System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters Source
3. Alternative 2: System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters Source
4. Alternative 3: Essential services and related assets that underpin American society and serve as the backbone of the nation's economy, security, and health Source

Critical National Infrastructure

1. **Recommended:** Add Nationwide perspective to **Critical Infrastructure**
2. Alternative 1: An organisation that is core to the underlying operation of a nation or principality, for which an outage or a cyber attack would have potentially massive implications on the operation of the country. This includes the power companies, water providers, telecoms providers, government IT infrastructure, health service, rail and road infrastructure operators and the owners/operators of the major ports and airports https://www.ukcybersecuritycouncil.org.uk/glossary/
3. Alternative 2: National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example). https://www.cpni.gov.uk/critical-national-infrastructure-0

4. Alternative 2: Critical infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety. https://www.techtarget.com/whatis/definition/critical-infrastructure

Cross Certificate

1. **Recommended:** A certificate issued from a certificate authority (CA) that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs [4] Source
2. Alternative 1: A certificate issued by a Certification Authority to sign the certificate of another Certification Authority Source
3. Alternative 2: A certificate used to establish a trust relationship between two certification authorities Source

Cross Site Request Forgery

1. **Recommended:** A type of Web exploit where an unauthorized party causes commands to be transmitted by a trusted user of a Web site without that user’s knowledge Source
2. Alternative: An attack in which a subscriber currently authenticated to an RP and connected through a secure session browses to an attacker’s website, causing the subscriber to unknowingly invoke unwanted actions at the RP. For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window Source

Cross Site Scripting

1. **Recommended:** See **Cross Site Request Forgery**
2. Alternative 1: A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user-supplied data from requests or forms without sanitizing the data so that it is not executable Source
3. Alternative 2: Cross-Site Scripting is a security flaw found in some Web applications that enables unauthorized parties to cause client-side scripts to be executed by other users of the Web application Source

Cryptanalysis

1. **Recommended:** The study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of

[4] Note: This is a more narrow definition than described in X.509

looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself Source

2. Alternative 1: The study of the mathematics and other techniques involved in Cryptography Source
3. Alternative 2: Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection Source

Cryptographic Key

1. **Recommended:** A parameter used in conjunction with a cryptographic algorithm that determines its operation. Examples applicable to this Standard include: 2. The computation of a digital signature from data, and 2. The verification of a digital signature Source
2. Alternative: The third element (of three) when encrypting data: one takes an Encryption Algorithm and combines it with a Cryptographic Key to transform Plain Text into Cipher Text Source

Cryptographic Strength

1. **Recommended:** The level of difficulty in breaking a cryptographic system: a high cryptographic strength means the cipher is very difficult to break Source
2. Alternative 1: The ability of a cryptographic system to protect information from attack is called its strength Source
3. Alternative 2: The strength of encryption is related to the difficulty of discovering the key, which in turn depends on both the cipher used and the length of the key. For example, the difficulty of discovering the key for the RSA cipher most commonly used for public-key encryption depends on the difficulty of factoring large numbers, a well-known mathematical problem Source

Cryptography

1. **Recommended:** The discipline of transforming data from its raw form into a form where it cannot easily be read by unauthorized individuals Source
2. Alternative 1: The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification Source
3. Alternative 2: Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form Source

Cyber incident

1. **Recommended:** Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. See incident. See also event, security-relevant event, and intrusion Source
2. Alternative 1: A breach of a system or service’s security policy Source

3. Alternative 2: Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein Source

Cyber Security

1. **Recommended:** The defense of information held and processed on digital systems against unauthorized access, damage or misuse. It includes the protection of the hardware, software and associated infrastructure, the data that is held, and the services provided, and encompasses both technical and non-technical defense mechanisms. Cyber security is defined by ITU-T Recommendation X.1205 Source
2. Alternative: The ability to protect or defend the use of cyberspace from cyber attacks Source

Cyclic Redundancy Check

1. **Recommended:** A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected Source
2. Alternative 1: A means of error checking data by computing a function against the transmitted and received versions of data and comparing the results. Similar to a Checksum Source
3. Alternative 2: A method to ensure data has not been altered after being sent through a communication channel Source

Data at rest

1. **Recommended:** Data that is in persistent storage – i.e. data that remains on a device whether or not it is connected to a power source – such as hard disks, removable media or backups Source
2. Alternative 1: Data at rest is data currently in storage, typically on a computer's or server's hard disk. Data at rest contrasts with data in transit — also called data in motion — which is the state of data as it travels from one place to another. It also contrasts with data in use — data loaded into memory and actively in use by a software program Source
3. Alternative 1: Data at rest is one of the three states of digital data and it refers to any digital information that is stationary and contained within permanent storage devices, such as hard drives and tapes, or information reservoirs such as off-site backups, databases, archives, etc. The other states of digital data are data in motion, and data in use. Once data is transported and settles in its final destination, it is called data at rest during the entire period it remains inactive. If the data needs to be utilized for whatever purpose, and is being processed, it is then classified as data in use Source

Data breach

1. **Recommended:** A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system’s owner. A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary,

or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security Source
2. Alternative: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose Source

Data Encryption Standard

1. **Recommended:** A symmetric encryption algorithm (known commonly as “DES”) devised in the 1970s; superseded by Triple DES Source
2. Alternative 1: Data Encryption Standard specified in FIPS 46-3 Source
3. Alternative 2: The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for modern applications, it has been highly influential in the advancement of cryptography Source

Data integrity

1. **Recommended:** The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit Source
2. Alternative 1: The quality of data that is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner Source
3. Alternative 2: A property possessed by data items that have not been altered in an unauthorized manner since they were created, transmitted, or stored Source

Data Loss Prevention

1. **Recommended:** Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users Source
2. Alternative 1: A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information Source
3. Alternative 2: Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and comply with regulations Source

Data Loss

1. **Recommended:** Data loss is a serious problem for businesses of all sizes— losing files means losing time and money to restore or recover information that is essential to your business. Data loss occurs when data is accidentally deleted or something causes data to become corrupted. Viruses, physical damage or formatting errors can render data

unreadable by both humans and software. Losing files and documents often has a lasting impact on your company's financial health Source
2. Alternative 1: The exposure of proprietary, sensitive, or classified information through either data theft or data leakage Source
3. Alternative 2: The exposure of proprietary, sensitive, or classified information through either data theft or data leakage Source

Data Protection

Recommended: Data protection is about protecting the freedoms and fundamental rights of individuals with regard to the processing of their personal data, meaning any information relating to an identified or identifiable natural person, including name, date of birth, photographs, video footage, email addresses, telephone numbers and IP addresses. Data protection is a fundamental right enshrined in EU primary and secondary law Source

Data security

1. **Recommended:** Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures Source
2. Alternative 1: The measures taken to protect confidential data and prevent it from being accidentally or deliberately disclosed, compromised, corrupted or destroyed Source
3. Alternative 2: The process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything—hardware, software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures Source

Decipher

See **Decryption**

Decrypt

See **Decryption**

Decryption Algorithm

1. **Recommended:** The opposite of an **Encryption** Algorithm
2. Alternative: The decryption algorithms specify the data and key encryption algorithms that are used to decrypt the SOAP message. The WSS API for decryption (WSSDecryption) specifies the algorithm uniform resource identifier (URI) of the data and key encryption methods Source

Decryption

1. **Recommended:** The process of changing ciphertext into plain text using a cryptographic algorithm and key Source
2. Alternative 1: The process of transforming ciphertext into plaintext Source
3. Alternative 2: The process of a confidentiality mode that transforms encrypted data into the original usable data Source

Defense in Depth

1. **Recommended:** A defense-in-depth strategy, aka[5] a security-in-depth strategy, refers to a cybersecurity approach that uses multiple layers of security for holistic protection. A layered defense helps security organizations reduce vulnerabilities, contain threats, and mitigate risk. In simple terms, with a defense-in-depth approach, if a bad actor breaches one layer of defense, they might be contained by the next layer of defense Source
2. Alternative 1: Employing several layers of protection to improve your chances of preventing someone from breaking into your systems - so if they breach the outermost layer of security they then have several more different types of protection to breach before they can access your systems Source
3. Alternative 2: Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack Source

Deleted File

A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data Source

Demilitarised Zone

1. **Recommended:** Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks Source
2. Alternative 1: A network that sits between the Internet and the secure LAN [6], in which you put services such as Web and email servers Source
3. An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic - Alternative 2: moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied Source

[5] Also Known As

[6] Local Area Network

Denial of Service

1. **Recommended:** An attack that bombards a system with connections to keep it so busy that it is unable to accept legitimate connections. See also Distributed Denial of Service instead Source
2. Alternative 1: The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided) Source
3. Alternative 2: The prevention of authorized access to a system resource or the delaying of system operations and functions Source

DevSecOps

1. **Recommended:** DevSecOps stands for development, security, and operations. It's an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle Source
2. Alternative 1: A development regime in which the Operations and Security teams work with the Development teams throughout the project in order that the security team can provide constant, ongoing feedback to help developers get the operations and security aspects of the system right Source
3. Alternative 2: DevSecOps—short for development, security, and operations—automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery Source

Dictionary attack

1. **Recommended:** A targeted form of brute force attack, dictionary attacks run through lists of common words, phrases, and leaked password to gain access to accounts Source
2. Alternative 1: Known dictionary words, phrases or common passwords are used by the attacker to gain access to your information system. This is a type of brute force attack Source
3. Alternative 2: A dictionary attack is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document Source

Digital Forensics

1. **Recommended:** The process used to acquire, preserve, analyze, and report on evidence using scientific methods that are demonstrably reliable, accurate, and repeatable such that it may be used in judicial proceedings Source
2. Alternative 1: The application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data Source
3. Alternative 2: In its strictest connotation, the application of computer science and

investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony Source

Digital Signature

1. **Recommended:** An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection Source
2. Alternative 1: An electronic means of proving that a document you've sent someone really is for you. Generally based on Public Key Cryptography Source
3. Alternative 2: The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1. origin authentication, 2. data integrity, and 3. signer non-repudiation Source

Disaster Recovery Plan

1. **Recommended:** Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities Source
2. Alternative 1: Like a Business Continuity Plan but with a focus on the technical aspects of getting systems back up in the event of a severe security attack or outage Source
3. Alternative 2: A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities Source

Disk Imaging

1. **Recommended:** Generating a bit-for-bit copy of the original media, including free space and slack space. Also known as a bit stream image Source
2. Alternative 1: The technique of taking an exact copy of a computer's hard disk in order to preserve evidence and/or allow for forensic investigation without risking damaging the original and hence invalidating the Chain Of Evidence Source
3. Alternative 2: Disk imaging is a form of hard drive backup that places all of a hard drive's data into a compressed file. That file can be stored on other devices, in a file system, or in the cloud. Disk imaging allows individuals and businesses to recover all data that was on a computer when the image was made Source

Disruption

1. **Recommended:** An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction) Source
2. Alternative: Intent of damaging and disrupting critical business functions. The most frequent example, Ransomware, is used by cyber criminals to cryptographically lock and hold files and/or access to computer resources for a monetary ransom Source

Distributed Denial of Service

1. **Recommended:** A denial of service technique that uses numerous hosts to perform the attack. See also **Denial of Service** Source
2. Alternative 1: A security attack whereby the attacker exploits dozens, hundreds of thousands of systems around the world to target simultaneous attacks against a single organisation. It relies on the attacker being able to get a piece of [Malware] onto those worldwide systems. The idea of DDoS is that the collective bandwidth and processing power of the machines doing the attack far exceed the bandwidth and processing power of the attacked organisation Source
3. Alternative 2: Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic Source

DNSSec

1. **Recommended:** The Domain Name System Security Extensions (DNSSEC) is a set of specifications that extend the DNS protocol by adding cryptographic authentication for responses received from authoritative DNS servers. Its goal is to defend against techniques that hackers use to direct computers to rogue websites and servers. While DNSSEC has already been deployed for many of the generic and country-level top-level domains (TLDs), adoption at the individual domain level and end-user level has lagged behind Source
2. Alternative 1: The Domain Name System Security Extensions is a suite of extension specifications by the Internet Engineering Task Force for securing data exchanged in the Domain Name System in Internet Protocol networks Source
3. Alternative 2: Engineers in the Internet Engineering Task Force (IETF), the organization responsible for the DNS protocol standards, long realized the lack of stronger authentication in DNS was a problem. Work on a solution began in the 1990s and the result was the DNSSEC Security Extensions (DNSSEC) Source

Drive-By Attack

1. **Recommended:** A drive-by download is a program that is automatically installed on your computer when you’re visiting a booby-trapped website or viewing a HTML e-mail message. The malicious program is downloaded to your computer without your consent or knowledge, without your having to click on a link on the page or in the e-mail Source
2. Alternative 1: Malicious software or a **Virus** that is installed on a device without the user’s knowledge or consent – sometimes known as a drive-by download Source
3. Alternative 2: Drive by download attacks specifically refer to malicious programs that install to your devices — without your consent. This also includes unintentional downloads of any files or bundled software onto a computer device Source

Dynamic application security testing

1. **Recommended:** Dynamic Application Security Testing (DAST) is the process of analyzing a

web application through the front-end to find vulnerabilities through simulated attacks. This type of approach evaluates the application from the “outside in” by attacking an application like a malicious user would. After a DAST scanner performs these attacks, it looks for results that are not part of the expected result set and identifies security vulnerabilities Source

2. Alternative 1: Black-box testing method, meaning it is performed from the outside in. The principle revolves around introducing faults to test code paths on an application Source
3. Alternative 2: Dynamic Application Security Testing (DAST) examines applications for vulnerabilities like these in deployed environments. DAST uses the open source tool OWASP Zed Attack Proxy for analysis Source

Easter Egg

1. **Recommended:** Hidden code within computer software that does something that doesn't form part of its normal operation. Sometimes this is officially included by the vendor, but is sometimes illicit in order to provide a **Back Door** Source
2. Alternative: Easter eggs - at least, the coding variety - have been around since the 1970s. The creator of an Atari game, Adventure, was disappointed to learn that his name wouldn’t appear in the game’s credits. He added a hidden room to the game, with nothing in it other than the words ‘Created by Warren Robinett’. Players soon began searching for the room, in the same way that they’d hunt for literal Easter eggs, and the name quickly stuck Source

Eavesdropping Attack

1. **Recommended:** An attack in which the attacker listens passively to supposedly secret transmissions in order to perpetrate an attack Source
2. Alternative 1: A party that secretly receives communications intended for others Source
3. Alternative 2: An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices Source

Elliptic Curve Algorithm

See **Elliptic Curve Cryptography**

Elliptic Curve Cryptography

1. **Recommended:** Elliptic Curve Cryptography (ECC) is an encryption technique that provides public-key encryption similar to RSA. While the security strength of RSA is based on very large prime numbers, ECC uses the mathematical theory of elliptic curves and achieves the same security level with much smaller keys Source
2. Alternative 1: Cryptography that is based upon the use of Elliptic Curve Algorithms Source
3. Alternative 2: Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data. ECC focuses on pairs of public and private keys for decryption and encryption of web traffic. ECC is frequently discussed in the context of the Rivest–Shamir–Adleman (RSA)

cryptographic algorithm Source

Encode

1. **Recommended:** Encoding is the process of converting data into a format required for a number of information processing needs Source
2. Alternative 1: The use of a code to convert plain text to cipher text Source
3. Alternative 2: Character encoding is the process of assigning numbers to graphical characters, especially the written characters of human language, allowing them to be stored, transmitted, and transformed using digital computer Source

Encrypt

1. **Recommended:** Any procedure used in **Cryptography** to convert plain text into **cipher text** to prevent anyone but the intended recipient from reading that data Source
2. Alternative 1: To convert Clear Text into **Cipher Text** using an **Encryption Algorithm** so that it can't be read by someone you don't want to see it Source
3. Alternative 2: Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state Source

Encryption Algorithm

1. **Recommended:** Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key Source
2. Alternative: The mechanism used to Encrypt data, which is usually based on a mathematical formula Source

See **Encrypt**

Endpoint Protection Platform

1. **Recommended:** Endpoint security, or endpoint protection, is the cybersecurity approach to defending endpoints – such as desktops, laptops, and mobile devices – from malicious activity Source
2. Alternative 1: Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection and prevention systems, etc.) Source
3. Alternative 2: Endpoint protection provides essential security for many types of endpoints, from smart phones to printers. An endpoint protection platform (EPP) is an integrated suite of endpoint protection technologies—such as antivirus, data encryption, intrusion prevention, and data loss prevention—that detects and stops a variety of threats at the endpoint Source

Endpoint

1. **Recommended:** A collective term for internet-capable computer devices connected to a network – for example, modern smartphones, laptops and tablets are all endpoints Source
2. Alternative 1: An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples of endpoints include: Desktops Laptops Source
3. Alternative 2: An endpoint is any device that connects to a computer network. When Bob and Alice talk on the phone, their connection extends from one person to the other, and the "endpoints" of the connection are their respective phones. Similarly, in a network, computerized devices have "conversations" with each other, meaning they pass information back and forth. Just as Bob is one endpoint of his and Alice's conversation, a computer connected to a network is one endpoint of an ongoing data exchangeSource

Ethical hacking

1. **Recommended:** The use of hacking techniques for legitimate purposes – i.e. to identify and test cyber security vulnerabilities. The actors in this instance are sometimes referred to as 'white hat hackers' Source
2. - Alternative 1: The actors in this instance are sometimes referred to as 'white hat hackers'. Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers Source
3. Alternative 2: Ethical hacking (or penetration testing) is the exploitation of an IT system with the permission of its owner to determine its vulnerabilities and weak points. It is an effective way of testing and validating an organisation's cyber security Source

Event

1. **Recommended:** Occurrence or change of a particular set of circumstances Source
2. Alternative 1: An occurrence relating to security that's sufficiently interesting that you think it's worth recording for later reference or reporting Source
3. Alternative 2: Any observable occurrence on a manufacturing system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation) Source

Exfiltration

1. **Recommended:** The unauthorized transfer of information from an information system Source
2. Alternative: Data exfiltration occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer. It is also commonly called data extrusion or data exportation. Data exfiltration is also considered a form of data theft Source

Exploit kit

1. **Recommended:** An exploit kit or exploit pack is a type of toolkit cybercriminals use to attack vulnerabilities in systems so they can distribute malware or perform other malicious activities. Exploit kits are packaged with exploits that can target commonly installed software such as Adobe Flash®, Java®, Microsoft Silverlight® Source
2. Alternative 1: Computer programs designed to discover vulnerabilities in software apps and use them to gain access to a system or network. Once they have infiltrated a system they will feed it with harmful code Source
3. Alternative 2: Exploit kits are automated threats that use compromised sites to divert web traffic, scan for vulnerable browser-based applications, and run malware Source

Exploit

1. **Recommended:** An exploit is a program, or piece of code, designed to find and take advantage of a security flaw or vulnerability in an application or computer system, typically for malicious purposes such as installing malware. An exploit is not malware itself, but rather it is a method used by cybercriminals to deliver malware Source
2. Alternative 1: A technique to breach the security of a network or information system in violation of security policy Source
3. Alternative 2: An exploit (in its noun form) is a segment of code or a program that maliciously takes advantage of vulnerabilities or security flaws in software or hardware to infiltrate and initiate a denial-of-service (DoS) attack or install malware, such as spyware, ransomware, Trojan horses, worms, or viruses Source

External Audit

See **Audit**

Extranet

1. **Recommended:** An extranet is a controlled private network that allows access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet Source
2. Alternative 1: An Internet site that's designed for partner or customer organisations to connect to your systems to access information and other materials Source
3. Alternative 2: A computer network that an organization uses for application data traffic between the organization and its business partners Source

Failover

1. **Recommended:** The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby system upon the failure or abnormal termination of the previously active system Source
2. Alternative 1: Where you have systems configured in a High Availability setup, a Failover is

where you switch from the active element to the standby element Source

3. Alternative 2: The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system Source

False Positive

1. **Recommended:** An instance in which a security system gives an Alert that turns out to be spurious. False Positives are inevitable in many security systems that work on statistical probability when establishing whether a threat exists Source
2. Alternative 1: An alert that incorrectly indicates that a vulnerability is present Source
3. Alternative 2: An erroneous acceptance of the hypothesis that a statistically significant event has been observed. This is also referred to as a type 1 error. When "health-testing" the components of a device, it often refers to a declaration that a component has malfunctioned – based on some statistical test(s) – despite the fact that the component was actually working correctly Source

Firewall

1. **Recommended:** A device that filters traffic between two networks (commonly between a private LAN and the Internet) in order to ensure that only the desired connections can happen. Often old and obsolete and running an antique version of the firmware that's so long in the tooth as to make the device's existence largely pointless Source
2. Alternative 1: An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open Source
3. Alternative 2: An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall) Source

Firmware

1. **Recommended:** Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs Source
2. Alternative 1: Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution Source
3. Alternative 2: Computer programs and associated data that may be dynamically written or modified during execution Source

Forensic Copy

1. **Recommended:** An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm Source
2. Alternative 1: A copy of a computer disk that is used for forensic analysis, generally set to be read-only so that the content cannot be damaged by the investigation process Source
3. Alternative 2: A bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm Source

Forensics

See **Digital Forensics**

Formal Proof

1. **Recommended:** A formal proof is a proof in which every logical inference has been checked all the way back to the fundamental axioms of mathematics. All the intermediate logical steps are supplied, without exception Source
2. Alternative: A step-by-step sequence of mathematical operations that show unequivocally that a theorem is true Source

GDPR

1. **Recommended:** The General Data Protection Regulation (EU) (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an important component of EU privacy law and of human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also addresses the transfer of personal data outside the EU and EEA areas Source
2. Alternative: The GDPR aims to regulate the processing of personal data of individuals, hereafter referred to as “EU citizens,” residing in the European Economic Area (EEA), i.e., EU member states and Iceland, Liechtenstein, and Norway. The GDPR is designed to have a wider scope and includes other major changes that take into account the current cybersecurity landscape Source

Governance, Risk Management and Compliance

1. **Recommended:** Three aspects of organisational management that aim to ensure the organisation and its people behave ethically, run the organisation effectively, take appropriate measures to mitigate risks and maintain compliance with internal policies and external regulations Source
2. Alternative 1: GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity Source
3. Alternative 2: GRC as an acronym stands for governance, risk, and compliance, but the

term GRC means much more than that. The OCEG (formerly known as “Open Compliance and Ethics Group”) states that the term GRC was first referenced as early as 2003, but was mentioned in a peer reviewed paper by their co-founder in 2007 Source

Graduated Security

1. **Recommended:** A system that has various levels of security based on the nature of the different data sets stored and processed Source
2. Alternative: Graduated security refers to a model or architecture in which information security is implemented in multiple layers based on the requirements, threats and vulnerabilities of the system or environment. It enables securing a system in several different protection modes that work on par with the base requirement of the underlying IT system, environment or infrastructure Source

Hack

1. **Recommended:** A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals Source
2. Alternative 1: Unauthorized attempt or access to an information system Source
3. Alternative 2: Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. And while hacking might not always be for malicious purposes, nowadays most references to hacking, and hackers, characterize it/them as unlawful activity by cybercriminals—motivated by financial gain, protest, information gathering (spying), and even just for the “fun” of the challenge Source

Hacker

1. **Recommended:** Traditionally, someone who uses novel techniques to achieve something with a computer system. These days, someone who attempts to break into computer systems Source
2. Alternative: Unauthorized user who attempts to or gains access to an information system Source

Hardening

1. **Recommended:** Taking a default installation of a computer system (particularly a server) and changing its configuration to make it more secure - by disabling system components that aren't used, for instance, or by enabling on-board security software Source
2. Alternative 1: A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services Source
3. Alternative 2: Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system’s attack surface. By removing

superfluous programs, accounts functions, applications, ports, permissions, access, etc. attackers and malware have fewer opportunities to gain a foothold within your IT ecosystem Source

Hash Function

1. **Recommended:** An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message Source
2. Alternative: A function that maps a bit string of arbitrary length to a fixed length bit string and is expected to have the following three properties: 1) Collision resistance (see Collision resistance), 2) Preimage resistance (see Preimage resistance) and 3) Second preimage resistance (see Second preimage resistance) Source

High Availability

1. **Recommended:** Implementation of a system using multiple devices so that if one fails, the others will automatically take over service Source
2. Alternative 1: A failover feature to ensure availability during device or component interruptions Source
3. Alternative 2: High availability (HA) is a component of a technology system that eliminates single points of failure to ensure continuous operations or uptime for an extended period. High Availability solutions ensure your systems, databases, and applications operate when and as needed Source

Honeypot

1. **Recommended:** A honeypot is a cybersecurity mechanism that uses a manufactured attack target to lure cybercriminals away from legitimate targets. They also gather intelligence about the identity, methods and motivations of adversaries Source
2. Alternative 1: A system (generally a Web site) that is set up to entice attackers, and which does not contain any of the organisation's sensitive data Source
3. Alternative 2: One honeypot definition comes from the world of espionage, where Mata Hari-style spies who use a romantic relationship as a way to steal secrets are described as setting a ‘honey trap’ or ‘honeypot’. Often, an enemy spy is compromised by a honey trap and then forced to hand over everything he/she knows Source

Host Intrusion Prevention System

1. **Recommended:** A system that runs on computers (typically servers) to identify and block intrusion attempts that somehow got through the firewall. A component of Defense in Depth Source
2. Alternative 1: A program that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity Source
3. Alternative 2: By definition HIPS is an installed software package which monitors a single

host for suspicious activity by analyzing events occurring within that host. In other words a Host Intrusion Prevention System (HIPS) aims to stop malware by monitoring the behavior of code. This makes it possible to help keep your system secure without depending on a specific threat to be added to a detection update Source

HTTP tunnel

1. **Recommended:** HTTP tunneling is used to create a network link between two computers in conditions of restricted network connectivity including firewalls, NATs and ACLs, among other restrictions. The tunnel is created by an intermediary called a proxy server which is usually located in a DMZ Source
2. Alternative 1: HTTP Tunneling is a technique by which communications using various network protocols are encapsulated(masked) using the HTTP (80,8080,443)protocol, since HTTP protocol is not Monitored or can't be blocked by Firewall Source
3. Alternative 2: HTTP tunneling is used to bypass firewalls and other network restrictions and an HTTP tunnel is used to create a direct network link between two locations. A tunnel is used to ship a foreign protocol across a network that normally wouldn't support it. You can take protocol A and wrap it or put it in a tunnel with protocol B Source

Hybrid Instructor-Led Training

1. **Recommended:** Instructor-Led Training that is conducted with a mix of classroom-based sessions and Online Instructor-Led Training Source
2. Alternative 1: Hybrid instructor-led training incorporates both a traditional classroom setting and a virtual learning environment. This approach allows learners from remote locations to interact and participate in an instructor-led classroom through the use of technology Source
3. Alternative 2: With the migration of schools, universities, and workplaces to remote meetings and virtual classrooms, the term hybrid learning is popping up in education and learning and development conversations. Although some educational institutions use the term interchangeably with other terms, like blended learning or even virtual learning, these terms actually describe different ways to interact with and teach learners using digital platforms. This article explores some of these approaches to remote learning Source

Impact

1. **Recommended:** The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability Source
2. Alternative 1: With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII Source
3. Alternative 2: The effect on organizational operations, organizational assets, individuals,

other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system Source

Inadvertent Disclosure

1. **Recommended:** Type of incident involving accidental exposure of information to an individual not authorized access Source
2. Alternative 1: Where someone unwittingly sends sensitive information outside the company systems Source
3. Alternative 2: Accidental exposure of information to a person not authorized access Source

Incident Response Plan

1. **Recommended:** The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s) Source
2. Alternative 1: Largely synonymous with a **Business Continuity Plan**
3. Alternative 2: Incident response is a structured process organizations use to identify and deal with cybersecurity incidents. Response includes several stages, including preparation for incidents, detection and analysis of a security incident, containment, eradication, and full recovery, and post-incident analysis and learning Source

Incident Response

1. **Recommended:** An organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs Source
2. Alternative 1: The mitigation of violations of security policies and recommended practices Source
3. Alternative 2: An IT security incident is an adverse event in a computer system or network caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms Source

Incident

1. **Recommended:** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices Source
2. Alternative 1: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies Source
3. Alternative 2: Anomalous or unexpected event, set of events, condition, or situation at any time during the life cycle of a project, product, service, or system Source

Indicator

1. **Recommended:** A technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred Source
2. Alternative 1: A signal that a cyber incident may have occurred or is in progress Source
3. Alternative 2: Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack Source

Industrial Control System

1. **Recommended:** The control unit for a non-IT system, such as an air conditioning system or heavy machine plant. Industrial Control Systems are increasingly being provided with network interfaces to permit them to be managed remotely, which has made them a common target for cyber attack as they have a reputation for having poor security features. ICS is commonly used synonymously with Supervisory Control and Data Acquisition systems Source
2. Alternative 1: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes Source
3. Alternative 2: General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy) Source

Information Owner

1. **Recommended:** Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal Source
2. Alternative 1: The individual who has Accountability for a given collection of data Source
3. Alternative 2: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. See information steward. Note: Information steward is a related term, but it is not identical to information owner Source

Information Security Architect

1. **Recommended:** The person within the organisation who designs the systems and technology for implementing and maintaining Information Security Source
2. Alternative 1: Individual, group, or organization responsible for ensuring that the

information security requirements necessary to protect the organization’s core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes Source
3. Alternative 2: A security architect creates and designs security for a system or service, maintains security documentation and develops architecture patterns and security approaches to new technologies. At this level, you will: recommend security controls and identify solutions that support a business objective Source

Information security policy

1. **Recommended:** A high-level policy of an organization that is created to support and enforce portions of the organization’s Information Management Policy by specifying in more detail what information is to be protected from anticipated threats and how that protection is to be attained Source
2. Alternative 1: The directives, regulations, rules, and practices that form an organisation’s strategy for managing, protecting and distributing information Source
3. Alternative 2: Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information Source

Information Security

1. **Recommended:** The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability Source
2. Alternative 1: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability Source
3. Alternative 2: The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability Source

Inside Threat

1. **Recommended:** The threat of a security attack that originates inside the organisation, such as a disgruntled employee Source
2. Alternative 1: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities Source
3. Alternative 2: An insider threat refers to a cyber security risk that originates from within an organization. It typically occurs when a current or former employee, contractor, vendor or partner with legitimate user credentials misuses their access to the detriment of the organization's networks, systems and data Source

Instructor-Led Training

1. **Recommended:** Interactive training in which a qualified trainer teaches one or more students face-to-face in a classroom-like environment Source
2. Alternative: Instructor-led training is any kind of training that occurs in a training room, typically in an office, classroom, or conference room. This form of training can have one or more instructors. And they teach skills or material to another person or group through lectures, presentations, demonstrations, and discussions Source

Integrity

1. **Recommended:** The property that data or information have not been altered or destroyed in an unauthorized manner Source
2. Alternative 1: The correctness of data. If data is corrupted or altered it becomes useless, and so an attack on data integrity is often just as bad as an attack that steals data Source
3. Alternative 2: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity Source

Interactive application security testing

1. **Recommended:** IAST (interactive application security testing) is an application security testing method that tests the application while the app is run by an automated test, human tester, or any activity “interacting” with the application functionality Source
2. Alternative 1: IAST (interactive application security testing) analyzes code for security vulnerabilities while the app is run by an automated test, human tester, or any activity “interacting” with the application functionality Source
3. Alternative 2: Interactive application security testing (IAST) is an application security testing method that tests your application for vulnerabilities in execution, while the app is actually being used (either by a real user or an automated test runner) Source

Internal Network

1. **Recommended:** A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology provides the same effect. An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned Source
2. Alternative 1: The network connecting all of an organisation's internal systems together Source
3. Alternative 2: Leans a private, proprietary network resource accessible only by employees and individual contractors (i.e., temporary employees) of a specific corporation or similar business entity. Internal Network does not include portions of the Internet or any other network community open to the public, such as membership or subscription driven groups, associations and similar organizations Source

Internal Security Testing

1. **Recommended:** Security testing conducted from inside the organization's security perimeter Source
2. Alternative 1: Probing the Internal Network to see how susceptible it is to an attack from within (or by an intruder who has managed to gain access) Source
3. Alternative 2: An internal network or infrastructure penetration test assesses the extent of your vulnerability to insider attacks. An insider is anyone with access to organisational applications, systems and data, such as employees, contractors or partners. The target is typically the same as an external penetration test, but relies on some sort of authorized access or starts from a point within your network. Our internal network test will assess specified internal-facing network devices, using both automated scans and advanced manual testing techniques to assess your security and identify vulnerabilities Source

Interoperability

1. **Recommended:** The ability of one entity to communicate with another entity Source
2. Alternative 1: Interoperability is the ability of two or more systems to exchange health information and use the information once it is received. It will take time for all types of health IT to be fully interoperable Source
3. Alternative 2: Health information exchange (HIE) is frequently cited as an important objective of health information technology investment because of its potential to improve quality, reduce cost, and increase patient satisfaction. In this paper we examine the status and practices of HIE in six countries, drawn from a range of higher and lower income regions Source

Intrusion Detection System

1. **Recommended:** Software which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment Source
2. Alternative 1: Software that automates the intrusion detection process Source
3. Alternative 2: IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host- based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks Source

Intrusion Prevention System

1. **Recommended:** An intrusion prevention system (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur Source

2. Alternative 1: An intrusion prevention system (IPS) – sometimes referred to as an intrusion detection prevention system (IDPS) – is a network security technology and key part of any enterprise security system that continuously monitors network traffic for suspicious activity and takes steps to prevent it. Largely automated, IPS solutions help filter out this malicious activity before it reaches other security devices or controls, effectively reducing the manual effort of security teams and allowing other security products to perform more efficiently Source
3. Alternative 1: Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents Source

Intrusion

1. **Recommended:** A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so Source
2. Alternative: Any set of actions that attempts to compromise the integrity, confidentiality, or availability of a resource Source

IP Security

1. **Recommended:** Provide(s) interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality Source
2. Alternative 1: A protocol that adds security features to the standard IP protocol to provide confidentiality and integrity services Source
3. Alternative 2: IPsec is a group of protocols that are used together to set up encrypted connections between devices. It helps keep data sent over public networks secure. IPsec is often used to set up VPNs, and it works by encrypting IP packets, along with authenticating the source where the packets come from Source

IP spoofing

1. **Recommended:** IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure Source
2. Alternative 1: A tactic used by attackers to supply a false IP address in an attempt to trick the user or a cyber security solution into believing it is a legitimate actor Source
3. Alternative 2: Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity. It's one of many tools that hackers use to gain access to computers to mine them for sensitive data, turn them into zombies (computers taken over for malicious use), or launch Denial-of-Service (DoS) attacks. Of the different types of spoofing, IP spoofing is the most common Source

IT Security Policy

1. **Recommended:** A high-level policy of an organization that is created to support and enforce portions of the organization’s Information Management Policy by specifying in more detail what information is to be protected from anticipated threats and how that protection is to be attained Source
2. Alternative 1: A set of rules that are applied to all members of an organisation regarding acceptable use of its IT systems in a security-specific sense Source
3. Alternative 2: Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information Source

Jailbreak

1. **Recommended:** The removal of a device’s security restrictions, with the intention of installing unofficial apps and making modifications to the system. Typically applied to a mobile phone Source
2. Alternative 1: Jailbreaking is the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features. It is called jailbreaking because it involves freeing users from the ‘jail’ of limitations that are perceived to exist Source
3. Alternative 2: Jailbreaking refers to removing software restrictions built into iOS devices such as iPhones and iPads. Before springing your Apple product out of software jail, consider this: Is jailbreaking safe? Is jailbreaking legal? One thing’s for sure, jailbreaking exposes your device to viruses and other security threats. So before playing your get out of jail card, shore up your phone with a strong antivirus and security app Source

Jamming

1. **Recommended:** A deliberate communications disruption meant to degrade the operational performance of the RF subsystem. Jamming is achieved by interjecting electromagnetic waves on the same frequency that the reader to tag uses for communication Source
2. Alternative 1: An attack that attempts to interfere with the reception of broadcast communications Source
3. Alternative 2: The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing the effective use of a signal Source

JavaScript-Binding-Over-HTTP

1. **Recommended:** A form of Android-focused mobile device attack that enables an attacker to be able to initiate the execution of arbitrary code on a compromised device. A JBOH attack often takes place or is facilitated through compromised or malicious apps Source
2. Alternative 1: A mobile device attack that enables an attacker to execute arbitrary code on a previously compromised device Source
3. Alternative 2: JBOH (JavaScript-Binding-Over-HTTP) is a mobile device attack that enables

an attacker to execute arbitrary code on a previously compromised device. These attacks are known to be deployed through malicious JBOH Android software applications Source

Key Escrow

1. **Recommended:** Key escrow is a method of storing important cryptographic keys. Each key stored in an escrow system is tied to the original user and subsequently encrypted for security purposes. Much like a valet or coat check, each key is stored in relation to the user that leverages it, and then returned once queried. By using key escrow, organizations can ensure that in the case of catastrophe, be it a security breach, lost or forgotten keys, natural disaster, or otherwise, their critical keys are safe Source
2. Alternative 1: Where one lodges a copy of a Key with a trusted third party, generally when there is a risk of one of the two parties involved in the data exchange going out of business Source
3. Alternative 2: The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery Source

Key Exchange

1. **Recommended:** The process of exchanging a Public Key between the sender and receiver of a piece of data Source
2. Alternative 1: Process of exchanging public keys (and other information) in order to establish secure communications Source
3. Alternative 2: The key exchange method specifies how one-time session keys are generated for encryption and for authentication, and how the server authentication is done. The Diffie-Hellman Key Exchange is a method for exchanging secret keys over a non-secure medium without exposing the keys Source

Key Logger

1. **Recommended:** A rogue piece of software or hardware that monitors what a user types on a keyboard (which potentially includes usernames and passwords) and sends it to an attacker Source
2. Alternative 1: A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures Source
3. Alternative 2: A keylogger is an insidious form of spyware You enter sensitive data onto your keyboard, believing nobody is watching. In fact, keylogging software is hard at work logging everything that you type Source

Key

1. **Recommended:** In cryptography, a key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it Source
2. Alternative 1: A parameter used in a cryptographic algorithm: you apply the algorithm to

the Plain Text and the key, and the result is the Cipher Text. If a different key is used for the same Plain Text, the result will be a different Cipher Text Source

3. Alternative 2: An encryption key is a random string of bits created explicitly for scrambling and unscrambling data. Encryption keys are designed with algorithms intended to ensure that every key is unpredictable and unique. The longer the key built in this manner, the harder it is to crack the encryption code. An encryption key is used to encrypt, decrypt, or carry out both functions, based on the sort of encryption software used Source

Least Privilege

1. **Recommended:** The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function Source
2. Alternative 1: The principle of assigning every user with only the privileges they actually need to do their job, and no more Source
3. Alternative 2: The principle of least privilege (PoLP) refers to an information security concept in which a user is given the minimum levels of access – or permissions – needed to perform his/her job functions Source

Link Encryption

1. **Recommended:** A situation in which the entire end-to-end connection between the sending endpoint and the receiving endpoint is encrypted in some way Source
2. Alternative 1: Encryption of information between nodes of a communications system Source
3. Alternative 2: Link Encryption is a technique in which a communication traveling along a network is encrypted and decrypted at every stage, or node. It is used to prevent traffic analysis and avoid human error Source

Local Area Network

1. **Recommended:** A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network Source
2. Alternative 1: A collection of network-connected computers and other electronic systems that are all located within a specific location such as a home, office or other building, and are hence “local” to each other Source
3. Alternative 2: LAN stands for local area network. A network is a group of two or more connected computers, and a LAN is a network contained within a small geographic area, usually within the same building. Home WiFi networks and small business networks are common examples of LANs. LANs can also be fairly large, although if they take up multiple buildings, it is usually more accurate to classify them as wide area networks (WAN) or metropolitan area networks (MAN) Source

Logic Bomb

1. **Recommended:** A piece of malicious code that's planted in a computer system and set to activate when certain conditions are met (for example a particular date and time being reached) Source
2. Alternative 1: A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met Source
3. Alternative 2: A logic bomb may sound like a nugget of truth you drop on your friends to demonstrate your intelligence, but in computing, it's a cybersecurity attack. Not only can logic bombs wipe your precious data, but they may bring your operations to a halt. And just like real bombs, these threats can hit your organization when you least expect them Source

Macro Virus

1. **Recommended:** A **virus** that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate Source
2. Alternative 1: A piece of Malware that exploits the macro languages in popular applications such as word processor and spreadsheet software Source
3. Alternative 2: A specific type of computer virus that is encoded as a macro embedded in some document and activated when the document is handled Source

Malicious Code

1. **Recommended:** Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content Source
2. Alternative 1: Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses Source
3. Alternative 1: Malicious code is the kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors, security breaches, information and data theft, and other potential damages to files and computing systems. It's a type of threat that may not be blocked by antivirus software on its own Source

Malvertising

1. **Recommended:** Malvertising is an attack in which perpetrators inject malicious code into legitimate online advertising networks. The code typically redirects users to malicious websites Source
2. Alternative 1: Malvertising, or malicious advertising, is the term for criminally controlled advertisements within Internet connected programs, usually web browsers (there are exceptions), which intentionally harm people and businesses with all manner of malware,

potentially unwanted programs (PUPs), and assorted scams. In other words, malvertising uses what looks like legitimate online advertising to distribute malware and other threats with little to no user interaction required Source

3. Alternative 2: Aka malicious advertising — is a relatively new cyberattack technique that injects malicious code within digital ads. Difficult to detect by both internet users and publishers, these infected ads are usually served to consumers through legitimate advertising networks. Because ads are displayed to all website visitors, virtually every page viewer is at risk of infection Source

Malware

1. **Recommended:** Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code Source
2. Alternative 1: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim Source
3. Alternative 2: Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose Source

Man-in-the-middle

1. **Recommended:** An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them Source
2. Alternative 1: A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association Source
3. Alternative 2: An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them. In the context of authentication, the attacker would be positioned between claimant and verifier, between registrant and CSP during enrollment, or between subscriber and CSP during authenticator binding Source

Manual Key Transport

1. **Recommended:** A non-automated means of transporting cryptographic keys by physically moving a device or document containing the key or key share Source
2. Alternative: The approach of providing a third party Key in person or by phone rather than letting systems exchange it automatically Source

Media

1. **Recommended:** Physical storage devices such as tapes, disks or USB memory sticks Source
2. Alternative: Computer media is a term that is often used in informatics with several different meanings. It is used to describe the electronic devices used to store data, such as

hard drives, USB drives, DVDs, CD-ROM, and floppy disks Source

Message Digest 5

1. **Recommended:** A well-known Hash Function which is considered insecure owing to its susceptibility to Collisions Source
2. Alternative: **Message Digest** algorithm version 5

Message Digest

1. **Recommended:** The result of applying a hash function to a message. Also known as a “hash value” or “hash output” Source
2. Alternative 1: A hash that uniquely identifies data. Changing a single bit in the data stream used to generate the message digest will yield a completely different message digest Source
3. Alternative 2: The fixed-length bit string produced by a hash function Source

Metrics

1. **Recommended:** Quantitative data collected concerning performance, security attacks and the like Source
2. Alternative: Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data Source

Minus Day/Zero day

See zero day

Mission Critical

1. **Recommended:** Denotes a system that is critical to the organisation's operation, and whose demise as a result of a security incident would cause major impact Source
2. Alternative 1: Any telecommunications or information system that is defined as a national security system (FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency Source
3. Alternative 2: A mission critical task, service, or system is one whose failure or disruption would cause an entire operation or business to grind to a halt. It is a type of task, service, or system that is indispensable to continuing operations Source

Mitigation

1. **Recommended:** The steps taken to minimize and address cyber security risks Source

2. Alternative 1: A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities Source
3. Alternative 1: Reduction in severity or seriousness of an event. In cybersecurity, mitigation is centered around strategies to limit the impact of a threat against data in custody. Threats against data can come from outside attackers motivated by profit, activism, retribution, or mischief Source

Mobile Device Management

1. **Recommended:** Mobile device management (MDM) is a type of security software, specifically for monitoring, managing and securing mobile, tablet and other devices, allowing remote administration and management of the device Source
2. Alternative 1: The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices Source
3. Alternative 2: A Mobile Device Management (MDM) service combines device applications, built-in device management features and infrastructure services. Together, these components allow your organisation to remotely control, monitor, and enforce policies on employee devices Source

Multi Factor Authentication

1. **Recommended:** Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric) Source
2. Alternative 1: Generally used synonymously with Two Factor Authentication, though Multi Factor Authentication may use more than two different identification mechanisms Source
3. Alternative 2: The means used to confirm the identity of a user, process, or device (e.g., user password or token) Source

Multilevel Security

1. **Recommended:** Multilevel security or multiple levels of security is the application of a computer system to process information with incompatible classifications, permit access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization Source
2. Alternative 1: Multilevel security (MLS) is a technology to protect secrets from leaking between computer users, when some are allowed to see those secrets and others are not. This is generally used in defense applications (the military and intelligence communities) since nobody else is nearly as paranoid about data leaking Source
3. Alternative 2: A fundamental requirement of a secure system is that there is a set of guidelines that specify the authorization of subjects to access specific objects. “Access” is a key concept; it implies a flow of information from a subject to an object or from an object to a subject. For example, when a user (a subject) updates a data set (an object), the

information flows from the subject to the object. When a user reads a record from a data set, the information flows from the object to the subject Source

Mutual Authentication

1. **Recommended:** Two parties authenticating each other at the same time. Also known as mutual authentication or two-way authentication Source
2. Alternative 1: The act of two parties in a data exchange authenticating each other prior to transmission taking place Source
3. Alternative 2: The process of both entities involved in a transaction verifying each other. See bidirectional authentication Source

Mutual Suspicion

1. **Recommended:** Condition in which two information systems need to rely upon each other to perform a service, yet neither trusts the other to properly protect shared data Source
2. Alternative: An approach whereby neither party in a data exchange trusts the other, and hence each insists on the other authenticating itself Source

Need-To-Know

1. **Recommended:** Where users only have access to systems and data they need in order to do their job. Synonymous with Least Privilege Source
2. Alternative: The need to know principle can be enforced with user access controls and authorization procedures and its objective is to ensure that only authorized individuals gain access to information or systems necessary to undertake their duties Source

Network Admission Control

1. **Recommended:** Also known as network admission control, is the process of restricting unauthorized users and devices from gaining access to a corporate or private network. NAC ensures that only users who are authenticated and devices that are authorized and compliant with security policies can enter the network Source
2. Alternative 1: A mechanism whereby the network infrastructure forbids a device from communicating until it has proven its identify and that its operating software and Anti-Malware Software are up to date Source
3. Alternative 2: A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the telework client device Source

Network Sniffing

1. **Recommended:** A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique Source
2. Alternative 1: The act of putting a monitor on a network and capturing/examining the

traffic as it flies past Source

3. Alternative 2: Network sniffing is the practice of using a network interface on a computer system to monitor or capture information regardless of whether it is the specified destination for the information Source

Network

1. **Recommended:** Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices Source
2. Alternative 1: An open communications medium, typically the Internet, used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the network’s security; it is assumed to be open and subject to active (e.g., impersonation, man-in-the- middle, session hijacking) and passive (e.g., eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP, RP) Source
3. Alternative 2: A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices Source

Non-repudiation

1. **Recommended:** Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information Source
2. Alternative 1: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information Source
3. Alternative 2: Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message Source

One Time Pad

1. **Recommended:** Manual one-time cryptosystem produced in pad form Source
2. Alternative 1: A paper pad of encryption Keys on which each key is different from the next and where there is no discernible pattern to the various keys. The sender and receiver must have the same One-Time Pads in order that the receiver can decrypt the message. One of the most secure approaches to an Encryption Algorithm so long as nobody is able to duplicate the One Time Pad Source
3. Alternative 2: The One-Time Pad, or OTP is an encryption technique in which each character of the plaintext is combined with a character from a random key stream. Originally described in 1882 by banker Frank Miller (USA), it was re-invented in 1917 by

Gilbert Vernam and Joseph Mauborgne. When applied correctly, the OTP provides a truely unbreakable cipher. It is named after the sheets of paper (pads) on which the key stream was usually printed. It also exists as One Time Tape (OTT) Source

One-Way Hash Function

See **Hash Function**

Open Web Application Security Project

1. **Recommended:** The Open Web Application Security Project, or OWASP, is an international non-profit organization dedicated to web application security. One of OWASP's core principles is that all of their materials be freely available and easily accessible on their website, making it possible for anyone to improve their own web application security. The materials they offer include documentation, tools, videos, and forums. Perhaps their best-known project is the OWASP Top 10 Source
2. Alternative 1: An online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. The Open Web Application Security Project provides free and open resources Source
3. Alternative 2: The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web Source

Operations Security

1. **Recommended:** Operational security (OPSEC), also known as procedural security, is a risk management process that encourages managers to view operations from the perspective of an adversary in order to protect sensitive information from falling into the wrong hands Source
2. Alternative 1: The concept of taking a systemic, proactive approach to the operation of the security function in your organisation Source
3. Alternative 2: Operational security (OPSEC) is a security and risk management process that prevents sensitive information from getting into the wrong hands. Another OPSEC meaning is a process that identifies seemingly innocuous actions that could inadvertently reveal critical or sensitive data to a cyber criminal. OPSEC is both a process and a strategy, and it encourages IT and security managers to view their operations and systems from the perspective of a potential attacker. It includes analytical activities and processes like behavior monitoring, social media monitoring, and security best practice Source

Outside Threat

1. **Recommended:** A threat posed by a system or individual outside your organisation's network and premises Source
2. Alternative 1: An unauthorized entity outside the security domain that has the potential to

harm an information system through destruction, disclosure, modification of data, and/or denial of service Source

3. Alternative 2: Insider threats present a complex and dynamic risk affecting the public and private domains of all critical infrastructure sectors. This section provides an overview to help frame the discussion of insiders and the threats they pose; defining these threats is a critical step in understanding and establishing an insider threat mitigation program Source

Outsourcing

1. **Recommended:** The business practice of hiring a party outside a company to perform services or create goods that were traditionally performed in-house by the company's own employees and staff Source
2. Alternative 1: Outsourcing is the business practice of hiring a party outside a company to perform services or create goods that were traditionally performed in-house by the company's own employees and staff. Outsourcing is a practice usually undertaken by companies as a cost-cutting measure Source
3. Alternative 2: Outsourcing can bring big benefits to your business, but there are significant risks and challenges when negotiating and managing outsourcing relationships. Here, we break down everything you need to know to ensure your IT outsourcing initiatives succeed Source

Over-The-Air

1. **Recommended:** In general, OTA may refer to any wireless system that uses open space as its transmission medium, including TV, Wi-Fi, Bluetooth and cellular. An OTA update is a new version of the operating system sent via Wi-Fi to a phone, tablet or laptop computer Source
2. Alternative 1: An approach in which key exchange is carried out over the same path that the encrypted data is traversing Source
3. Alternative 2: Over-The-Air (OTA) is a technology that updates and changes data in the SIM card without having to reissue it. It is also referred to as Over-the-Air provisioning Source
4. Alternative 3: Over-the-air (OTA) refers to the wireless transmission of information. It is most commonly used for sending information to Internet-of-things (IoT) devices and for facilitating TV and radio broadcasts Source

Packet Filter

1. **Recommended:** Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports Source
2. Alternative 1: A mechanism, typically within a router or a firewall, that only allows specific types of traffic to and from specific addresses Source
3. Alternative 2: A routing device that provides access control functionality for host addresses and communication sessions Source

Packet Sniffer

1. **Recommended:** Software that observes and records network traffic Source
2. Alternative 1: Software that monitors network traffic on wired or wireless networks and captures packets Source
3. Alternative 2: The piece of software that does Network Sniffing Source

Passive Attack

1. **Recommended:** Synonymous with an **Eavesdropping Attack**, where one listens into a transmission without actually interrupting it Source
2. Alternative 1: An attack that does not alter systems or data Source
3. Alternative 2: An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping) Source

Password Generator

1. **Recommended:** An application that generates complex, hard-to-crack **Password**s for Users Source
2. Alternative 1: A password generator is a tool that automatically generates a password based on guidelines that you set to create strong and unpredictable passwords for each of your accounts Source
3. Alternative 2: A password generator is a software tool that creates random or customized passwords for users. It helps users create stronger passwords that provide greater security for a given type of access Source

Password Protected

1. **Recommended: Password** protection is a security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information Source
2. Alternative 1: The ability to protect the contents of a file or device from being accessed until the correct password is entered. Source
3. Alternative 2: Password protection allows you to protect your data set by assigning it a password. Another user cannot read, change, or delete your data set without knowing the password Source

Password sniffing

1. **Recommended: Password** Sniffing is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic Source

2. Alternative 1: A password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password Source
3. Alternative 2: Password sniffing is an attack on the Internet that is used to steal user names and passwords from the network. Today, it is mostly of historical interest, as most protocols nowadays use strong encryption for passwords. However, it used to be the worst security problem on the Internet in the 1990s, when news of major password sniffing attacks were almost weekly Source

Password

1. **Recommended:** A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization Source
2. Alternative 1: Confidential authentication information, usually composed of a string of characters Source
3. Alternative 2: A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data Source

Patch Management

1. **Recommended:** The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs Source
2. Alternative 1: A regime of regularly downloading and applying the Patches required for your systems and monitoring Patch currency Source
3. Alternative 2: Patch management is about keeping software on computers and network devices up to date and capable of resisting low-level cyber attacks. Any software is prone to technical vulnerabilities. Once discovered and shared publicly, these can rapidly be exploited by cyber criminals. Criminal hackers can take advantage of known vulnerabilities in operating systems and third-party applications if they are not properly patched or updated Source

Patch

1. **Recommended:** A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component Source
2. Alternative 1: An update for an operating system or software application, to correct a functional problem or security vulnerability Source
3. Alternative 2: A “repair job” for a piece of programming; also known as a “fix”. A patch is the immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary

file or object module). In many operating systems, a special program is provided to manage and track the installation of patches Source

Payload

1. **Recommended:** In the context of a cyber-attack, a payload is the component of the attack which causes harm to the victim. Much like the Greek soldiers hiding inside the wooden horse in the tale of the Trojan Horse, a malicious payload can sit harmlessly for some time until triggered Source
2. Alternative 1: In cybersecurity, a payload is malware that the threat actor intends to deliver to the victim. For example, if a cybercriminal sent out an email with a malicious Macro as the attachment and the victim gets infected with ransomware, then the ransomware is the payload (and not the email or document) Source
3. Alternative 2: Consists of the information passed down from the previous layer Source

Peer Review

1. **Recommended:** Peer review is designed to assess the validity, quality and often the originality of articles for publication. Its ultimate purpose is to maintain the integrity of science by filtering out invalid or poor quality articles. From a publisher's perspective, peer review functions as a filter for content, directing better quality articles to better quality journals and so creating journal brands Source
2. Alternative 1: Reviewers play a pivotal role in scholarly publishing. The peer review system exists to validate academic work, helps to improve the quality of published research, and increases networking possibilities within research communities Source
3. Alternative 2: The peer review process starts once you have submitted your paper to a journal. After submission, your paper will be sent for assessment by independent experts in your field. The reviewers (who also known as referees) are asked to judge the validity, significance, and originality of your work. Below we expand on what is peer review is, and how the peer review works. It is important to fully understand the process, as it will help you know how to make sure that every article you publish, is as good as it can be Source

Penetration Testing

1. **Recommended:** Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability Source
2. Alternative 1: A method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources Source
3. Alternative 2: Testing that verifies the extent to which a system, device or process resists active attempts to compromise its security Source

Perimeter

1. **Recommended:** Perimeter security in cybersecurity refers to the process of defending a company's network boundaries from hackers, intruders, and other unwelcome individuals. This entails surveillance detection, pattern analysis, threat recognition, and effective response. Each private network is surrounded by a perimeter Source
2. Alternative 1: The point at which a private network meets the public Internet Source
3. Alternative 1: Encompasses all those components of the system that are to be accredited by the DAA, and excludes separately accredited systems to which the system is connected Source

Personal data breach

1. **Recommended:** Data breach related to **Personal Data**
2. Alternative: A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes Source

Personal Data

1. **Recommended:** Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data Source
2. Alternative 1: Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual Source
3. Alternative 2: Any information relating to an identified or identifiable natural person (data subject) Source

Personal Firewall

1. **Recommended:** A personal firewall is software application that shields internet users from potential hackers by permitting or denying network traffic to and from their computer and warning them about attempted intrusions. It's like a filter between the Internet and your network Source
2. Alternative 1: Security software that resides on an individual PC or other computer Source
3. Alternative 2: A personal firewall is a software resource that controls network traffic to and from a single computer. This is a common part of consumer computing security software, and something that may be sold along with individual anti-virus applications and other security programs for a single personal computer Source

Personal Identification Number

1. **Recommended:** A secret that a claimant memorizes and uses to authenticate his or her

identity. PINs are generally only decimal digits Source

2. Alternative 1: A passcode comprising only numeric digits, commonly used as authentication for users of credit and debit cards, and which is known only to the individual to whom the entity being protected has been entrusted Source
3. Alternative 2: A numeric secret that a cardholder memorizes and uses as part of authenticating their identity Source

Personally Identifiable Information

1. **Recommended:** See **Personal Data**
2. Alternative 1: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information Source
3. Alternative 2: Information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.) Source
4. Alternative 3: Personally Identifiable Information is Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means Source

Pharming

1. **Recommended:** An attack in which an attacker corrupts an infrastructure service such as DNS (Domain Name System) causing the subscriber to be misdirected to a forged verifier/RP, which could cause the subscriber to reveal sensitive information, download harmful software, or contribute to a fraudulent act Source
2. Alternative 1: An attack on network infrastructure where a user is redirected to an illegitimate website, despite having entered the right address Source
3. Alternative 2: Using technical means to redirect users into accessing a fake Web site masquerading as a legitimate one and divulging personal information Source

Phishing

1. **Recommended:** Tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites) Source
2. Alternative 1: A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person Source
3. Alternative 2: A digital form of social engineering that uses authentic-looking—but bogus—e-mails to request information from users or direct them to a fake Web site that requests information Source

Physically Isolated Network

1. **Recommended:** A network that is deliberately and entirely isolated from all others, in order to eliminate entirely the risk of a network-based intrusion Source
2. Alternative 1: Air-gapped networks are physically isolated from any public or private networks. Learn what they are and why you should try one Source
3. Alternative 2: Security measure that isolates a digital device or private local area network (LAN) from other devices and networks, including the public internet. An air gap is also known as an air wall and the strategy of using air gaps to protect critical data is also known as security by isolation Source

Port Scanning

1. **Recommended:** A simple test where a piece of software computer attempts to make every possible type of connection from the machine on which it is running to one or more other (target) machines. Used by Hackers as the first step in identifying potential vulnerabilities in a system Source
2. Alternative 1: Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports) Source
3. Alternative 2: A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization Source

POS Malware

1. **Recommended:** The goal of PoS malware is to steal information related to financial transactions, including credit card information Source
2. Alternative 1: A POS Intrusion is an attack that happens at the Point-of-Sale device. The POS device in retail stores process credit card transactions at check out. Newer devices allow you to Tap or Insert your credit card to charge you for your mechandise Source
3. Alternative 2: POS malware is specifically designed for point-of-sale (POS) terminals and systems with the intention of stealing payment card data. It is commonly used by cybercriminals who want to resell stolen customer data from retail stores. Payment card data is encrypted end-to-end and is only decrypted in the random-access memory (RAM) of the device while the payment is processing. A POS malware attack enters through compromised or weakly secured systems and scrapes the RAM to find payment card data, which is then sent unencrypted to the hacker Source

POS

Recommended: Point-Of-Sale Terminal or (POS device) in retail stores process credit card transactions at check out. Newer devices allow you to Tap or Insert your credit card to charge you for your mechandise Source

Privacy

1. **Recommended:** The ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively Source
2. Alternative 1: Maintaining the confidentiality of systems and data such that they are readable, and read, only by those authorised to do so Source
3. Alternative 2: Assurance that the confidentiality of, and access to, certain information about an entity is protected Source
4. Alternative 3: Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual Source

Private Key

1. **Recommended:** A cryptographic key that is kept secret and is used with a public-key cryptographic algorithm. A private key is associated with a public key Source
2. Alternative: A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key Source

Privilege

1. **Recommended:** A right granted to an individual, a program, or a process Source
2. Alternative 1: The rights that someone is granted to a computer system to control the types and levels of access they are given Source
3. Alternative 2: A special authorization that is granted to particular users to perform security relevant operations Source

Promiscuous Mode

1. **Recommended:** In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. In an Ethernet local area network (LAN), promiscuous mode is a mode of operation in which every data packet transmitted can be received and read by a network adapter Source
2. Alternative 1: The network card in your PC will, in normal operation, filter traffic that arrives over the network and only accept traffic that is addressed to it. If switched it to “promiscuous mode” it will accept everything that arrives - which is useful for (say) analysing all the traffic on a network segment for diagnostic purposes Source
3. Alternative 2: Promiscuous mode is a type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode. It is a network security, monitoring and administration technique that enables access to entire network data packets by any configured network adapter on a host system Source

Protocol

1. **Recommended:** In computer terms, a defined and agreed way of two systems interacting Source
2. Alternative 1: Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks Source
3. Alternative 2: The Internet Protocol, as defined in IETF RFC 6864, which is the principal communications protocol in the IETF Internet protocol suite for specifying system address information when relaying datagrams across network boundaries Source

Proxy

1. **Recommended:** A system that makes requests to a server on behalf of the client - useful because there is no direct end-to-end connection between the client and the server, thus reducing the risk of something nefarious at one the server from directly infecting the other Source
2. Alternative 1: An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a hyper text transfer protocol (HTTP) proxy used for Web access, and a simple mail transfer protocol (SMTP) proxy used for e-mail Source
3. Alternative 2: An agent that acts on behalf of a requester to relay a message between a requester agent and a provider agent. The proxy appears to the provider agent Web service to be the requester Source

Pseudorandom Number Generator

1. **Recommended:** An algorithm that generates numbers that are almost random, using sources of unpredictability within the host computer. Used because the generation of truly random numbers is complex and costly, and pseudorandom numbers are generally sufficient for most applications Source
2. Alternative 1: A pseudorandom number generator (PRNG) is a function that, once initialized with some random value (called the seed), outputs a sequence that appears random, in the sense that an observer who does not know the value of the seed cannot distinguish the output from that of a (true) Source
3. Alternative 2: A pseudorandom number generator (PRNG), also known as a deterministic random bit generator (DRBG), is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers Source

Public Key Cryptography

1. **Recommended:** A cryptographic algorithm that uses two related keys, a **Public Key** and a

Private Key. The two keys have the property that determining the private key from the public key is computationally infeasible Source

2. Alternative 1: Public-key cryptography (PKC) is a technology often used to validate the authenticity of data using asymmetric encryption. PKC was first used primarily to encrypt and decrypt messages in traditional computing. Cryptocurrencies now use this technology to encrypt and decrypt transactions. Without PKC, the technology underpinning cryptocurrencies would be practically impossible Source

Public Key Infrastructure

1. **Recommended:** A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. The PKI includes the hierarchy of certificate authorities that allow for the deployment of digital certificates that support encryption, digital signature and authentication to meet business and security requirements Source
2. Alternative 1: The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates Source
3. Alternative 2: A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and the storage of sensitive verification system data within identity cards and the verification system Source

Public Key

1. **Recommended:** A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key) Source
2. Alternative 1: The other of the two Cryptographic Keys in a Public Key Cryptography setup, alongside the Private Key Source
3. Alternative 2: A public key is created in public key encryption cryptography that uses asymmetric-key encryption algorithms. Public keys are used to convert a message into an unreadable format. Decryption is carried out using a different, but matching, private key. Public and private keys are paired to enable secure communication Source

Quarantine

1. **Recommended:** Quarantine is a technique used by anti-virus and anti-malware software to isolate infected files on a computer. Files identified by this software can include viruses and worms, as well as system files that have been infected Source
2. Alternative 1: A storage area to which Anti-Malware Software moves infected files for further inspection, removing them from their original locations in order that they cannot

cause damage Source
3. Alternative 2: Quarantine is a special isolated folder on a machine's hard disk where the suspicious files detected by Antivirus and Antimalware protection are placed to prevent further spread of threats Source

Radio Frequency Identification

1. **Recommended:** Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. Tags, which use radio waves to communicate their identity and other information to nearby readers, can be passive or active. Passive RFID tags are powered by the reader and do not have a battery. Active RFID tags are powered by batteries Source
2. Alternative 1: A mechanism assets are given passive electronic tags that respond with a unique identifier when irradiated with radio waves Source
3. Alternative 2: Radio Frequency Identification (RFID) is a technology that uses radio waves to passively identify a tagged object. It is used in several commercial and industrial applications, from tracking items along a supply chain to keeping track of items checked out of a library Source

Random Number Generator

1. **Recommended:** A process that is invoked to generate a random sequence of values (usually a sequence of bits) or an individual random value Source
2. Alternative 1: A system that uses a source of genuinely random data in order to generate random numbers for consumption by computers. As sources of random data can be expensive to implement, Pseudorandom Number Generators are often used in their stead Source
3. Alternative 2: A mechanism that purports to generate truly random dataSource

Ransomware

1. **Recommended:** Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom Source
2. Alternative 1: Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption Source
3. Alternative 2: Ransomware made headlines throughout 2021 and continues to make the news in 2022. You may have heard stories of attacks on large companies, organizations, or government agencies, or perhaps you as an individual have experienced a ransomware attack on your own device. It’s a significant problem and a scary prospect to have all of your files and data held hostage until you pay up. If you want to know more about this

threat, read on to learn about ransomware's different forms, how you get it, where it comes from, who it targets, and ultimately, what you can do to protect against it Source

Read Access

1. **Recommended:** Where a user who as access to data can only read it, not update or delete it Source
2. Alternative 1: The read only user role gives users access to most areas of Xero, without the ability to change data in an organisation. This user role would suit company directors, trustees, auditors or liquidators, who only need to view records in an organisation Source
3. Alternative 2: Adding this role to a user or group on the instance will cause all users with this role to immediately have read-only access to any tables they could previously modify or otherwise manipulate Source

Recovery Point Objective

1. **Recommended:** Recovery point objective (RPO) is defined as the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization. An RPOs determines the maximum age of the data or files in backup storage needed to be able to meet the objective specified by the RPO, should a network or computer system failure occur Source
2. Alternative 1: The point in time to which the data on a system must be recovered in the case of a data loss. For example, if the RPO is 24 hours, backups or snapshots must be taken at least daily Source
3. Alternative 2: The point in time to which data must be recovered after an outage Source

Recovery Procedures

1. **Recommended:** The sequence of actions taken to restore a failed system such that it is usable Source
2. Alternative 1: A recovery procedure is a process that attempts to bring a system back to a normal operating state Source
3. Alternative 2: You need to perform certain procedures to recover the system to minimize the impact of the issue reported in the system and to bring the system back to the normal operating state. The procedure re-creates the system by using saved configuration data or by restarting the affected services Source

Recovery Time Objective

1. **Recommended:** The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs Source
2. Alternative 1: The longest acceptable time between a system failing and it being returned to service such that it can be used, even if not optimally Source
3. Alternative 2: The overall length of time an information system's components can be in the

recovery phase before negatively impacting the organization's mission or mission/business processes Source

Red Team

1. **Recommended:** A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team Source
2. Alternative 1: A group of security specialists who analyses an organisation's systems by simulating cyber attacks on the system, in order to identify vulnerabilities that can then be mitigated. Often paired with a Blue Team in order to examine security from multiple angles Source
3. Alternative 3: A red team is a team that is formed with the objective of subjecting an organisation's plans, programs, ideas and assumptions to rigorous analysis and challenge Source

Redundancy

1. **Recommended:** Process through which additional or alternate instances of network devices, equipment or communication mediums are installed within network infrastructure. It is a method for ensuring network availability in case of a network device or path failure and unavailability Source
2. Alternative 1: Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process Source
3. Alternative 2: Enterprise IT operations strategize failure, recovery and business continuity plans that typically include redundancies for critical servers, network segments, security tools and internet connectivity, where a failure would cause significant downtime. In the event of a failure, redundancy allows your network to remain in service by providing alternative data paths or backup equipment Source

Remediation

1. **Recommended:** Corrective action undertaken to fix or mitigate a security vulnerability. Source
2. Alternative 1: Threat remediation is a strong and capable tool for fighting the cyber security compromises. As the word 'remedy' suggests, remediation process involves the treatment of a security breach Source
3. Alternative 2: This process of identifying and fixing problems is called cybersecurity remediation. It's a structured approach that your organization should create and use to intercept IT security threats before they do harm, as well as to resolve any issues that may have already occurred Source

Remote Access Trojan

1. **Recommended:** Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response Source
2. Alternative 1: Remote Access Trojans are programs that provide the capability to allow covert surveillance or the ability to gain unauthorized access to a victim PC. Remote Access Trojans often mimic similar behaviors of keylogger applications by allowing the automated collection of keystrokes, usernames, passwords, screenshots, browser history, emails, chat lots, etc. Source
3. Alternative 2: Malware developers code their software for a specific purpose, but to gain remote control of a user's device is the ultimate benefit for an attacker who wants to steal data or take over a user's computer. A Remote Access Trojan (RAT) is a tool used by malware developers to gain full access and remote control on a user's system, including mouse and keyboard control, file access, and network resource access. Instead of destroying files or stealing data, a RAT gives attackers full control of a desktop or mobile device so that they can silently browse applications and files and bypass common security such as firewalls, intrusion detection systems, and authentication controls Source

Remote Access

1. **Recommended:** A mechanism for users to access your organisation's systems from outside the organisation's premises Source
2. Alternative 1: Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet)Source
3. Alternative 2: Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device) Source

Remote Maintenance

1. **Recommended:** Carrying out system maintenance using Remote Access mechanisms Source
2. Alternative 1: Maintenance activities conducted by individuals communicating external to an information system security perimeter Source
3. Alternative 2: The basic definition of remote maintenance means that computer systems can be supervised and controlled from a remote location. This is done by placing software on local systems, that can be accessed from other locations Source

Removable Media

1. **Recommended:** Removable media is any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives. Removable media makes it easy for a

user to move data from one computer to another Source
2. Alternative 1: A storage device (such as a USB memory stick or a FireWire-connected hard drive) on which data can be stored for off-site transport Source
3. Alternative 2: Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD). See also portable storage device Source

Replay Attacks

1. **Recommended:** An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access Source
2. Alternative 1: An attack in which the attacker monitors and records traffic from your network then pushes the recording back into your system, perhaps with some subtle modifications, in order to break in or cause a problem Source
3. Alternative 2: An attack in which the Attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to masquerade as that Claimant to the Verifier or vice versa Source

Residual Risk

1. **Recommended:** Portion of risk remaining after security measures have been applied Source
2. Alternative 1: The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards Source
3. Alternative 2: Risk that remains after risk responses have been documented and performed Source

Resilience

1. **Recommended:** The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents Source
2. Alternative 1: The ability to maintain required capability in the face of adversity Source
3. Alternative 2: The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. Source

Right to Privacy

1. **Recommended:** Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used Source
2. Alternative 1: The right of a person to be free from intrusion into or publicity concerning matters of a personal nature Source
3. Alternative 2: The right to privacy is an element of various legal traditions that intends to restrain governmental and private actions that threaten the privacy of individuals Source

Risk Assessment

1. **Recommended:** The process of identifying and documenting risks that exist in an organisation Source
2. Alternative 1: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis Source
3. Alternative 2: Overall process of risk identification, risk analysis, and risk evaluation Source

Risk Management

1. **Recommended:** The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time Source
2. Alternative 1: The on-going process of assessing the risk to IT resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk Source
3. Alternative 2: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system Source

Risk Mitigation

1. **Recommended:** Reducing risk by making changes to systems, policies and/or processes Source
2. Alternative 1: Prioritizing, evaluating, and implementing the appropriate risk-reducing

controls/countermeasures recommended from the risk management process Source

3. Alternative 2: Comparable to risk reduction, risk mitigation takes steps to reduce the negative effects of threats and disasters on business continuity (BC). Threats that might put a business at risk include cyberattacks, weather events and other causes of physical or virtual damage Source

Risk Tolerance

1. **Recommended:** The level of risk an organisation is willing to accept, on the basis that risk is inevitable and can never be reduced to zero Source
2. Alternative 1: The organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. Note: Risk tolerance can be influenced by legal or regulatory requirements Source
3. Alternative 2: The level of risk an entity is willing to assume in order to achieve a potential desired result Source

Rogue Device

1. **Recommended:** An unauthorized system on a network that is neither known to nor supported by the official IT team Source
2. Alternative 1: An unauthorized node on a network Source
3. Alternative 2: Rogue devices are just plain malicious in nature. They exist for the sole purpose of doing harm to your network and, in the process, to your reputation and career. They exist to steal information or to disrupt network operations. In rare cases they can even permanently damage systems Source

Role-Based Access Control

1. **Recommended:** A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities Source
2. Alternative 1: Mapped to job function, assumes that a person will take on different roles, overtime, within an organization and different responsibilities in relation to IT systems Source
3. Alternative 2: Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals Source

Root Cause Analysis

1. **Recommended:** Establishing the underlying issue that was the cause of a security incident or system outage Source
2. Alternative 1: A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks Source
3. Alternative 2: Root Cause Analysis is the process of discovering the root causes of problems

in order to identify appropriate solutions. RCA assumes that it is much more effective to systematically prevent and solve underlying issues rather than just treating ad-hoc symptoms and putting out fires Source

Rootkit

1. **Recommended:** A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means Source
2. Alternative 1: A set of covert tools installed by an attacker to compromise the security of a computer system, particularly one with a Unix-style system such as Linux Source
3. Alternative 2: A collection of files that is installed on a host to alter the standard functionality of the host in a malicious and stealthy way Source

Rule-based access control

1. **Recommended:** With the rule-based model, a security professional or system administrator sets access management rules that can allow or deny user access to specific areas, regardless of an employee's other permissions Source
2. Alternative 1: Rule Based Access Control (RBAC) allows system owners to personalize the type of access a user has based on their role within an organisation Source
3. Alternative 2: Rule-based access control is one method of access control that allows certain people to access devices, databases, or other restricted network areas based on preset criteria Source

Runtime application self-protection

1. **Recommended:** A technology that runs on a server and kicks in when an application runs. It's designed to detect attacks on an application in real time. When an application begins to run, RASP can protect it from malicious input or behavior by analyzing both the app's behavior and the context of that behavior Source
2. Alternative 1: A technology capable of inspecting application behavior, as well as the surrounding context. It captures all requests to ensure they are secure and then handles request validation inside the application Source
3. Alternative 2: A security solution designed to provide personalized protection to applications. It takes advantage of insight into an application's internal data and state to enable it to identify threats at runtime that may have otherwise been overlooked by other security solutions Source

Salt

1. **Recommended:** A non-secret value used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker Source
2. Alternative 1: A variable passed into a cryptographic algorithm or Pseudorandom Number Generator to improve randomness/strength Source
3. Alternative 2: A bit string generated during digital signature generation using the RSA

Signature Scheme with Appendix - Probabilistic Signature Scheme (RSASSA-PSS RSA) Source

Sandboxing

1. **Recommended:** A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized Source
2. Alternative 1: Isolating each guest OS from the others and restricting what resources they can access and what privileges they have Source
3. Alternative 2: A system that allows an untrusted application to run in a highly controlled environment where the application's permissions are restricted to an essential set of computer permissions. In particular, an application in a sandbox is usually restricted from accessing the file system or the network. A widely used example of applications running inside a sandbox is a Java applet Source

Scam

1. **Recommended:** A deceptive scheme or trick used to cheat someone out of something, especially money Source
2. Alternative 1: Scam is any use of internet technology to defraud people. Internet scams are carried out by cybercriminals for some type of personal gain, financial or otherwise. Scammers use deceptive methods like phishing emails, fake websites, and malicious software to gain access to their victims' data, files, and personal information Source
3. Alternative 2: Using online services and software with access to the internet to defraud or take advantage of victims. The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money Source

Secure Hash Algorithm

1. **Recommended:** A hash algorithm with the property that it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest Source
2. Alternative 1: The most commonly used family of Hash Functions; unlike Message Digest 5 there are no known vulnerabilities in the more recently devised SHA algorithms Source
3. Alternative 2: A modified version of MD5 and used for hashing data and certificates. A hashing algorithm shortens the input data into a smaller form that cannot be understood by using bitwise operations, modular additions, and compression functions Source

Secure Socket Layer

1. **Recommended:** A security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol Source
2. Alternative 1: A protocol used for protecting private information during transmission via the Internet. Note: SSL works by using the service public key to encrypt a secret key that is

used to encrypt the data that is transferred over the SSL session. Most web browsers support SSL and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https: " instead of "http: ". The default port for SSL Source
3. Alternative 2: Provides privacy and data integrity between two communicating applications. It is designed to encapsulate other protocols, such as HTTP. TLS v1.0 was released in 1999, providing slight modifications to SSL 3.0 Source

Secure Software Development Life Cycle

1. **Recommended:** The result of adding a security focus to the Software Development Life Cycle Source
2. Alternative 1: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation Source
3. Alternative 2: A formal or informal methodology for designing, creating, and maintaining software (including code built into hardware) Source

Security Assertion Markup Language

1. **Recommended:** A framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called assertions, enhancing the interoperability between disparate applications Source
2. Alternative 1: A standard protocol for authenticating user logins against computer systems Source
3. Alternative 2: A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners Source

Security Control

1. **Recommended:** The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature Source
2. Alternative 1: Security controls exist to reduce or mitigate the risk to those assets. They include any type of policy, procedure, technique, method, solution, plan, action, or device designed to help accomplish that goal. Recognizable examples include firewalls, surveillance systems, and antivirus software Source
3. Alternative 2: Measure that is modifying risk (Note: controls include any process, policy, device, practice, or other actions which modify risk.) Source

Security Incident

1. **Recommended:** An occurrence that actually or potentially jeopardizes the confidentiality,

integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies Source

2. Alternative 1: Anomalous or unexpected event, set of events, condition, or situation at any time during the life cycle of a project, product, service, or system Source
3. Alternative 2: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices Source

Security Information and Event Management

1. **Recommended:** Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface Source
2. Alternative 1: A system that collates log and event data that it receives from a wide variety of systems and then reports perceived issues to the security operations team Source
3. Alternative 1: A program that provides centralized logging capabilities for a variety of log types Source

Security Operations Centre

1. **Recommended:** Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents Source
2. Alternative 1: A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization’s security posture on an ongoing basis. The SOC team’s goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes Source
3. Alternative 2: Monitor, prevent, detect, investigate, and respond to cyber threats around the clock. SOC teams are charged with monitoring and protecting the organization’s assets including intellectual property, personnel data, business systems, and brand integrity. The SOC team implements the organization’s overall cybersecurity strategy and acts as the central point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks Source

Security Perimeter

1. **Recommended:** The perimeter is the border between one network and another. Creating a security perimeter, then, can be defined as placing the necessary safeguards at the entrance of a privately owned network to secure it from hackers Source
2. Alternative 1: Refers to natural barriers or built fortifications to either keep intruders out or to keep captives contained within the area the boundary surrounds Source
3. Alternative 2: All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected Source

Security Policy

1. **Recommended:** A high-level policy of an organization that is created to support and enforce portions of the organization’s Information Management Policy by specifying in more detail what information is to be protected from anticipated threats and how that protection is to be attained Source
2. Alternative 1: Statement detailing how the organisation wishes its staff to behave and its systems to operate in order to attain and preserve its desired level of security Source
3. Alternative 2: Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information Source

Security Posture

1. **Recommended:** The security status of an organization’s networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the organization and to react as the situation changes Source
2. Alternative 1: The state of an organisation's systems with regard to security, and the organisation's preparedness for response to a security incident Source
3. Alternative 2: The security status of an enterprise’s networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes Source

Self-Regulatory Body

1. **Recommended:** A self-regulatory organization (SRO) is an entity such as a non-governmental organization, which has the power to create and enforce stand-alone industry and professional regulations and standards on its own Source
2. Alternative 1: A model of regulation in which an organisation conducts an internal regime of assessment to confirm that its operation is aligned with a documented or agreed Standard Source
3. Alternative 2: A non-government organization that has statutory responsibility to regulate its own members through the adoption and enforcement of rules of conduct for fair, ethical, and efficient practices in its industry. FINRA, NYSE, and Nasdaq are examples of SROs for the securities industry Source

Semi-Quantitative Assessment

1. **Recommended:** An evaluation of the organisation's security vulnerability which involves quantifying the level of risk faced by the organisation using data sources that are partially quantitative but partially qualitative. Source
2. Alternative 1: Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts Source

3. Alternative 2: Semi-quantitative risk assessment is one approach to measuring risk. It involves expressing one parameter, such as likelihood, quantitively. The other parameter is assigned a descriptive or numerical ranking Source

Sensitive Information

1. **Recommended:** Data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization Source
2. Alternative 1: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy Source
3. Alternative 2: Information that the organisation wishes to keep confidential from outside parties Source

Server Side Request Forgery

1. **Recommended:** Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location Source
2. Alternative 1: In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or modify a URL which the code running on the server will read or submit data to, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like http enabled databases or perform post requests towards internal services which are not intended to be exposed Source
3. Alternative 2: Server-side request forgery (SSRF) is the only type of vulnerability that has its own category in the OWASP Top 10 2021 list. Several major cybersecurity breaches in recent years, including Capital One and MS Exchange attacks, involved the use of SSRF as one of the break-in techniques. SSRF vulnerabilities let an attacker send crafted requests from the back-end server of a vulnerable application. Criminals usually use SSRF attacks to target internal systems that are behind firewalls and are not accessible from the external network. An attacker may also leverage SSRF to access services available through the loopback interface (127.0.0.1) of the exploited server Source

Server Side Template Injection

1. **Recommended:** Server-side template injection is a vulnerability where the attacker injects malicious input into a template to execute commands on the server-side. This vulnerability occurs when invalid user input is embedded into the template engine which can generally lead to remote code execution (RCE) Source
2. Alternative 1: Server-side template injection occurs when user-controlled input is embedded into a server-side template, allowing users to inject template directives. This allows an attacker to inject malicious template directives and possibly execute arbitrary

code on the affected server Source
3. Alternative 2: A server-side template injection occurs when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side Source

Service Level Agreement

1. **Recommended:** Represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities, details on the type of service, expected performance level (e.g., reliability, acceptable quality, and response times), and requirements for reporting, resolution, and termination Source
2. Alternative 1: Defines the specific responsibilities of the service provider and sets the customer expectations Source
3. Alternative 2: A service contract between an FCKMS service provider and an FCKMS service-using organization that defines the level of service to be provided, such as the time to recover from an operational failure or a system compromise Source

Short Message Service

1. **Recommended:** A mobile phone network facility that allows users to send and receive alphanumeric text messages of up to 160 characters on their cell phone or other handheld device Source
2. Alternative: A basic text messaging system used by mobile telephones. SMS is a common mechanism used to alert IT and cyber security staff to potential issues that have been detected by a system Source

Smishing

1. **Recommended:** Smishing is a form of phishing that uses mobile phones as the attack platform. The criminal executes the attack with an intent to gather personal information, including social insurance and/or credit card numbers. Smishing is implemented through text messages or SMS, giving the attack the name “SMiShing” Source
2. Alternative 1: Similar to Phishing but using SMS text messages instead of email Source
3. Alternative 2: Smishing is a form of phishing in which an attacker uses a compelling text message to trick targeted recipients into clicking a link and sending the attacker private information or downloading malicious programs to a smartphon Source

Sniffer

1. **Recommended:** A network sniffer tool can decode traffic and analyze either the metadata or entire contents. A network sniffer app works by intercepting the packets of data being sent across a network, analyzing the metadata or raw contents, and presenting it in a readable form Source
2. Alternative 1: A piece of software for Network Sniffing Source
3. Alternative 2: Software that monitors network traffic on wired or wireless networks and captures packets Source

Social Engineering

1. **Recommended:** The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust Source
2. Alternative 1: Tricking people into giving up sensitive information by pretending to be someone authoritative - the company's Service Desk, the CEO of the company, and so on Source
3. Alternative 2: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks Source

Software composition Analysis

1. **Recommended:** The act of putting a monitor on a network and capturing/examining the traffic as it flies past. Source

2. Alternative 1: This analysis is performed to evaluate security, license compliance, and code quality Source
3. Alternative 2: Best bet for finding vulnerabilities in open source packages and learning how to fix them, empowering you to secure your code and the health of your applications. Use this guide for best practices when using SCA tools Source
4. Alternative 3: Software Composition Analysis (SCA) is the process of automating the visibility into open source software (OSS) use for the purpose of risk management, security and license compliance. With the rise of open source (OS) use in software across all industries, the need to track components increases exponentially to protect companies from issues and open source vulnerabilities. Because the majority of software creation includes OS, manual tracking is difficult, requiring the need to use automation to scan source code, binaries and dependencies Source

Spam

1. **Recommended:** The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages Source
2. Alternative 1: Unsolicited bulk messages, generally sent by email. Spam is a popular way to target people because although only a fraction of the messages penetrate the organisation's defense, the sheer quantity of messages makes this fraction numerically significant Source
3. Alternative 2: Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages Source

Split Brain

1. **Recommended:** Split-brain is essentially what happens when two or more resources are supposed to be synchronized but somehow loses referential integrity, operate independently, and begin storing and processing information without synchronizing content Source

2. Alternative 1: In a resilient implementation where primary and secondary systems enter a state where the secondary mistakenly acts as if it were the primary, causing network disruption due to traffic routing inconsistently and switching between the two devices Source
3. Alternative 2: In high availability clustering, split-brain is a problem scenario that can occur when one of the nodes fails. Within a CyberArk implementation with disaster recovery enabled, a split-brain condition might arise if high availability is not configured as per the recommendations Source

Split Tunnelling

1. **Recommended:** When a computer is connected to two networks at once, for example, to the Internet and also via a VPN to a company network. This has a security risk as there is the potential for illicit traffic ingress from the Internet to use the computer as a route to the company network Source
2. Alternative 2: A method that routes organization-specific traffic through the SSL VPN tunnel, but routes other traffic through the remote user's default gateway Source
3. Alternative 1: The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices, and simultaneously, access uncontrolled networks Source

Spoofing

1. **Recommended:** Faking the source address of a communication in order to masquerade as a different individual or system Source
2. Alternative 1: Faking the sending address of a transmission to gain illegal entry into a secure system Source
3. Alternative 2: The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing Source

Spyware

1. **Recommended:** Software that is secretly or surreptitiously installed into a system to gather information on individuals or organizations without their knowledge; a type of malicious code Source
2. Alternative 1: Although it sounds like a James Bond gadget, it’s actually a type of malware that infects your PC or mobile device and gathers information about you, including the sites you visit, the things you download, your usernames and passwords, payment information, and the emails you send and receive Source
3. Alternative 2: A program embedded within an application that collects information and periodically communicates back to its home site, unbeknownst to the user Source

SQL injection

1. **Recommended:** SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior Source
2. Alternative 1: A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands Source
3. Alternative 2: Attacks that look for web sites that pass insufficiently-processed user input to database back-ends Source

Static application security testing

1. **Recommended:** Static Application Security Testing (SAST) or static code analysis detects application vulnerabilities by scanning the source code, byte code, or binaries of an application. By analyzing code patterns, control flows and data flows within an app, SAST can identify a range of vulnerabilities without running the application Source
2. Alternative 1: Known as white-box testing, meaning it tests the internal structures or workings of an application, as opposed to its functionality Source
3. Alternative 2: SAST takes place very early in the software development life cycle (SDLC) as it does not require a working application and can take place without code being executed. It helps developers identify vulnerabilities in the initial stages of development and quickly resolve issues without breaking builds or passing on vulnerabilities to the final release of the application Source

Static Key

1. **Recommended:** A key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a cryptographic key-establishment scheme. Contrast with an Ephemeral key Source
2. Alternative 1: A Key that changes infrequently, if at all Source
3. Alternative 2: A cryptographic key is called static if it is intended for use for a relatively long period of time and is typically intended for use in many instances of a cryptographic key establishment scheme. Contrast with an ephemeral key Source

Steganography

1. **Recommended:** Embedding data within other data to conceal it Source
2. Alternative 1: The science of communicating in such a way that hides the communication - for instance by concealing sensitive data within an innocuous-looking document such as a photograph Source
3. Alternative 1: The art, science, and practice of communicating in a way that hides the existence of the communication Source

Supervisory Control and Data Acquisition

1. **Recommended:** Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to: i)Control industrial processes locally or at remote locations; ii) Monitor, gather, and process real-time data; iii) Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software; iv) Record events into a log file Source
2. Alternative 1: A controller module for a piece of equipment that would not usually be connected to the network (a generator, for instance or some other piece of plant machinery) so it can be monitored and/or controlled from a PC. SCADA interfaces have a reputation for having a disproportionate level of security vulnerabilities. Commonly used synonymously with Industrial Control Systems Source
3. Alternative 2: A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated Source

System Administrator

1. **Recommended:** A person who manages a computer system, including its operating system and applications. Responsibilities are similar to that of a network administrator Source
2. Alternative 1: Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures Source

Tabletop Exercise

1. **Recommended:** A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario Source
2. Alternative 1: The act of testing one's [Incident Response Plan] by going through a

simulated Incident rather than by actually taking any real systems out of action Source

3. Alternative 2: Definition: A tabletop exercise is an. activity in which key personnel assigned emergency management roles and responsibilities are gathered to discuss, in a non-threatening environment, various simulated emergency situations Source

Threat Analysis

1. **Recommended:** Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat Source
2. Alternative 1: A detailed, rigorous analysis of the threats faced by an organisation Source
3. Alternative 2: Threat analysis is a cybersecurity strategy that aims to assess an organization's security protocols, processes and procedures to identify threats, vulnerabilities, and even gather knowledge of a potential attack before they happen Source

Threat

1. **Recommended:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service Source
2. Alternative 1: Potential cause of an unwanted incident, which may result in harm to a system or organization Source
3. Alternative 2: An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss. Note: The specific causes of asset loss, and for which the consequences of asset loss are assessed, can arise from a variety of conditions and events related to adversity, typically referred to as disruptions, hazards, or threats. Regardless of the specific term used, the basis of asset loss constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions Source

Time Bomb

1. **Recommended:** Resident computer program that triggers an unauthorized act at a predefined time Source
2. Alternative 1: Rather like a Logic Bomb - a piece of nefarious software that lies dormant until the date and time at which it has been programmed to become active Source
3. Alternative 2: Time Bomb is a Logic Bomb, the execution of which is triggered on a specific day or time, such as Valentine's Day or 1st April Source

Transport Layer Security

1. **Recommended:** An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by RFC 5246. TLS is similar to the older SSL protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, specifies how TLS is to be used in government applications Source

2. Alternative 1: Provides privacy and data integrity between two communicating applications. It is designed to encapsulate other protocols, such as HTTP. TLS v1.0 was released in 1999, providing slight modifications to SSL 3.0 Source
3. Alternative 2: Provides privacy and reliability between two communicating applications. It is designed to encapsulate other protocols, such as HTTP. SSL v3.0 was released in 1996. It has been succeeded Source

Trap Door

1. **Recommended:** In the context of an encryption algorithm, an algorithm that is very simply and quick to execute in one direction, and intractably hard and slow to execute in the other direction Source
2. Alternative 1: A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data. See Backdoor Source
3. Alternative 2: In cryptography, one-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information Source

Triple DES

1. **Recommended:** A development of the Data Encryption Standard which is considerably more secure Source
2. Alternative 1: An approved cryptographic algorithm as required by FIPS PUB 140-2. TDEA specifies both the DEA cryptographic engine employed by TDEA and the TDEA algorithm itself Source
3. Alternative 2: DES is a symmetric-key algorithm based on a Feistel network. As a symmetric key cipher, it uses the same key for both the encryption and decryption processes. The Feistel network makes both of these processes almost exactly the same, which results in an algorithm that is more efficient to implement Source

Trojan Horse

1. **Recommended:** A malicious program hidden inside an ostensibly innocuous one Source
2. Alternative 1: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program Source
3. Alternative 2: A useful or seemingly useful program that contains hidden code of a malicious nature that executes when the program is invoked Source

Trusted Certificate

1. **Recommended:** A digital certificate that is trusted by the machine that is using it for identification; certificates are deemed “trusted” when they have been issued by a reputable issuing organisation Source
2. Alternative: A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start

certification paths. Also known as a “trust anchor” Source

Tunneling

1. **Recommended:** Tunneling, also known as “port forwarding,” is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network Source
2. Alternative 1: Sending data using one protocol through a connection established using another. Virtual Private Networks are a good example of tunnels Source
3. Alternative 2: Technology enabling one network to send its data via another network’s connections. Tunneling works by encapsulating a network protocol within packets carried by the second network Source

Two Factor Authentication

1. **Recommended:** Two-factor authentication (2FA) is a specific type of multi-factor authentication (MFA) that strengthens access security by requiring two methods (also referred to as authentication factors) to verify your identity. These factors can include something you know — like a username and password — plus something you have — like a smartphone app — to approve authentication requests Source
2. Alternative 1: A mechanism for improving security by making users identify themselves by two means rather than one (the latter generally being a password) - typically using a one-time code generated by an electronic token or smartphone program or by entering a code that is sent by the target system to the user's phone by SMS Source
3. Alternative 2: Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric) Source

Unauthorized access

1. **Recommended:** A person gains logical or physical access without permission to a network, system, application, data, or other resource Source
2. Alternative 1: Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access, it is considered unauthorized access Source
3. Alternative 2: Any access that violates the stated security policy Source

Virtual Machine

1. **Recommended:** A software-based computer that runs on another computer Source
2. Alternative 1: A simulated environment created by virtualization Source
3. Alternative 2: A virtual data processing system that appears to be at the disposal of a particular user but whose functions are accomplished by sharing the resources of a real

data processing system Source

Virtual Private Network

1. **Recommended:** A point-to-point connection between two computers or networks which uses a potentially insecure network (usually the Internet) to transport data securely by using strong Authentication and Encryption Algorithms. Source
2. Alternative 1: Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line Source
3. Alternative 2: A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network Source

Virus

1. **Recommended:** A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active Source
2. Alternative 1: A common alternative term for Malware Source
3. Alternative 2: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See malicious code Source

Vishing

1. **Recommended:** Voice phishing, or vishing, is the use of telephony to conduct phishing attacks. Landline telephone services have traditionally been trustworthy; terminated in physical locations known to the telephone company, and associated with a bill-payer Source
2. Alternative: Vishing uses verbal scams to trick people into doing things they believe are in their best interests. Vishing often picks up where phishing leaves off Source

VLAN Hopping

1. **Recommended:** VLAN hopping is a computer security exploit, a method of attacking networked resources on a virtual LAN. The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible Source
2. Alternative 1: This type of exploit allows an attacker to bypass any layer 2 restrictions built to divide hosts. With proper switch port configuration, an attacker would have to go through a router and any other layer 3 devices to access their target. However, many networks either have poor VLAN implementation or have misconfigurations which will allow for attackers to perform said exploit. In this article, I will go through the two primary

methods of VLAN hopping, known as 'switched spoofing', and 'double tagging'. I will then discuss mitigation techniques Source

3. Alternative 2: VLAN hopping is a type of network attack which allows frames from one VLAN to pass into another VLAN. This enables adversaries to send traffic to a VLAN, which their host should not be able to reach. Two main methods of VLAN hopping attacks are Switch spoofing and Double tagging Source

Vulnerability

1. **Recommended:** An aspect of a computer system or network that is susceptible to intrusion due to a flaw in design or programming Source
2. Alternative 1: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source Source
3. Alternative 2: A security exposure in an operating system or other system software or application software component. A variety of organizations maintain publicly accessible databases of vulnerabilities based on the version numbers of software. Each vulnerability can potentially compromise the system or network if exploited Source

Warm Site

1. **Recommended:** A premises that is not a fully live backup to one's primary site, but which is equipped such that it can be brought into operation within a reasonable time following an incident (such as a fire or a flood) that has rendered all or part of the primary site inoperative Source
2. Alternative 1: An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption Source
3. Alternative 2: A warm site is a type of facility an organization uses to recover its technology infrastructure when its primary data center goes down. A warm site features an equipped data center but no customer data. Source

Web Application Firewall

1. **Recommended:** A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors Source
2. Alternative 1: A system that examines inbound connections to an internet-connected system (generally a web server) with the intention of blocking illicit requests (particularly, but not limited to Distributed Denial of Service attacks) so that such attacks do not reach the target system Source
3. Alternative 2: A web application firewall (WAF) protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie

poisoning, among others. Attacks to apps are the leading cause of breaches—they are the gateway to your valuable data. With the right WAF in place, you can block the array of attacks that aim to exfiltrate that data by compromising your systems Source

Web Filtering Software

1. **Recommended:** Web filtering software monitors and manages the locations where users are browsing on the Internet, enabling an organization to either allow or block web traffic in order to protect against potential threats and enforce corporate policy Source
2. Alternative 1: Software that is put at the edge of your network to prevent users from accessing material on the Internet that is classed as threatening or otherwise unwanted Source
3. Alternative 2: A Web filter, which is commonly referred to as "content control software", is a piece of software designed to restrict what websites a user can visit on his or her computer. These filters can work using either a whitelist or a blacklist: Source

White Box Testing

1. **Recommended:** A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing Source
2. Alternative 1: A security test in which the testing team are given detailed information regarding the design and implementation of the system. See also **Black Box Testing** Source
3. Alternative 2: Also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing) Source

Whitelist

1. **Recommended:** Synonymous with [Allow List], the term "Whitelist" is widely falling into disuse following the growth of the Black Lives Matter movement Source
2. Alternative 1: A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline Source
3. Alternative 2: An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments Source

Wi-Fi Protected Access

1. **Recommended:** More commonly known by the abbreviation WPA, a mechanism for [Wireless Local Area Network] access which is (particularly in the case of WPA2) considerably more secure than it predecessor [Wired Equivalent Privacy]. WPA2 is not yet known to have been successfully cracked Source
2. Alternative 1: Wi-Fi Protected Access (WPA) is a security standard for computing devices equipped with wireless internet connections. WPA was developed by the Wi-Fi Alliance to

provide more sophisticated data encryption and better user authentication than Wired Equivalent Privacy (WEP), the original Wi-Fi security standard Source

3. Alternative 2: Short for Wi-Fi Protected Access 2, WPA2 is the security method added to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks Source

Wired Equivalent Privacy

1. **Recommended:** A wireless encryption standard that, although the name may suggests otherwise, is very insecure. WEP was an early wireless encryption standard that is no longer considered usable Source
2. Alternative 1: Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. That standard is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN Source
3. Alternative 2: Wired Equivalent Privacy (also known as the WEP) is a security algorithm introduced to provide data confidentiality for wireless networks. Wired Equivalent Privacy was brought as part of the 802.11 standard. One of the most characteristic features of Wired Equivalent Privacy is its key of 10 or 26 hexadecimal digits, in other words, 40 or 104 bits Source

Wireless Application Protocol

1. **Recommended:** An early form of mobile phone based data access, introduced in 1999 but obsolete today Source
2. Alternative 1: Wireless Application Protocol or WAP is a programming model or an application environment and set of communication protocols based on the concept of the World Wide Web (WWW), and its hierarchical design is very much similar to TCP/IP protocol stack design. See the most prominent features of Wireless Application Protocol or WAP in Mobile Computing: Source
3. Alternative 2: WAP stands for Wireless Application Protocol. It is a protocol designed for micro-browsers and it enables the access of internet in the mobile devices. It uses the mark-up language WML (Wireless Markup Language and not HTML), WML is defined as XML 1.0 application. It enables creating web applications for mobile devices. In 1998, WAP Forum was founded by Ericson, Motorola, Nokia and Unwired Planet whose aim was to standardize the various wireless technologies via protocols Source

Wireless Local Area Network

1. **Recommended:** A LAN that uses radio transmission in place of copper or fibre cables. Wireless LANs provide versatility and are simpler and less expensive to set up than cabled networks, but are slower and more susceptible to security attacks, particularly Eavesdropping Attacks Source
2. Alternative 1: A wireless local-area network (WLAN) is a group of colocated computers or other devices that form a network based on radio transmissions rather than wired

connections. A Wi-Fi network is a type of WLAN; anyone connected to Wi-Fi while reading this webpage is using a WLAN Source

3. Alternative 2: A wireless local area network (WLAN) is a wireless distribution method for two or more devices. WLANs use high-frequency radio waves and often include an access point to the Internet. A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection Source

Worm

1. **Recommended:** A self-replicating program that propagates itself through a network onto other computer systems without requiring a host program or any user intervention to replicate Source
2. Alternative 1: A Malware computer program that spreads to other machines by replicating itself and sending copies of itself using vulnerabilities in those other machines. The most famous worm was created in 1988 by Robert Tappan Morris Source
3. Alternative 2: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively Source

Zero Day Attack

1. **Recommended:** An attack on a computer system which exploits a vulnerability of which the software or anti-malware vendor is not aware Source
2. Alternative 1: An attack that exploits a previously unknown hardware, firmware, or software vulnerability Source
3. Alternative 2: A zero-day attack is the use of a zero-day exploit to cause damage to or steal data from a system affected by a vulnerability Source

Zero-Day

1. **Recommended:** A zero-day vulnerability is a software vulnerability discovered by attackers before the vendor has become aware of it. Because the vendors are unaware, no patch exists for zero-day vulnerabilities, making attacks likely to succeed Source
2. Alternative 1: A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for detection … at first Source
3. Alternative 2: Zero-day“ is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems. The term “zero-day” refers to the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it. A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it Source

Zeroisation

1. **Recommended:** A method of erasing electronically stored data, cryptographic keys, and

credentials service providers (CSPs) by altering or deleting the contents of the data storage to prevent recovery of the data Source

2. Alternative 1: Overwriting data on disk or tape multiple times in order to render it unreadable, on the premise that deleting a file in most operating systems usually just removes the directly entry but leaves the file content on the disk. On magnetic disks the accuracy tolerance of the read/write head on the disk is such that an attempt to overwrite an item once may be slightly askew of the precise point at which the data is located, and so Zeroisation of magnetic disks involves writing each element several times to achieve a high probability of overwiting the exact location Source
3. Alternative 2: A method of sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data Source

Zombie

1. **Recommended:** Computer or personal computer (PC) connected to the Internet and taken over by a computer worm, virus, or other “malware.” Groups of such machines, called botnets (from a combination of robot and network), often carry out criminal actions without their owners’ detecting any unusual activity Source
2. Alternative 1: In computing, a zombie is a computer connected to a network that has been compromised by a hacker, a virus or a Trojan. It can be used remotely for malicious tasks Source
3. Alternative 2: A zombie computer is a compromised machine that hackers can control remotely and instruct it to perform various malicious tasks. The majority of zombie computers are actually home-based machines owned and used by the average Joe and Jane. The worst part is that users rarely suspect hackers have taken over their computers and turned them into zombies Source