Alphabetical Index

A B C D E F G H I L M N O P Q R
S T U V W X

A

Back to top

Acceptable Use Policy

A set of guidelines outlining the dos and don'ts of using an company's computer systems. It highlights parts of the full security policy and details the consequences of not following the rules.

Access

The process of interacting with data within a computer system, whether it's obtaining, changing, copying, or sharing it across various mediums such as paper, digital files, or screens.

Accountability

The duty of a person or an company to explain their actions, accept the outcomes, and share the data openly and in a timely manner.

Acknowledgement of Acceptable Use

A written attestation from a user of an computer system indicating the user's acceptance and willingness to comply with the relevant computer systems control policies.

ACL (Access Control List)

A list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

Source: Wikipedia

Anti-Tailgating / Anti-Piggybacking Mechanism

Two sets of doors whereby access to the second is not granted until the individual has passed through (and closed) the first, often referred to as a "man trap." A controlled turnstile is also considered an anti-tailgating/ piggybacking mechanism.

API

Application program interface (API) is a set of routines, protocols, and tools for building software applications. An API specifies how software components should interact and APIs are used when programming graphical user interface (GUI) components.

Source: Webopedia

Applicable Privacy Law

Relevant laws, enactments, regulations, binding industry codes, regulatory permits and licenses that are in effect and address the protection, handling and privacy of scoped privacy data, selected as being in scope for the assessment.

Application Inventory System

An asset-based approach that includes an itemized list of applications or application components, such that software versions, security testing results and additional attributes can be individually identified against such assets.

Application Segmentation

In response to the advent of borderless applications, application segmentation has evolved and should be applied consistently on the application no matter where it goes, which borders it crosses, or which siloes are carrying its traffic. In enterprises where segmentation is oriented around applications instead of infrastructure, the security benefit is immediately apparent. If a hacker manages to compromise a user, then the hacker’s access is contained and limited to only the applications that the compromised user is allowed to access. They cannot move laterally or hop from application to application, browsing through the IT infrastructure until they find the most sensitive or valuable applications and data. The data breach is, by default, contained and cannot spread.

Source: http://www.cloudstrategymag.com/articles/85958-application-segmentation

Asset

In computer security, a major application, general-support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems.

Source: NIST: CNSSI-4009

Asset Classification

The category or type assigned to an asset, which is derived from the asset classification policy. Asset classifications frequently vary from company to company.

Asset Control Tag

A unique identification number assigned to all inventoried assets.

Asset Management Program

A program for managing an company's assets which includes formalized governance, policies, and procedures.

Asset Tracking

Asset tracking refers to the method of tracking physical assets, either by scanning barcode labels attached to the assets or by using tags using GPS or RFID which broadcast their location.

Source: Wikipedia

Attack Vector

Path or means by which an attacker can gain access to a system or network in order to deliver a payload or malicious outcome.

Attribute

A property or field of a particular object.

Authentication

The process of verifying the identity of a person user, machine, software component, or any other entity

Source: FFIEC Information Security Booklet

B

Back to top

Baseline

A benchmark by which subsequent items are measured.

Battery

An electrochemical cell (or enclosed and protected material) that can be charged electrically to provide a static potential for power or released electrical charge when needed.

Biometric Reader

A device that uses measurable biological characteristics such as fingerprints or iris patterns to assist in authenticating a person to an electronic system.

Business Associate

A business associate is a person or company, other than an employee of a covered entity, that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI. A business associate can also be a subcontractor responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate. Business associates provide services to covered entities that include: Accreditation Billing Claims processing Consulting Data analysis Financial services Legal services Management administration Utilization review NOTE: A covered entity can be a business associate of another covered entity.

Source: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf

Business Continuity

A set of planning, preparatory and related activities which are intended to ensure an company's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period.

Business Continuity Plan

A process that defines exactly how, for which applications and for how long, a business plans to continue functioning after a disruptive event. The business continuity plan is usually an overarching plan that includes both operational and technology-related tasks.

Business Impact Analysis (BIA)

This term is applicable across Technology Risk Management, in both data security and business continuity planning domains. An impact analysis results in the differentiation between critical and non-critical business functions. A function may be considered critical if there is an unacceptable impact to stakeholders from damage to the function. The perception of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law.

Business Process

An end-to-end service made available to internal or external parties that usually corresponds to standard service products that the Service Provider offers to clients.

Business Resiliency

The ability an company has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity. Business resilience is more than disaster recovery, it includes post-disaster strategies to avoid costly downtime, the identification and resolution of vulnerabilities and the ability to maintain business operations in the face of additional, unexpected breaches.

Business Resiliency Procedure

A process that defines exactly how, for which applications, and for how long a business plans to continue functioning after a disruptive event. The business resiliency procedure is usually an overarching procedure that includes both operational and technology-related tasks.

C

Back to top

Change Control

Also known as Change Management - The broad processes for managing companyal change. Change management encompasses planning, oversight or governance, project management, testing, and implementation. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted and that resources are used efficiently.

Source: FFIEC Operations Booklet and WhatIS.com

Change Initiation Request (CIR)

A document (physical or electronic) used to track change requests, including new features, enhancement requests, defects, and changed requirements. The change initiation request document must contain: - The name of the person initiating the change - The system affected by the change - A description of the change, including the file name(s) and file location(s) - The date the change will occur - An approval signature by someone other than the person initiating the change - An approval date

Cipher Lock

A cipher lock is opened with a programmable keypad. The purpose of cipher locks is to control access, limiting either unannounced intrusions or unescorted entry to particular areas of a facility that are sensitive. A cipher lock may have four or five pushbuttons, depending on the manufacturer. Even with five pushbuttons, the code may be one to five digits. When the cipher lock unit is set up the code is programmed and shared with authorized personnel.

Source: http://www.wisegeek.com/what-is-a-cipher-lock.htm

Clean Room

A network segment or subnet where data is sanitized for mobile devices access only.

Client

A client is the individual and/or entity for whom services are being provided by the company.

Client Scoped Privacy Data

Data received from the company’s client that includes EU “sensitive personal data” (health, religion, criminal records, trade union membership, sexual orientation and race) and in the US, protected scoped privacy data includes name, address or telephone number in conjunction with Social Security number, driver’s license number, account number, credit or debit card number, personal identification number or user ID or password.

Climate Control System

A combination of sensors and equipment that monitors the temperature and humidity in a sensitive environment (such as a data center) and that automatically heats/cools/dehumidifies as needed to keep the atmosphere within acceptable tolerances.

Closed Circuit TV (CCTV)

CCTV is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. CCTV relies on strategic placement of cameras and private observation of the camera's input on monitors.

Source: WhatIs.com

Cloud Computing - NIST Definition

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud Computing - NIST Definition of Deployment Models - Community Cloud

The Cloud infrastructure is shared by several respondents and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the respondent or subcontractor and may exist on premise or off premise.

Cloud Computing - NIST Definition of Deployment Models - Hybrid Cloud

The Cloud infrastructure is a composition of two or more Clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load balancing between Clouds).

Cloud Computing - NIST Definition of Deployment Models - Private Cloud

The Cloud infrastructure is operated solely for the respondent. It may be managed by the company or a third party and may exist on premise or off premise.

Cloud Computing - NIST Definition of Deployment Models - Public Cloud

The Cloud infrastructure is made available to the general public or a large industry group and is owned by the Respondent selling Cloud services.

Cloud Computing - NIST Definition of Essential Characteristics - Broad Access Network

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Cloud Computing - NIST Definition of Essential Characteristics - Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud Computing - NIST Definition of Essential Characteristics - On-Demand Self-Service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

Cloud Computing - NIST Definition of Essential Characteristics - Rapid Elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Cloud Computing - NIST Definition of Essential Characteristics - Resource Pooling

The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Cloud Computing - NIST Definition of Service Models - Cloud Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud Computing - NIST Definition of Service Models - Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Computing - NIST Definition of Service Models - Cloud Software as a Service (SaaS)

The capability provided to the consumer is to use the provider’s applications running on a Cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application.

Cloud Service Provider (CSP)

The business or entity providing Cloud services.

Co-Location

A colocation (colo) is a data center facility in which a business can rent space for servers and other computing hardware. Typically, a colo provides the building, cooling, power, bandwidth and physical security while the customer provides servers and storage.

Source: WhatIs.com

Cold Site

A remote facility that provides the equipment necessary for data and process restoration.

Communications Plan

A tool for communicating data on the considerations and implications of respondent business continuity to improve decision making.

Complex Password

A password that combines alphabetic and non-alphabetic characters, such as special or numeric characters.

Confidential Information

Confidential data means any data and/or documents of the client or its affiliates to which the company has had access, whether in oral, written, graphic or machine-readable form, and includes, but is not limited to: (i) trade secrets and work product; (ii) data relating to business plans or practices, sales, pricing, financial data or marketing plans or methods; (iii) software, applications, systems and networks, including source code, object code and documentation and commentary related thereto; (iv) data relating to one or more customers of the subscriber or its affiliates, including, but not limited to, the following (collectively, “client data”): (1) personal data such as a customer’s name, address, telephone number, account relationships, account numbers, account balances and account histories, (2) data concerning such customers that would be considered “nonpublic personal data” within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 113 Stat. 1338) and its implementing regulations, as the same may be amended from time to time and (3) data concerning such customers that is protected from disclosure by other applicable federal or state laws and regulations regarding privacy; (v) confidential data of third parties in the subscriber's or its affiliates' possession; (vi) security procedures and measures; and (vii) all other data related to the subscriber's and/or its affiliates' business(es). Except with respect to customer data, "client confidential data" does not include data that (i) is at the time of its disclosure publicly known; (ii) was rightfully known by licensor at the time of disclosure; or (iii) is lawfully received by licensor from a third party not bound by confidentiality obligations to the owner of such client confidential data.

Confidentiality

The protection of sensitive data from unauthorized disclosure and sensitive facilities due to physical, technical, or electronic penetration or exploitation.

Configuration Management

Is the practice of handling changes systematically so that a system maintains its integrity over time. The Information Technology Infrastructure Library (ITIL) specifies the use of a Configuration management system (CMS) or Configuration management database (CMDB) as a means of achieving industry best practices for Configuration Management. CMDBs are used to track Configuration Items (CIs) and the dependencies between them, where CIs represent the things in an enterprise that are worth tracking and managing, such as but not limited to computers, software, software licenses, racks, network devices, storage, and even the components within such items. The benefits of a CMS/CMDB includes being able to perform functions like root cause analysis, impact analysis, change management, and current state assessment for future state strategy development.

Source: Wikipedia

Constituent

An active employee or contractor.

Contractor

A contracted professional with expertise in a particular domain or area.

Covered Account

A covered account is (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft. Each financial institution and creditor must periodically determine whether it offers or maintains a ‘‘covered account.’’

Source: Section 114 of the FACT Act A. Red Flag Regulations and Guidelines

Covered Entity

(As defined by the HIPAA Rules requirement) A covered entity can be an Individual, a business and/or an agency who must comply with HIPAA rules to protect the privacy and security of health data and must provide individuals with certain rights related to their health data (i.e. Doctors, Health Insurance Companies, healthcare clearing house).

Critical third party service provider

A service provider that is so vital that the incapacity or unavailability of such may have a debilitating impact on the business utilizing the service provider. Provides a product or performs a service for which there is no backup or alternate provider.

Cross Site Request Forgery (CSRF)

An attack which can occur when a malicious website, email, blog, instant message (IM) or program causes a user’s web browser to perform unwanted action on a trusted website. CSRF allows an attacker to access functionality in a target web application via the victim’s already authenticated browser.

Cross Site Scripting (XSS)

A computer-related security vulnerability typically found in website applications. This hacking technique can enable attackers to inject client-side script into web pages viewed by other users.

D

Back to top

Data Controller

Any person (including a public authority, agency or any other body) which alone or jointly with others determines the purposes and means of processing scoped privacy data (EU Directive).

Data Flow

A flow describing and/or depicting the scoped privacy data for a given data subject for a given country or jurisdiction. The data flow defines the scoped privacy data and the protected scoped privacy data collected, stored, used, accessed, shared and transferred across borders of the country or jurisdiction that are secured, retained and retired.

Data segmentation and separation

(see also Network Segmentation) Better security can be achieved by not mixing trusted and untrusted applications, data, and networks. Segmentation on a cloud-computing infrastructure must provide an equivalent level of isolation as that achievable through physical network separation. Mechanisms to ensure appropriate isolation may be required at the network, operating system, and application layers; and most importantly, there should be guaranteed isolation of data that is stored.

Source: PCI_DSS_v2_Cloud_Guidelines

Data Subject

Any person who can be identified, directly or indirectly, by data that identifies one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. In certain countries (such as Austria, Luxembourg and Italy), this also includes data concerning legal entities/corporations.

Data Subject Category

Includes, for example, employees, clients, business partners, customers or users.

Demilitarized Zone (DMZ)

A controlled network space, delimited by firewalls or other policy-enforcing devices, which is neither inside an company's network nor directly part of the Internet. A DMZ is typically used to isolate the respondent's most highly secured data assets while allowing predefined access to those assets that must provide or receive data outside of the respondent. The access and services provided should be restricted to the absolute minimum required.

Disaster Recovery

The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to the respondent after a natural or human-induced disaster. Disaster recovery is a subset of business continuity

E

Back to top

Electronic Health Records

An Electronic Health Record (EHR) is an electronic version of a patients medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that persons care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports The EHR automates access to data and has the potential to streamline the clinician's workflow. The EHR also has the ability to support other care-related activities directly or indirectly through various interfaces, including evidence-based decision support, quality management, and outcomes reporting.

Source: https://www.cms.gov/Medicare/E-health/EHealthRecords/index.html

Electronic System

The combination of hardware and software used to manage electronic data. A system which stores data from internal and external sources to facilitate better decision making.

Source: http://thelawdictionary.org/electronic-information-system/

Emergency Periods

Duration of time when a client’s service provider is experiencing an emergency event that has an impact on the client.

Enclosed

Closed in, surrounded, or included within.

Encryption

The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext). Use of encryption protects data between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure

Source: ISACA CSX Fundamentals and pci_dss_glossary_v1-1

Enterprise Risk Governance Program

A program implemented, reviewed and maintained by an company’s Executive Board (if applicable) and Senior Management to govern the relevant factors of risks to the company. This risk factors can include but are not limited to the following: Strategic Risks Financial Risks Operational Risks IT and Infrastructure Risks

Event

Any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT service and evaluation of the impact a deviation might cause to the services. Events are typically notifications created by an IT service, Configuration Item (CI) or monitoring tool.

Source: Wikipedia

Exception

A result that deviates from the norm or expectation.

Exclusion

An item not fully covered by the question.

External Parties

Any entity other than the company providing responses to the SIG. Examples include (but are not limited to) service providers, contractors/consultants, vendors, etc.

External Vulnerability Scan

A systematic review process executed from a network address outside of the Scoped Systems and Data network that uses software tools designed to search for and map systems for weaknesses in an application, computer or network. The intent is to determine if there are points of weakness in the security control system that can be exploited from outside the network.

Externally Facing

The network entry point that receives inbound traffic.

Extranet

An intranet that is partially accessible to authorized outsiders.

F

Back to top

Facility

A structure or building, or multiple structures or buildings, in which operations are conducted for the services provided. These operations include handling, processing and storage of data, data or systems, as well as personnel that support the operations.

Fire Suppression System

A combination of sensors and equipment designed to detect the presence of heat/smoke/fire and actuate a fire retardant or fire extinguishing system.

Firewall

A set of related programs, located at a network gateway server, that protects the resources of private networks from other networks. Firewalls may be application/proxy, packet-filtering, or stateful-based. Examples of firewalls are Cisco PIX, Check Point Firewall, Juniper NetScreen and Cyberguard. (Though they contain some firewall functionality, routers are not included in this definition.)

Firewall Rule

Information added to the firewall configuration to define the respondent's security policy through conditional statements that tell the firewall how to react in a particular situation.

Fluid Sensor

A mechanical device that is sensitive to the presence of water or moisture that transmits a signal to a measuring or control instrument.

G

Back to top

Gateway

A node on a network that facilitates the communication of data between two or more nodes.

General Perimeter

An area with fully enclosed walls that extend from floor to ceiling (beyond raised floors and ceilings) surrounding the secure perimeter. This may be the same floor as the secure perimeter, if shared by other tenants in the facility, or the facility itself.

Generator

A device that converts mechanical energy to electrical energy via an engine (usually fuel-powered) that provides electrical current as input to a power source.

H

Back to top

Hardware Systems

Includes servers and network devices.

Heat Detector

A mechanical device that is sensitive to temperature and transmits a signal to a measuring or control instrument.

HIPAA

Acronym that stands for the Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health data provided to health plans, doctors, hospitals and other health care providers. The HIPAA Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic and the Security Rule deals specifically with Electronic Protected Health Information (EPHI). The Security Rule lays out three types of security safeguards required for compliance: administrative, physical, and technical.

Source: http://www.medicinenet.com/script/main/art.asp?articlekey=31785 and Wikipedia

HITECH

Health Information Technology for Economic and Clinical Health Act was enacted to promote the adoption and meaningful use of health data technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health data, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Source: http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

Hot Site

A duplicate of the respondent’s original site, with full computer systems and near-complete backups of user data.

HVAC

HVAC (heating, ventilating/ventilation, and air conditioning) is the technology of indoor and vehicular environmental comfort. Its goal is to provide thermal comfort and acceptable indoor air quality.

Source: Wikipedia

Hypervisor

A piece of software that provides abstraction of all physical resources (such as central processing units, memory, network, and storage) and thus enables multiple computing stacks (consisting of an operating system, middleware and application programs) called virtual machines to be run on a single physical host.

Source: NIST SP 800-125B

Hypervisor Console

A control panel for a virtual machine manager (hypervisor) which allows multiple operating systems to share a single hardware processor.

I

Back to top

Immediate Perimeter

A rack or cage that houses the Scoped Systems and Data.

Incident

Events outside normal operations that disrupt normal operational processes. An incident can be a relatively minor event, such as running out of disk space on a server, or a major disruption, such as a breach of database security and the loss of private and confidential customer data.

Incident Management

A term describing the activities of an company to identify, analyze, and correct hazards to prevent a future re-occurrence. These incidents within a structured company are normally dealt with by either an Incident Response Team (IRT), or an Incident Management Team (IMT). These are often designated before hand, or during the event and are placed in control of the company whilst the incident is dealt with, to restore normal functions.

Source: Wikipedia

Incident Severity

A ranking of an event’s significance that uses, at a minimum, a three-point scale: minor, moderately severe, and severe. For each level of severity, the respondent's IT department should define acceptable resolution times, escalation procedures, and reporting procedures.

Information Assets

Scoped target and/or system data utilized/owned by an company.

Information Security

Smetimes shortened to InfoSec, is the practice of defending data from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical). An data security program should include all aspects of the sensitivity of corporate data, including confidentiality, integrity and availability.

Source: Wikipedia

Information Security Review

An data security assessment is a measurement of the security posture of a system or company. The security posture is the way data security is implemented. Security assessments are risk-based assessments, due to their focus on vulnerabilities and impact. Security assessments rely on assessment methods that can accurately assess the Technology, People, and Process elements of security.

Source: Scoping Security Assessments - A Project Management Approach (SANS Institute Reading Room site - SANS Institute May 2011)

Intermediate Distribution Frame IDF

A free-standing or wall-mounted rack for managing and interconnecting the telecommunications cable between end user devices and a main distribution frame (MDF).

Internal Vulnerability Scan

A systematic review process using software tools designed to search for and map systems for weaknesses in an application, computer or network, executed from a network address within the Scoped Systems and Data network. Internal vulnerability scans are used to determine whether points of weakness in the security control system exist that could be exploited by a user with access to the internal network.

Internet

A global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions.

Internet Protocol (IP)

A networking standard that allows messages to be sent back and forth over the Internet or other IP networks.

Intranet

An IP network that resides behind a firewall and is accessible only to people who are members of the same company.

Intrusion Detection Systems (IDS)

A security inspection system for computers and networks that can allow for the inspection of systems activity and inbound/outbound network activity. The IDS key function identifies suspicious activity or patterns that may indicate a network or system attack.

Intrusion Protection System (IPS)

A more sophisticated Intrusion Detection System (IDS) that allows administrators to configure predefined actions to be taken if suspicious activity is detected.

Inventory

An itemized list of current assets.

L

Back to top

Local Backup

A method for backing up data on the local system. For example, an attached tape or storage device.

M

Back to top

Main Distribution Frame

A wiring rack that connects outside lines with internal lines. Main distribution frames are used to connect public or private lines entering the building to the respondent's internal networks

Malware

Is designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs.

Source: http://ithandbook.ffiec.gov/glossary.aspx

Man-trap

Two sets of doors whereby access to the second is not granted until the individual has passed through (and closed) the first, often referred to as a "man trap." A controlled turnstile is also considered an anti-tailgating/ piggybacking mechanism.

Map of Dependencies

A diagram that illustrates how a business process relates to its supporting capabilities. ("Supporting capabilities" include: people involved in the delivery of the business process, application software, middleware software, servers, storage, networking, physical facilities, and people involved in the IT and physical infrastructure management.)

Master Change Log

A document or database that contains a report of each change initiation request (CIR) (approved or rejected). The document or database must contain: - Reference to a CIR - Date submitted - Date of change - Name of affected system - Approval status (approved or rejected)

MD5

A one-way cryptographic hash algorithm that produces a unique 128-bit alphanumeric fingerprint of its input.

Media

Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).

Source: http://ithandbook.ffiec.gov/glossary.aspx

Mobile Code

Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).

Mobile Device

smartphones, tablet computers, laptops; anyng that is not affixed to a desk or operates wirelessly

Mobile Device Management Solution

Mobile device management (MDM) is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices. It can incorporate safeguards related to but not limited to password controls, remote wipe, remote lock, detection of jailbreak devices, encryption validation.

Mobile Device Policy

Policy implemented which governs the use of Mobile devices whether they be BYOD or corporate issued. This policy can incorporate details related to Security training, Terms of Use, constituent responsibilities, data handling and access controls.

Modem

A device that allows a computer or terminal to transmit data over an analog telephone line.

Multi-factor Authentication

Multifactor authentication requires the use of solutions from two or more of the three categories of factors: • Something the user knows (e.g., password, PIN). • Something the user has (e.g., ATM card, smart card). • Something the user is (e.g., biometric characteristic, such as a fingerprint). Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute multifactor authentication.

N

Back to top

N+1

N+1 redundancy is a form of resilience that ensures system availability in the event of component failure. Components (N) have at least one independent backup component (+1).

Source: Wikipedia

Network Address Translation (NAT)

A process of rewriting the source and/or destination addresses of IP packets as they pass through a network device.

Network Devices

Units that mediate data in a computer network. Computer networking devices are also called network equipment, Intermediate Systems (IS) or InterWorking Unit (IWU).

Network Segment

A portion of a computer network that is separated from the remainder of the network by a device such as a repeater, hub, bridge, switch or router. Each segment may contain one or multiple computers or other hosts. Network segments are typically established for throughput and/or security reasons.

Network time protocol (NTP)

A protocol designed to synchronize the clocks of computers over a network.

Node

Any physical device with a unique network address.

Non-Employees

Auditors, consultants, contractors, and vendors.

Non-Public Information (NPI)

Any personally identifiable or company proprietary data that is not publicly available. Non-public data includes but is not limited to: certain company proprietary data, such as internal policies and memorandums; and personal data such as a person’s name, address or telephone number. It also includes data requiring higher levels of protection according to the company’s security policy, such as company proprietary trade secrets or personal data that bundles a person’s name, address or telephone number with a Social Security number, driver’s license number, account number, credit or debit card number, personal identification number, health data, religious opinions or a user ID or password.

Non-Public Personal Information (NPPI)

Any personally identifiable data that is not publicly available. Non-public, personal data includes but is not limited to name, address, city, state, zip code, telephone number, Social Security number, credit card number, bank account number and financial history.

Notice Consent Language

Any data subject consent language in a privacy notice to be accepted by a data subject (expressly or by implication). The language may relate to consent to the entire privacy notice or to particular uses of the scoped privacy data where a data subject’s non-consent to this use of the scoped privacy data results in a data subject rejecting the privacy notice. Examples of uses include cross-border transfer of scoped privacy data, special use of the scoped privacy data or special local regulatory requirements.

O

Back to top

Open Web Application Security Project (OWASP)

An open, online community dedicated to enabling companys to conceive, develop, acquire, operate and maintain web applications that can be trusted.

Owner

An individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. Ownership is not an indication of property rights to the asset.

Ownership

A formally assigned responsibility for a given asset.

P

Back to top

Penetration Testing

A conventional security control and the one most widely used by software vendors.

Permission

Any data subject permission (opt in or opt out) required to use or share scoped privacy data that can be easily switched on and off, including for the following purposes: marketing, affiliate sharing, product use, promotions, newsletters, tailoring services to data subject’s particular requirements, behavioral and purchasing patterns, social networking and professional networking, excluding notice consent language.

Personal Health Records

A personal health record (PHR) is an electronic application used by patients to maintain and manage their health data in a private, secure, and confidential environment. PHRs are managed by patients.

Source: https://www.healthit.gov/providers-professionals/faqs/what-personal-health-record

Personal Identification Number (PIN)

A secret shared between a user and a system that can be used to authenticate the user to the system.

Personally Identifiable Informatin (PII)

NIST Special Publication 800-122 defines PII as "any data about a person maintained by an agency, including (1) any data that can be used to distinguish or trace a person's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other data that is linked or linkable to a person, such as medical, educational, financial, and employment data."

Source: Wikipedia and NIST 800-122

Physical Media

Any portable device or substance (e.g., paper) used to store data for specific and legitimate purposes. Examples of physical media include: - Magnetic tapes and disks - Cartridges, including 9-track, DAT, and VHS - Optical disks in CD and DVD format - Microfilm/fiche - Paper (e.g., computer-generated reports and other printouts) - Static memory devices, such as USB memory sticks

Port Scan

A systematic scan of a computer's ports that identifies open doors. Used in managing networks, port scanning also can be used maliciously to find a weakened access point from which to break into computer.

Post-Deployment Test Document

A document that provides evidence that the change was tested and approved in the production environment. The document must contain: - Reference to a CIR - Identified deployment resources - Deployment start date - Deployment end date - Expected results - Actual results - Approval signature - Approval date

Potential Access

Under ordinary circumstances, individuals that are not permitted access to Scoped Data are, however, in certain circumstances able or are permitted access to Scoped Data. For example: a senior executive who reviews Scoped Data in the course of an investigation, or a courier and truck driver who picks up documents in a locked shred bin and transports them in the locked shred bin to a warehouse for shredding.

Power Redundancy

Any type of power delivery mechanism that provides continuous power to connected systems in the event of a failure in the main delivery mechanism for electricity. Such mechanisms include multiple electric feeds, automatic failover generators, and uninterruptible power supplies.

Pre-Deployment Test Document

A document (electronic or paper) that provides evidence that the requested changes were tested prior to deployment in the production environment. A pre-deployment test document is inspected for: - Reference to a CIR - Identified testing resources - Testing start date - Testing end date - Expected test results - Actual test results

Privacy Incident

A privacy incident is the unauthorized collection, use, access, retention or disclosure of personal or otherwise sensitive data.

Privacy Inventory Flow

The current scoped privacy data inventory/list and flow by data subject category that has been approved by management of the company. A privacy inventory flow identifies the ownership of the scoped privacy data, its sources, collection methods, storage locations, uses (by who, where and for what purpose), sharing within the company and among its third parties, trans-border flows and adequacy mechanisms chosen to ensure the protection of such scoped privacy data, security, retention and deletion schedules and mechanisms.

Privacy Notice

Notice given to data subjects on the collection, use, storage, sharing, transfer, retention and destruction of their scoped privacy data in accordance with privacy applicable law and company policy.

Privacy Policy

An company’s internal policy adopted for the life cycle of the scoped privacy data.

Privacy Risk Assessment

A privacy risk/impact assessment states what personally identifiable data (PII) is collected and explains how that data is maintained, how it will be protected and how it will be shared. A PIA should identify: - Whether the data being collected complies with privacy-related legal and regulatory compliance requirements. - The risks and effects of collecting, maintaining and disseminating PII. - Protections and processes for handling data to alleviate any potential privacy risks. - Options and methods for individuals to provide consent for the collection of their PII. Generally Accepted Privacy Principles (GAPP) is a recognized framework for assessing privacy risk. GAPPoperationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles.

Source: http://searchcompliance.techtarget.com/definition/Privacy-impact-assessment-PIA and http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/10261378ExecOverviewGAPP.pdf

Privileged Access

This access grants an employee access to more than usual company data or make changes to the company network. Companies need privileged users because they have access to source code, file systems and other assets that allow them to upgrade the systems or make other technical changes.

Source: 2016 AUP Glossary

Protected Health Information (PHI)

The Privacy Rule protects individually identifiable health data, called PHI, held or transmitted by a covered entity or its business associate, in any form, whether electronic, paper, or verbal. PHI includes data that relates to all of the following: - The individual fs past, present, or future physical or mental health or condition - The provision of health care to the individual - The past, present, or future payment for the provision of health care to the individual PHI includes many common identifiers, such as name, address, birth date, and Social Security number.

Source: HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES

Protected Scoped data

Scoped data or any other data that requires a higher level of protection or special treatment due to its sensitivity under: security applicable law; company security policy; and/or as identified in the scope definition of protected scoped data of the Shared Assessments Standardized Information

Gathering (SIG) questionnaire and Shared Assessments Agreed Upon Procedures (AUP), a tool for standardized onsite assessments. This may include: scoped data, such as name, address or telephone number in conjunction with Social Security number, driver's license number, account number, credit or debit card number, personal identification number, user ID or password; a person's health data; company trade secrets or certain confidential data. Data that falls under the definitions of both scoped data and protected scoped data (for example, credit card details).

Protected Scoped Privacy data

Any scoped privacy data required to have a higher level of protection or special treatment under privacy applicable law due to its sensitivity, e.g., encryption. This includes EU "sensitive personal data" (health, religion, criminal records, trade union membership, sexual orientation and race). In the US, protected scoped privacy data includes name, address or telephone number in conjunction with Social Security number, driver's license number, account number, credit or debit card number, personal identification number or user ID or password.

Protocol

A set of rules and formats that enable the proper exchange of data between different systems.

Publicly Accessible

In networking terms, able to accept a connection originating from the public domain, e.g., the Internet.

Q

Back to top

Quality Analysis and User Acceptance Testing (QA UAT)

QA testing usually precedes UAT. QA examines the functional behavior of individual components and integrated feature-level capacity. UAT typically refers to the final testing process prior to deployment.

R

Back to top

Raised Floor

Used in data center construction, a raised floor above the "true" floor allows air conditioning flow and wiring to pass freely under equipment. The space between the true and raised floors is accessed by removable floor tiles.

Receiver Company

The company that has contracted with a service provider for a specific service.

Recovery Time Objective (RTO)

The targeted duration of time and a service level for which a business process must be restored after a disaster or disruption of service, in order to avoid unacceptable consequences, should a break occur in business continuity.

Red Flag

The Red Flags Rule requires many businesses and companys to implement a written identity theft prevention program designed to detect the “red flags” of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage. A program can help businesses spot suspicious patterns and prevent the costly consequences of identity theft. The Federal Trade Commission (FTC) enforces the Red Flags Rule with several other agencies. “Red Flags Rule" is formally known as the "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule”. The rule applies only to federally regulated financial institutions, and through the FTC, to certain creditors. The term Covered Accounts is contained in the rule.

Source: ftc.gov and Web Hull

Remediation

The process by which companys address computer systems control deficiencies and maturity gaps to ensure that deficiencies are appropriately corrected.

Remote Access

Remote access refers to the ability to access a computer, such as a home computer or an office network computer, from a remote location. This allows employees to work offsite, such as at home or in another location, while still having access to a distant computer or network, such as the office network.

Source: Technopedia

Removable Device

Removable devices are 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.

Residual Risk Rating Scoring Method

A calculation of the risk that remains after security controls have been applied.

Risk Assessment

The process of identifying variables that have the potential to negatively impact an company’s ability to conduct business. A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.

Source: TechTarget and FFIEC IT Examination Handbook Glossary

Risk Governance

Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented. Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks Effective risk governance should provide the operating model and decision-making framework needed to identify and respond to risks.

Source: https://www.irgc.org/risk-governance/what-is-risk-governance/

Risk Prioritization Scoring Method

A systematic approach that quantifies risk in terms of loss potential, then sequences individual risks to determine the order in which compensating controls should be implemented.

Risk Scenario

An IT risk scenario is a description of an IT related event that can lead to a business impact, when and if it should occur. A risk scenario is characterized by: - a threat actor - a threat type - event - asset or resource affected - time The risk scenario structure differentiates between loss events (events generating the negative impact), vulnerabilities or vulnerability events (events contributing to the magnitude or frequency of loss events occurring), and threat events (circumstances or events that can trigger loss events).

Source: Wikipedia

Role-Based User Access

Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. Roles are defined according to job competency, authority and responsibility within the enterprise.

Root cause analysis

A root cause is a factor that caused a nonconformance and should be permanently eliminated through process improvement. Root Cause Analysis (RCA) describes a wide range of approaches, tools, and techniques used to uncover causes of problems. RCA is based on the basic idea that effective management requires more than merely “putting out fires” for problems that develop, but finding a way to prevent them.

Source: ASQ.org

S

Back to top

Safe Harbor

Intended for U.S. companys that process personal data collected in the EU, the Safe Harbor Principles are designed to assist eligible companys to comply with the EU Data Protection Directive and maintain the privacy and integrity of that data. NOTE: The EU Privacy Shield program is the successor of the EU US Safe Harbor program. Announced in Feb 2016 it became operational on the 1st August 2016

Source: https://www.privacytrust.com/guidance/safe_harbor.html

Sanctions Check

In most countries, companys are prohibited by law from doing business with drugs and arms merchants and terrorist companys. Sanctions lists ranging from OFAC to the EU Consolidated Lists to the Interpol Most Wanted to the Hong Kong and Singapore Monetary Authority exist. Part of due diligence in vendor selection should include screening of the third party against sanctions lists.

Source: should this be removed from the questionnaire? P.3.5

Scoped Data

A client’s non-public personal data (NPPI), protected health data (PHI), personal data (PI) or non-public data that is stored, transmitted or processed by the service provider. Scoped data may also include any data selected as being in scope by the company or client at the scoping of the engagement. Any reference to scoped data includes protected scoped data, where applicable.

Scoped Privacy Data

Any data relating to a data subject, who can be identified directly or indirectly, by that data, and in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Examples of scoped privacy data include name, address, telephone number and email address. Scoped privacy data may exist in any media or format. Any reference to scoped privacy data includes protected scoped privacy data, where applicable.

Scoped Systems and Data

Computer hardware, software and/or Non-Public Personal Information that is stored, transmitted, or processed by the service provider in scope for the engagement.

Scoping Meeting

A meeting held prior to commencement of a Shared Assessments engagement, to determine the Scoped Systems and Data to be included in a company's Standardized Information Gathering Questionnaire (SIG) and Agreed Upon Procedures (AUP) assessment.

Secure Code Review

The process of identifying whether software code meets the respondent's security requirements.

Secure Perimeter

A space fully enclosed by walls that surround the immediate perimeter and that extend from floor to ceiling (beyond raised floors and ceilings), which is contained, and whose points of entry are secured.

Secure Socket Layer (SSL)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system with two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of the message.

Secure Workspace

An environment from where people work from their desks with the purpose of accessing, editing or inputting Scoped Systems and Data on a computer, telephone or physical media, e.g., a BPO or call center environment.

Secure Workspace Perimeter

A space fully enclosed by walls that surround the Secure Workspace which is contained, and whose points of entry and exit are secured.

Security Applicable Law

Applicable laws, enactments, regulations, binding industry codes, regulatory permits and licenses which are in effect that address the protection, handling and security of scoped data and protected scoped data and that are determined to be in scope by the company or client at the scoping of the engagement.

Security Architecture Risk Analysis

Defines concepts, methods, and techniques for analyzing the architecture and design of software systems for security flaws.

Security Policy

A published document or set of documents defining requirements for one or more aspects of data security.

Segmentation / Separation (of data)

see Data Segmentation / Separation

Sensitive customer financial information

A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer data also includes any combination of components of customer data that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

Source: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Sensitive Information

Also known as “scoped data,” any customer data stored at the company’s facility. This data may be stored in the form of physical media, digital media or any other storage medium.

Server

A computer that makes services, such as access to data files, programs, and peripheral devices, available to workstations on a network.

Service Account

A service account is a user account that has been created to run a particular piece of software or service. The account belongs to the software application instead of to a person end user.

Service Level Agreement (SLA)

An agreement that details the responsibilities of an IT service provider, the rights of the service provider’s customers, and the penalties assessed when the service provider violates any element of the SLA. SLAs also identify and define the service, plus the supported products, evaluation criteria, and quality of service customers should expect. SLAs are typically measured in terms of metrics. Examples include processing completion times and systems availability times.

Source: FFIEC IT Examination Handbook Glossary

Service Provider

An subcontractor that provides outsourced services, such as data processing, business operations, applications, systems or staffing.

Service Set Identifier (SSID)

A 32-character unique identifier attached to the header of packets sent over a wide area network to identify each packet as part of that network.

Simple Mail Transfer Protocol (SMTP)

The de facto standard for email transmissions across the Internet.

Smoke Detector

A mechanical device that is sensitive to the presence of smoke or particulate material in the air that transmits a signal to a measuring or control instrument.

Software

Vendor developed software code used for custom or commercial-off-the-shelf purposes.

Software Architecture

The process of defining a structured software solution that meets all of the technical and operational requirements, while optimizing common quality attributes such as performance, security, and manageability.

Software Security Group

A group whose charter is to assist in the design, review and implementation of software that protects the data and resources contained in and controlled by that software.

Status Change

Change to employment status that is recorded by human resources, such as promotions, demotions or departmental changes.

Stewardship

The act of managing and maintaining a given asset.

Storage Facility

The physical location where target systems and data are stored.

Strong Password

Password length must be a minimum of seven (7) characters, must not to contain a common usage word or a word found in the English dictionary, may not contain user name, any part of a full name or access level of the user and must contain characters from at least three (3) of the following four (4) classes of characters: • Upper case letters (A, B, C, ...Z) • Lower case letters (a, b, c, ...z) • Numbers (0,1, 2, ...9) • Non-alphanumeric ("special characters") such as punctuation symbols

Subcontractor

is a business or a person that signs a contract to perform part or all of the obligations of another's contract.

System Owner

The business unit that retains financial ownership or decision rights for the business use of the asset.

System Steward

The primary assigned administrator responsible for maintenance and day-to-day tasks that support the business.

Systems Development Life Cycle (SDLC)

A process for planning, creating, developing, testing and deploying a software application or computer system.

T

Back to top

Target System

Computer hardware and software in scope for the engagement that contains scoped data.

Third Party

All entities or persons that work on behalf of the company but are not its employees, including consultants, contingent workers, clients, business partners, service providers, subcontractors, vendors, suppliers, affiliates and any other person or entity that accesses Scoped Systems and Data.

Threat Impact Calculation Method

A systematic method of determining the loss potential of a particular threat, based on the value of assets affected.

Threat Modeling

Threat modeling allows you to systematically identify and rate the threats that are most likely to affect your system. By identifying and rating threats based on a solid understanding of the architecture and implementation of your application, you can address threats with appropriate countermeasures in a logical order, starting with the threats that present the greatest risk. Threat modeling has a structured approach that is far more cost efficient and effective than applying security features in a haphazard manner without knowing precisely what threats each feature is supposed to address.

Threat Probability Calculation Method

A systematic method of determining the potential for a particular threat to occur, based on the likelihood of the occurrence collected from internal staff, past records, and official security records. Threats x Vulnerability x Asset Value = Total Risk (Threats x Vulnerability x Asset Value) x Controls Gap = Residual Risk

Token

A unique identifier generated on both a host and small, user-held device that allows the user to authenticate to the host.

Transmission Control Protocol (TCP)

A protocol of TCP/IP networks. TCP, the basic communication language (or protocol) of the Internet, enables two hosts to establish a connection and exchange streams of data.

True Ceiling

The permanent overhead interior surface of a room, constructed of solid building materials offering resistance to and evidence of unauthorized entry.

True Floor

The permanent bottom interior surface of a room, constructed of solid building materials offering resistance to and evidence of unauthorized entry.

Two-factor Authentication

(aka multi-factor authentication) The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric).

Source: FFIEC_CAT_App_C_Glossary_June_2015_PDF5

U

Back to top

UI

In data technology, the user interface (UI) is everything designed into an data device with which a human being may interact -- including display screen, keyboard, mouse, light pen, the appearance of a desktop, illuminated characters, help messages, and how an application program or a Web site invites interaction and responds to it.

Source: TechTarget

Unapproved

Operating without consent.

Unidentified

Being or having an unknown or unnamed source.

Uninterruptible Power Supply (UPS)

A power supply consisting of a bank of batteries, which is continually charged. When power fails, the UPS becomes the source of electrical current for computer equipment until the batteries are discharged. A UPS is often connected to a generator that can provide electrical power indefinitely.

User Datagram Protocol (UDP)

A communications protocol within the Internet protocol suite. UDP, which uses a simple, connectionless transmission model with a minimum of protocol mechanism, performs similar functions as TCP (except datagrams are created instead of packets), but UDP lacks the flow-control and error-recovery functions, allowing for fewer system resources.

V

Back to top

Vendor Management

Vendor management is a discipline that enables companys to control costs, drive service excellence and mitigate risks to gain increased value from their vendors throughout the deal life cycle. Vendor risk management (VRM) is a comprehensive plan for identifying and decreasing potential business uncertainties and legal liabilities regarding the hiring of 3rd party vendors for data technology (IT) products and services.

Source: Gartner IT Glossary and TechTarget

Vibration Alarm Sensor

An alarm that responds to vibrations in the surface onto which it is mounted. A normally closed switch momentarily opens when the sensor is subjected to a vibration of sufficiently large amplitude.

Virtual Machine (VM)

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine is comprised of a set of specification and configuration files and is backed by the physical resources of a host.

Source: vmware.com

Virtual Private Network (VPN)

A communication tunnel running through a shared network, such as the Internet, which uses encryption and other security mechanisms to ensure the data cannot be intercepted and that the data senders and receivers are authenticated.

Volumetric Alarm Sensor

An alarm sensor designed and employed to detect an unauthorized person in a confined space when the space is normally unoccupied. Such alarms include ultrasonic, microwave, and infrared sensors.

Vulnerability

A hardware, firmware, or software flaw that leaves an computer system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to data or to disrupt critical processing.

Source: FFIEC IT Examination Handbook Glossary

Vulnerability Management

Vulnerability management is the process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of an company (e.g. in case the impact of an attack would be low or the cost of correction does not outweigh possible damages to the company).

Source: Implementing a vulnerability management process - SANS Institute Reading Room

W

Back to top

War Walk

Also known as "war drive," using a laptop to "sniff" for wireless access points. War walking may be used to locate a public access point for personal use or as a controls assessment to identify access points that are inadequately secured and may indicate an elevated risk of breach.

Warm Site

A remote facility which replicates production data in set intervals.

Water Sensor

A mechanical device sensitive to the presence of water or moisture that transmits a signal to a measuring or control instrument.

Whistleblowing Policy

A policy protecting anyone who has and reports insider knowledge of illegal activities occurring in an company. Whistleblowers can be employees, suppliers, contractors, clients or any individual who somehow becomes aware of illegal activities taking place in a business, either through witnessing the behavior or being told about it.

Wireless Networks

A wireless network, a.k.a. wireless local-area network (LAN), uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications instead of physical cables like a wired network does. An example of wireless network is when you connect a laptop to a WiFi hotspot at a cafe, hotel, airport lounge or other public place you're connecting to that business's wireless network.

Workstation

(1) Single-user computers typically linked together to form a local area network, that can also be used as standalone systems. (2) In networking, any computer connected to a local area network, including a workstation or personal computer.

X

Back to top

XSS

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

Source: Wikipedia