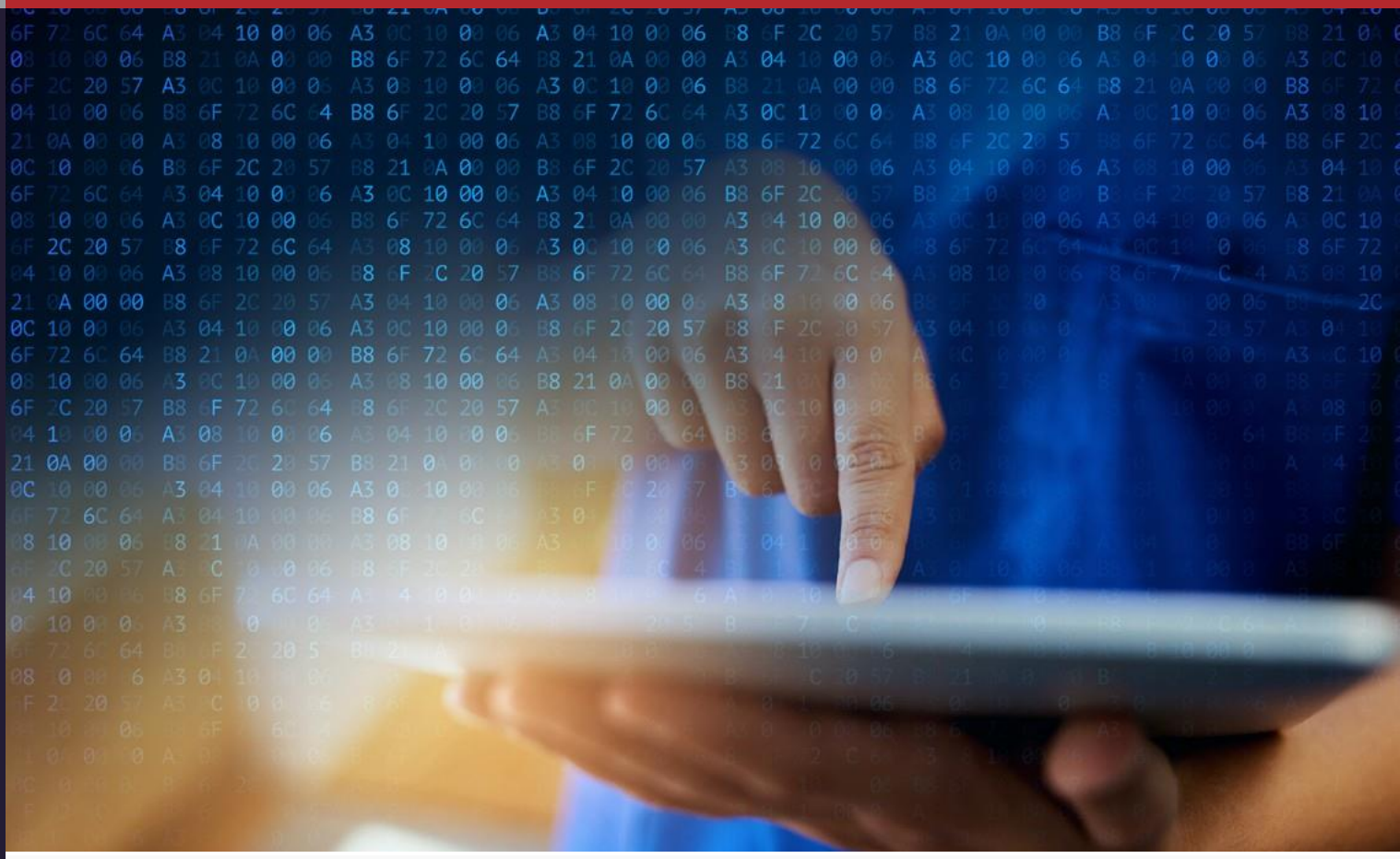
HITRUST



Glossary of Terms and Acronyms

Version 5

June 2020

Contents

Cautionary Notes

This publication contains material from HITRUST and other authoritative sources, e.g., ITIL®, and may be subject to multiple copyrights. Source of a potential copyright is indicated for each term contained in this document. A reference list of sources cited is included.

Note: Some definitions may be altered slightly to make them more generally applicable, such as removing language from a NIST definition that is particular to the U.S. Government or otherwise modified to accommodate the HITRUST Risk Management Framework. Such definitions are indicated by the word "*adapted*," after the source.

Definitions obtained from a discussion of the term, rather than a glossary, or obtained from a similar term (or multiple terms) in a glossary, are indicated by the word "*derived*," after the source.

Version History

Version #	Date Reviewed	Reviewed By	Brief Description
1.0	Dec 2009	HITRUST	Supported the initial release of the HITRUST CSF.
2.0	Aug 2017	HITRUST	Extensively expanded and updated based on a review of version 9 of the HITRUST CSF and the CSF Assurance Program.
3.0	Feb 2018	HITRUST	Added terms from the addition of 23 NYCRR 500 and the EU GDPR to the HITRUST CSF v9.1.
4.0	Oct 2019	HITRUST	Expanded and updated based on a review of version 9.3 of the HITRUST CSF and the CSF Assurance Program.
5.0	Jun 2020	HITRUST	Expanded and updated based on a review of version 9.4 of the HITRUST CSF.

List of Terms

Access Control	A security method that ensures users have the minimum, appropriate access level to electronic and physical assets. [HITRUST] The process of granting or denying specific requests to 1) obtain and use information and related information processing services; and 2) enter specific physical facilities. [NIST IR 7298 r2]
Access Control List (ACL)	A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. [NIST IR 7298 r2]
Accountability	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. [NIST IR 7298 r2]
Accounting of Disclosures	A listing of organizations and individuals who have received access to or have been provided with a copy of an individual's protected health information. [HHS HAS, derived from discussion]
Ad hoc	See Undocumented.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [NIST IR 7298 r2]
Adversary	Individual, group, organization or government that conducts or has the intent to conduct detrimental activities. [NIST IR 7298 r2]
Alternate Control	A compensating control that has been submitted and approved for general use by the HITRUST Alternate Controls Committee. See Compensating Control. [HITRUST]
Analysis Approach	The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated. [NIST SP 800-53 r4, derived from discussion]
Aperiodic	Of irregular occurrence. [Merriam-Webster]
Application	A software program that performs a specific function, or set of functions, and can be executed without access to system control, monitoring, or administrative privileges. [NIST IR 7298 r2, adapted]
Assessment	See Security Control Assessment or Risk Assessment. [HITRUST]

Assessor	An individual or organization that conducts control assessments, including HITRUST Approved Assessors, self-assessors or independent assessors (e.g., internal/external auditors or third-party assessors). [HITRUST]
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. [ISACA]
Asset Owner	An individual the organization designates as responsible for the overall procurement, development, integration, modification, or operation and maintenance of an asset. See asset. [NIST IR 7298 r2, derived from Information System Owner]
Assurance	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. [NIST IR 7298 r2]
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [NIST IR 7298 r2]
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NIST IR 7298 r2]
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period. [NIST IR 7298 r2]
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [NIST IR 7298 r2]
Authentication Data	Security-related information used to authenticate users and/or authorize user transactions (e.g., passwords and/or personal identification numbers). [PCI DSS, derived from Sensitive Authentication Data]
Authentication Parameter	Variables specified by an information system to authenticate a user or process (e.g., identity, role, clearance, operational need, risk, and heuristics). [HITRUST]
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication. [NIST IR 7298 r2]
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges. [NIST IR 7298 r2]
Availability	Ensuring timely and reliable access to and use of information. [NIST IR 7298 r2]

Best Practice	A technique, method, process, or procedure that has been shown by research and experience to produce optimal results, and that is established or proposed as a standard suitable for widespread adoption. [Merriam-Webster, adapted]
Binding Corporate Rules	Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. [EU GDPR]
Biometric Data	Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data. [EU GDPR]
Breach	The unauthorized acquisition, access, use, or disclosure of sensitive or covered information (e.g., protected health information), which compromises the security or privacy of such information. [HHS HAS, adapted]
Bring Your Own Device (BYOD)	All non-organizational devices (personally-owned), managed by the employees themselves, that are used to conduct the organization's businesses. [NIST SP 800-114 r1, adapted]
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity, but is not part of the covered entity's workforce. A member of the covered entity's workforce is not considered a business associate; however, a covered healthcare provider, health plan, or healthcare clearinghouse can be a business associate of another covered entity. [HHS HAS, adapted]
Business Continuity	Preventing, mitigating, and/or recovering from disruption to restore normal business operations following a security incident or other disaster. The terms "business resumption planning," "disaster recovery planning," and "contingency planning" also may be used in this context; they all concentrate on the recovery aspects of continuity. [ISACA, adapted]
Business Continuity Plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business functions will be sustained during and after a significant disruption. [NIST IR 7298 r2]
Business Impact Analysis (BIA)	An analysis of an enterprise's requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption. [NIST IR 7298 r2]
Business Process	A process that is owned and carried out by the business. A business process contributes to the delivery of a product or service to a business customer. For example, a retailer may have a purchasing process that helps to deliver services to its business customers. [ITIL]

Capability	The ability of an organization, person, process, application, IT service or other configuration item to carry out an activity. Capabilities are intangible assets of an organization. [ITIL]
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system, and specific scoring criteria for the maturity of the controls' implementation have been met under the HITRUST CSF Assurance Program. [NIST IR 7298 r2, adapted]
Change	The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items. [ITIL]
Change Control	Processes and procedures to review, test, and approve changes to systems and software for impact before implementation. [PCI DSS]
Change Management	The process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services. [ITIL]
Choice	An individual's ability to determine whether or how their personal information may be used or disclosed by the entity that collected the information. Also, the ability of an individual to limit certain uses of their personal information. For example; an individual may have choice about whether to permit a company to contact them or share their data with third parties. Can be express or implied. [IAPP]
Classification	See Data Classification. [HITRUST]
CMS-defined Level of Independence	No perceived or actual conflict of interest with respect to the developmental, operational, and/or management chain associated with the information system and the determination of security and privacy control effectiveness. [CMS Assessment]
Common Control	A security control that is inherited by one or more organizational information systems. See Security Control Inheritance. [NIST IR 7298 r2]
Compensating Control	See Compensating Security Control. [HITRUST]
Compensating Security Control	A safeguard or countermeasure employed by an organization in lieu of a primary security control that provides equivalent or comparable protection for an information system. Synonymous with Alternate Control. [NIST IR 7298 r2, adapted]
Confidential Information	Information that is not to be disclosed to unauthorized individuals, entities, or processes. [NIST IR 7298 r2, derived from Confidentiality]

Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST IR 7298 r2]
Configuration	A generic term used to describe a group of configuration items that work together to deliver an IT service, or a recognizable part of an IT service. Configuration is also used to describe the parameter settings for one or more configuration items. [ITIL]
Configuration Management	The process to control changes to a set of configuration items over a system life cycle. [ISACA, adapted]
Consent	An individual's way of giving permission for the collection, use, or disclosure of his or her information. Consent may be affirmative; i.e., opt-in; or implied; i.e., the individual didn't opt out. (1) Explicit Consent: A requirement that an individual "signifies" his or her agreement with a data controller by some active communication between the parties. (2) Implicit Consent: Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual. See Choice. [IAPP, adapted]
Continuous Monitoring	The process implemented to maintain ongoing awareness to support organizational risk decisions. See Information Security Continuous Monitoring, Risk Monitoring, and Status Monitoring. (Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.) [NIST IR 7298 r2, adapted]
Control Assessment	See Security Control Assessment. [HITRUST]
Control Objective	A statement of the desired result or purpose to be achieved by one or more controls within a HITRUST CSF Control Category. [ISACA, adapted]
Control Reference	HITRUST CSF control number and title. [HITRUST]
Control Specification	The policies, procedures, guidelines, practices, or organizational structures specified in a control, which can be of administrative, technical, management, or legal nature, to meet a control objective. [HITRUST]
Controlled Area	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. [NIST IR 7298 r2]
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. [EU GDPR]

Covered Entity	A health plan, a healthcare clearinghouse, or a healthcare provider who transmits any health information in electronic form regarding a HIPAA transaction. [HHS HAS, adapted] Any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law. [NYSDFS CS]
Covered Information	Any type of information subject to security, privacy, and/or risk regulations that is to be secured from unauthorized access, use, disclosure, disruption, modification, or destruction to maintain confidentiality, integrity, and/or availability. [HITRUST]
Critical Access Rights	An individual's ability to access information supporting critical business and/or clinical operations. The criticality of an information system is generally provided in the information system's BIA. [HITRUST]
Criticality	A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. Criticality is often determined by the impact to the organization due to a loss of integrity or availability. [NIST IR 7298 r2, adapted]
Cryptographic Controls	Safeguards that employ cryptography to achieve the desired protection. Examples include using encryption to protect confidentiality and using digital signatures or message authentication codes to protect authenticity and integrity. [HITRUST]
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [NIST IR 7298 r2]
Cyber Incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident. [NIST IR 7298 r2]
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks. [NIST IR 7298 r2]
Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [NIST IR 7298 r2]

Data Classification	The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the enterprise. [ISACA]
Data Concerning Health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. [EU GDPR] A subset of protected health information (PHI) as defined under the Health Insurance Portability and Accountability Act (HIPAA). [HITRUST]
Data Custodian	An individual or organization (e.g., Human Resources department) to which an information asset has been entrusted by another (e.g., employee) for safekeeping regardless of ownership. [HITRUST]
Data Owner	The individual(s), normally a manager or director, who has responsibility for the integrity, accurate reporting and use of computerized data. [ISACA]
Data Use Agreement	An agreement between a health provider, agency, or organization and a designated receiver of information to allow for the use of limited health information for research, public health, or healthcare operations. The agreement assures that the information will be used only for specific purposes. [HHS HAS, derived from discussion]
Defense-in-Breadth	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). See Defense-in-Depth. [NIST IR 7298 r2]
Defense-in-Depth	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle. See Defense-in-Breadth. [NIST IR 7298 r2]
De-identification	The process of anonymizing data so that the risk of re-identifying an individual is minimized to an acceptable level. [HITRUST]
Denial-of-Service (DoS) Attack	An attack meant to consume resources or shut down a machine or network, depriving legitimate users of the service or resource they expected. [Palo Alto Networks, derived from discussion]
Detective Control	A control that is used to identify and report when errors, omissions, and unauthorized uses or entries occur. [ISACA, adapted]

Digital Certificate	A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender's private key or applying a one-way hash function. [ISACA]
Digital Signature	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. [NIST IR 7298 r2]
Direct Treatment Relationship	A treatment relationship between an individual and a health care provider that is not an indirect treatment relationship. See Indirect Treatment Relationship. [HHS HAS]
Disaster	An unfavorable, natural or man-made, event (e.g., fire, hurricane, terrorism) that may result in a major hardware or software failure, destruction of facilities, or other major loss of enterprise capability. [NIST IR 7298 R2, derived from Disaster Recovery Plan]
Disaster Recovery Plan (DRP)	A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. [NIST IR 7298 r2]
Disclosure	The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. [HHS HAS]
Distributed Control System (DCS)	Information technology used to control production systems within the same geographic locations for industries such as oil refineries, water and wastewater treatment, electric power generation plants, chemical manufacturing plants, automotive production, and pharmaceutical processing facilities. [NIST SP 800-82 r2, derived from discussion]
Distributed Denial-of-Service (DDoS) Attack	An attack that occurs when multiple systems, from many locations, orchestrate a synchronized Denial-of-Service attack to a single target. [Palo Alto Networks, adapted]
Downtime	Total period that a service or component is disrupted (not operational). [NIST IR 7298 r2, derived from Maximum Tolerable Downtime]
Due Care	The level of care expected from a reasonable person of similar competency under similar conditions. [ISACA]
Due Diligence	The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis. [ISACA]
E-Commerce	A commercial (buying or selling) transaction conducted through an electronic mean (e.g., on the Internet). See Transaction. [HITRUST] The use of network technology (especially the internet) to buy or sell goods and services. [NIST]

Electronic Health Record (EHR)	An electronic record of all or part of an individual's medical file that may be created, collected, managed, and/or shared across multiple healthcare settings. [CMS Assessment, adapted].
Electronic Signature	The process of applying any mark in electronic form with the intent to sign a data object. See also Digital Signature. [NIST IR 7298 r2]
Embedded System	Information system that is an integral part of a larger system. [NIST IR 7298 r2, derived from Embedded Computer]
Encryption	Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. [NIST IR 7298 r2]
Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. [NIST IR 7298 r2]
Entropy	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. [NIST IR 7298 r2]
Escalation	In incident management, the process of bringing an incident to someone with more expertise/authority if it cannot be resolved by first-line support within a pre-established period of time. [HITRUST]
Event	See Security Event. [HITRUST]
Exploit	Full or partial use of a vulnerability for the benefit of an attacker. [ISACA, adapted] The successful execution of a code that takes advantage of a weakness or flaw. [HITRUST]
Exploitation	The process of taking advantage of a privacy or security vulnerability. [HITRUST]
Exposure	The potential loss to an area of business due to the occurrence of an adverse event. [ISACA, adapted]
External Information System (or Component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. [NIST IR 7298 r2]

External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. [NIST IR 7298 r2]
External Parties	Contractors, vendors, business partners, or other persons not directly employed by an organization. [HITRUST]
Facility	A building or premise being used by an organization or its vendors and business partners to conduct work on behalf of an organization. [HITRUST]
Failure	Failure is typically used to describe a disruption in service. Not all faults result in a service failure as there may be redundancy built into the infrastructure. [HITRUST]
Full Disk Encryption (FDE)	The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product. [NIST IR 7298 r2]
Good Security Practice	See Best Practice. [HITRUST]
Governance	The method by which an enterprise ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives are achieved. It involves setting direction through prioritization and decision making, and monitoring performance and compliance against agreed-on direction and objectives. [ISACA, adapted]
Group Health Plan	An employee welfare benefit plan established or maintained by an employer or by an employee organization (such as a union), or both, that provides medical care for participants or their dependents directly or through insurance, reimbursement, or otherwise. [DOL]
Guideline	A description of a particular way of accomplishing something that is less prescriptive than a procedure. [ISACA]
Hash Algorithm	A one-way cryptographic function that takes an input of an arbitrary length and produces an output that is a standard-sized binary string. The output is unique to the input in a way that a minor change to the input will result in a completely different output; however, the input cannot be readily determined by output. [ISACA, derived from Hash]

Health Care Operations	Any of the following activities of a covered entity that relate to its covered functions (e.g., acting as a health care provider or an employer group health plan): (i) conducting quality assessment and improvement activities; (ii) reviewing the competence or qualifications of health care professionals; (iii) underwriting (except as prohibited when involving genetic information), premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits; (iv) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (v) business planning and development; and (vi) business management and general administrative activities of the entity. [HHS HAS, adapted]
Health Care Provider (or Healthcare Provider)	A provider of services, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. [HHS HAS, adapted]
Health Information	Any information, whether oral or recorded in any form or medium, that (i) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. [HHS HAS, adapted]
Health Information Exchange	The electronic movement of health-related information among organizations according to nationally-recognized standards (e.g., X12 EDI and HL7). [Medscape, adapted]
Health Insurance Portability and Accountability Act (HIPAA)	A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F of HIPAA gives the Department of Health and Human Services the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. Also known as the Kennedy-Kassebaum Bill, K2, or Public Law 104-191. [HITRUST]
Health Plan	A type of insurance purchased in order to pay for the cost of medical care, either through an individual or group plan. “Plan” shall have the same meaning as the term “Health Plan.” [HHS HAS, adapted]

Healthcare (or Health Care)	Care, services, or supplies related to the health of an individual, including (i) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (ii) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. [HHS HAS, adapted]
HIPAA Rules	The privacy, security, breach notification, and enforcement rules at 45 CFR Parts 160 and 164 of HIPAA that establish national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. [HHS SR, adapted]
HITECH	Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH), found at Title XIII of the American Recovery and Reinvestment Act of 2009, and any regulations promulgated thereunder, including all amendments to the HIPAA Rules. [HITRUST]
HITRUST Approved CSF Assessor	An organization that has been approved by HITRUST for performing assessments and services associated with the CSF Assurance Program and the HITRUST CSF. HITRUST Approved CSF Assessors are critical to HITRUST's efforts to provide trained resources to organizations of varying size and complexity to assess compliance with data protection control requirements and document corrective action plans that align with the HITRUST CSF. [HITRUST]
HITRUST CSF	A framework for managing information security and privacy risks and compliance. [HITRUST]
HITRUST CSF Assessment	An data protection assessment provided by an assessor to organizations in accordance with the HITRUST Assurance Program. [HITRUST]
HITRUST CSF Assurance Program	The programs and systems for use of the HITRUST CSF and CSF tools in connection with data protection assurance assessments according to the standards set forth by HITRUST. [HITRUST]
HITRUST CSF Licensee	An entity that is an authorized licensee of the HITRUST CSF. [HITRUST]
HITRUST CSF Practitioner	A data protection practitioner who (i) meets criteria established by HITRUST of background and experience in industries which utilize security systems set forth in the Requirements and Procedures; (ii) has completed the HITRUST Training for HITRUST CSF Practitioners program as subject matter specialists in the subjects of HITRUST CSF and HITRUST CSF Assessments; (iii) continually maintains his or her qualifications by participating in continuing education as HITRUST may reasonably require; and (iv) is available to assist in conducting or supervising HITRUST CSF Assessments. [HITRUST]

HITRUST CSF Submission	The electronic submission to HITRUST of a file/object containing the results of a HITRUST CSF Assessment, either by the assessed entity as a self-assessment or by a HITRUST Approved CSF Assessor. [HITRUST]
HITRUST CSF Tools	The HITRUST CSF and related materials HITRUST deems necessary to perform information security and privacy assessments of organizations in accordance with the HITRUST Assurance Program. HITRUST CSF Tools may include, but not be limited to, Information Security Control Specifications, a Standards and Regulations Mapping Device, Assessment and Reporting Tools, an Implementation Manual, Cross-Reference Matrix and a Readiness Assessment Tool. [HITRUST]
HITRUST Organization	Refers to members of the HITRUST community, e.g., healthcare (covered entities and their business associates) or other industry and government organizations that have adopted the CSF in some way, either as a simple reference for accepted best practices or as a compliance standard. [HITRUST]
HITRUST Participating Organizations	Organizations that have adopted the HITRUST CSF as the data protection, risk, and compliance framework used internally and/or for third-parties. [HITRUST]
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized use or disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [NIST IR 7298 r2]
Impact Level	See Impact. [NIST IR 7298 r2]
Impact Value	The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type; may be expressed qualitatively (e.g., low, moderate, or high) or quasi-quantitatively (e.g., 1, 2, 3). [NIST IR 7298 r2, adapted]
Implementation Requirements	Detailed information to support the implementation of the control and meeting the control objective. [HITRUST]
Incident	A violation or imminent threat of violation of computer security policies, personal data protection policies, acceptable use policies, or standard security or privacy practices. [NIST IR 7298 r2, adapted]
Incident Response Plan	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 system(s). [NIST IR 7298 r2]
Independent	With respect to an assessor or measure, one that is not influenced by the person or entity that is responsible for the implementation of the requirement/control being evaluated or measured. [HITRUST]

Indirect Treatment Relationship	A relationship between an individual and a health care provider in which: (1) The health care provider delivers health care to the individual based on the orders of another health care provider; and (2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual. [HHS HAS]
Individually Identifiable Health Information	Information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. [HHS HAS]
Industrial Control System (ICS)	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 (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. [NIST IR 7298 r2]
Information	Any communication or reception of knowledge, such as facts, data or opinions, including numerical, graphic or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform or magnetic tape. [NIST IR 7298 r2, adapted]
Information Assets	See Asset. [HITRUST]
Information Processing Facility	A computer room and/or support area(s) housing equipment provided for the purpose of computing and/or processing an organization’s information asset(s). [ISACA, adapted]
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability through security controls. [NIST IR 7298 r2, adapted]
Information Security Continuous Monitoring (ISCM)	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. (Note: The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.) [NIST IR 7298 r2]
Information Security Management Program (ISMP)	See Information Security Program. [HITRUST]

Information Security Program	The overall combination of technical, operational and procedural measures and management structures implemented to provide for the confidentiality, integrity, and availability of information based on business requirements and risk analysis. [ISACA]
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. [NIST IR 7298 r2, adapted]
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST IR 7298 r2]
Information System-Related Security Risk	Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, and other organizations. A subset of Information Security Risk. [NIST IR 7298 r2, adapted]
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which—1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. See Information System. [NIST IR 7298 r2]
Inheritance	See Security Control Inheritance. [HITRUST]
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. [NIST IR 7298 r2]
Key Performance Indicator (KPI)	A metric that is used to help manage an IT service, process, plan, project or other activity. Key performance indicators are used to measure the achievement of critical success factors. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service or activity. They should be selected to ensure that efficiency, effectiveness and cost-effectiveness are all managed. [ITIL]
Leading Practice	See Best Practice. [HITRUST]
Least Privilege	Having the minimum access and/or privileges necessary to perform the roles and responsibilities of the job function. [PCI DSS]

Legacy System Data	Data stored in outdated formats or systems that is difficult to access or process using modern computing protocols. [HITRUST]
Likelihood of Occurrence	In risk analysis, a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. [NIST IR 7298 r2, adapted]
Limited Data Set	A data set with fewer identifiers deleted than a “HIPAA safe harbor” de-identified data set. The Limited Data Set allows the inclusion of all dates, 5-digit ZIP codes, and city as indirect identifiers. A limited data set can only be used for research, public health, or operations. Its use or disclosure may be further limited by the purpose statements in the Data Use Agreement. HIPAA defined sixteen identifiers that must be deleted in order for the information to be considered a limited data set. [HITRUST]
Local Access	Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. [NIST IR 7298 r2]
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. [NIST IR 7298 r2]
Malware	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. A virus, worm, Trojan horse, or other code-based malicious entity that infects a host. Ransomware, spyware, and some forms of adware are also examples of malware. [NIST IR 7298 R2, adapted]
Marketing	Means to make a communication about a product or service, a purpose of which is, to encourage recipients of the communication to purchase or use the product or service. [HITRUST]
Measure	A standard used to evaluate and communicate performance against expected results. Measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction. Reporting and monitoring measures help an organization gauge progress toward effective implementation of strategy. [ISACA, adapted]
Media	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, USB storage devices, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. [NIST IR 7298 r2, adapted]
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. [NIST IR 7298 r2]

Medical Device	An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory, which: (i) is (a) recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them; (b) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or (c) intended to affect the structure or any function of the body of man or other animals; and (ii) does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals; and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes. [FDA, adapted]
Metric	A quantifiable entity that allows the measurement of the achievement of a process goal. Metrics should be SMART—specific, measurable, actionable, relevant, and timely. Complete metric guidance defines the unit used, measurement frequency, ideal target value (if appropriate) and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment. [ISACA]
Minimum Necessary	Standard requiring that when PII or PHI is used or disclosed, only the information that is needed for the immediate use or disclosure should be made available. For PHI, this standard does not apply to uses and disclosures for treatment purposes (so as not to interfere with treatment) or to uses and disclosures that an individual has authorized, among other limited exceptions. [HITRUST]
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. [NIST IR 7298 r2]

Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers. [NIST] A computing and communication device that allows for portability (can operate without the use of an external power supply) and has the capability to store and process information, such as notebook/laptop computers, personal digital assistants, smart phones, tablets, digital cameras, and other Wi-Fi-enabled devices, etc. Mobile devices do not include portable storage devices (e.g., thumb/flash drives, external/removable hard disk drives, etc.) [HITRUST]
Monitoring	The act of observing, supervising, reporting, or controlling the activities of another entity. [HITRUST]
Multi-Factor Authentication	Authentication using two or more factors to verify the identity of a user, system, or process. Factors include (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Two-Factor Authentication. [NIST IR 7298 r2, adapted]
Need-to-know	Primarily associated with organizations that assign clearance levels to all users and classification levels to all assets; restricts users with the same clearance level from sharing information unless they are working on the same effort. Entails compartmentalization. [(ISC)²]
Non-conformance	Deviation from a standard or other requirement. [HITRUST]
Non-Organizational Asset	An information asset that is not owned and/or managed by the organization (e.g., personally-owned smartphone). [HITRUST]
Non-Organizational User	Any individual who is not under the direct supervisory control of the organization (e.g., service provider) to whom direct access to company-controlled resources is provided. [HITRUST]
Non-repudiation	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. [NIST IR 7298 r2] A transactional property that prevents a participant in an action or process from later denying participation in the act. [HITRUST]
Online Transaction	A transaction that takes place over a computer network or telecommunications system (e.g., the Internet). See Transaction. [HITRUST]

Operating Effectiveness	The degrees to which a security control is operating as designed and to which the individual implementing the control possesses the necessary authority and competence to implement the control as intended. [PCAOB, derived from discussion on Testing Operating Effectiveness]
Operational	With respect to a measure or metric, one that is produced by, or otherwise influenced by, the person or entity responsible for the requirement/control being tracked by the measure or metric. [HITRUST]
Operational Control	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). [NIST]
Opt-in	One of two central concepts of choice/consent. It means an individual makes an active affirmative indication of choice; i.e., checking a box signaling a desire to share his or her information with third parties. [IAPP]
Opt-out	One of two central concepts of choice/consent. It means that an individual's lack of action implies that a choice has been made; i.e., unless an individual checks or unchecks a box, his or her information will be shared with third parties. [IAPP]
Organizational User	An individual who is under the direct supervisory control of the organization (e.g., employee or supplemental staff), or any other individual who the organization deems to have equivalent status of an employee (e.g., staff augmentation) to whom direct access to company-controlled resources is provided. [NIST SP 800-53 r4, adapted]
Organized Health Care Arrangement	A clinically-integrated care setting in which individuals typically receive health care from more than one health care provider. An organized system of health care in which more than one covered entity participates and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement (and participate in joint activities), or a combination of a group health plans or group health plans and insurers. [HHS HAS, adapted.]
Overlay	A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. [NIST SP 800-53 r4]
Patch Management	An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk. [ISACA]
Penetration Test	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers. [ISACA]

Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [EU GDPR]
Personal Health Record (PHR)	In general, a PHR is an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in his or her own health care. [HHS PHR]
Personal Identifying Information (PII)	Any data that could potentially identify a specific individual, including (i) any piece of information or combination of information that, together , 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 (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. See Personal Data. [NIST, adapted]
Plan of Action and Milestones (POA&M)	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. See Corrective Action Plan. [NIST IR 7298 r2]
Plan, Do, Check, Act (PDCA) Cycle	An iterative four-step management method used in business for the control and continuous improvement of processes and products; also known as the Deming wheel or the Shewhart Cycle. [HITRUST]
Policy	Overall intention and direction as formally expressed by management, most often articulated in documents that record high-level principles or courses of action that have been decided on; the intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives, and strategic plans established by the enterprise's management teams. Policies may provide guidance on specific issues or systems, but should not be confused with standards or procedures. [ISACA, adapted]
Portable Media	Media that are designed and/or capable of being easily and routinely moved from one location to another (e.g., USB drives, memory cards, CDs/DVDs). See Media. [HITRUST]
Priority	A category used to identify the relative importance of an incident, problem or change. Priority is based on impact and urgency and is used to identify required times for actions to be taken. [ITIL]
Privacy Notice	A document that explains an organization's privacy practices, how information about the individual may be shared, the individual's rights, and the organization's legal duties. Also known as Notice of Privacy Practices. [HHS HAS, derived from discussion]

Privacy Officer	A person designated by an organization to develop, implement, and oversee the organization's compliance with applicable privacy laws, and acts as the point of contact for all patient privacy issues. [HHS HAS, derived from discussion]
Privacy Rule	The Standards for Privacy of Individually Identifiable Health Information set forth at 45 CFR Parts 160 & 164 of HIPAA. [HHS PR]
Private Network	A telecommunications network designed and operated to convey traffic between systems and users who share a common purpose (e.g., branches of a company or individual school campuses). Private networks are established for many purposes, such as reducing telecommunications cost, ensuring transmission security, and providing a level of functionality specific to those users. [HITRUST]
Privileged Access	Access to security-relevant functions, such as system control, monitoring, or administration functions. [NIST IR 7298 r2, derived from Privileged User]
Privileged User	A user that is authorized (and, therefore, trusted) to perform specific functions that ordinary users are not authorized to perform. See Privileged Access. [NIST IR 7298 r2, adapted]
Procedure	Systematic method of implementing policies and standards. [HITRUST]
Process	A logically related series of activities conducted toward a defined objective. [HITRUST]
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. [EU GDPR]
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. [EU GDPR]
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. [EU GDPR]
Program Source Code	Code that is compiled (and linked) to create executables. [HITRUST]

Protected Health Information (PHI)	Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral. PHI is information, including demographic information that relates to: (i) the individual's past, present, or future physical or mental health or condition; (ii) the provision of health care to the individual; or (iii) the past, present, or future payment for the provision of health care to the individual; and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security number) when they can be associated with the health information listed above. [HHS PR, adapted]
Protected Information	See Covered Information. [HITRUST]
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. See De-identification. [EU GDPR]
Public Area	A physical area that may be freely accessed by anyone (e.g., a lobby or hospital emergency room). [HITRUST]
Public Network	A network that can be freely accessed by anyone (e.g., the Internet). [HITRUST]
Publicly Positioned	Refers to the intentional physical placement of a system such that it is accessible by non-organizational personnel. [HITRUST, derived from discussion]
Qualitative Assessment	Use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels. [NIST IR 7298 r2]
Quality	The extent to which a service fulfills the requirements and expectations of the customer. [HITRUST]
Quality Assurance	The complete set of measures and procedures used by the organization to ensure that the services provided continue to fulfill the expectations of the customer as described in relevant agreements. [HITRUST]
Quality Control	Measures and procedures to ensure that services are predictable and reliable. [HITRUST]
Quantitative Assessment	Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment. [NIST IR 7298 r2]
Quasi-Quantitative Assessment	See Semi-Quantitative Assessment. [HITRUST]

Recipient	A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry shall not be regarded as recipients; the processing of the data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. [EU GDPR, adapted]
Records	Any item, collection, or grouping of sensitive information (e.g., PII, ePHI, payment card data) that is maintained, collected, used, or disseminated by or for a public or private entity. [HHS HAS, adapted]
Recovery	The phase in the incident response plan that ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDOs) or business continuity plan (BCP). [ISACA]
Recovery Point Objective (RPO)	The point in time to which data must be recovered after an outage. [NIST IR 7298 r2]
Recovery Time Objective (RTO)	The targeted duration of time and level of service to which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. [HITRUST] 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 functions. [NIST IR 7298 r2]
Reliability	The ability to produce consistent results under similar conditions. [HITRUST]
Remote Access	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). [NIST IR 7298 r2, adapted]
Remote Maintenance	Maintenance activities conducted by authorized individuals communicating through an external, non-organization-controlled network (e.g., the Internet). [NIST IR 7298 r2, adapted]
Removable Media	Portable electronic media with no independent processing capabilities, that are used to store information and can be inserted into and removed from a computing device (e.g., USB drives, floppy disks, and CDs/DVDs). See Media. [NIST IR 7298 r2, adapted]
Repeatability	The ability to produce consistent results over repeated trials, such as a measurement or set of measurements taken by a single instrument or person under similar conditions. Also known as Test-Retest Reliability. [HITRUST]

Replay Attack	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. [NIST IR 7298 r2]
Replay-resistant Authentication	Authentication methods that are resistant to a replay attack. See Replay Attack. [HITRUST]
Representative	A natural or legal person, designated by the controller or processor, who represents the controller or processor with regard to their respective obligations. [EU GDPR, adapted]
Reproducibility	The ability to duplicate something with the same results, either by the same individual or another individual working independently. [HITRUST]
Required by Law	A mandate contained in law that compels an entity to make a use or disclosure of protected heath information and that is enforceable in a court of law. [HHS HAS]
Residual Risk	Portion of risk remaining after data protection measures have been applied. [NIST IR 7298 r2, adapted]
Restricted Area	A controlled area within an organization with the highest level of restrictiveness and security (e.g., a data center with multiple layers of security). [HITRUST]
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST IR 7298 r2, adapted]
Risk Analysis	Examination of information to identify the risk to an information asset. See Risk Assessment. [NIST IR 7298 r2, adapted]
Risk Assessment	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and/or reputation), organizational assets, individuals, and other organizations. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by privacy and security controls planned or in place. See with Risk Analysis. [NIST IR 7298 r2, adapted]
Risk Evaluation	The process of comparing the estimated risk against given risk criteria to determine the significance of the risk. [ISACA]
Risk Factor	A characteristic in a risk model used as an input for determining the level of risk in a risk assessment. [HITRUST]

Risk Management	The program and supporting processes to manage information protection risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, 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. [NIST IR 7298 r2, adapted]
Risk Management Framework (RMF)	A common taxonomy and standard set of processes, procedures, activities, and tools that support the identification, assessment, response, control, and reporting of risk. [HITRUST]
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. A subset of Risk Response. [NIST IR 7298 r2, adapted]
Risk Model	A key component of a risk assessment methodology (in addition to the assessment approach and analysis approach) that defines key terms and assessable risk factors. [NIST IR 7298 r2]
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. (Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.) [NIST IR 7298 r2]
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, or other organizations. See Course of Action and Risk Treatment. [NIST IR 7298 r2, adapted]
Risk Treatment	The process of selection and implementation of measures to modify risk. See Risk Response. [ISACA]
Role-Based Access Control (RBAC)	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. [NIST IR 7298 r2]
Root Cause Analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks. [NIST IR 7298 r2]
Rubric	A scoring guide used to evaluate the quality or effectiveness of a HITRUST CSF control requirement's implementation. [HITRUST]
Safeguards	Protective measures prescribed to meet the privacy (e.g., data quality, transparency of use of personal data) and security (e.g., confidentiality, integrity, and availability) requirements specified for an information system. Safeguards may include privacy and security features, management constraints, personal data minimization, use limitations for personal data, personnel security, and security of physical structures, areas, and devices. [NIST IR 7298 r2, adapted]

Scaling	The act of applying the considerations necessary to select a specific control baseline in control frameworks with multiple baselines. A part of scoping. [NIST SP 800-53 r4, derived from the discussion on Tailoring]
Scoping	The act of applying specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security and privacy controls in the control baseline. Scoping considerations are considered a part of tailoring guidance. [NIST IR 7298 r2, derived from Scoping Guidance]
Secure Coding Guidelines	The general rule, principle, or advisement on creating and implementing applications that are resistant to tampering and/or compromise. [PCI DSS, derived from Secure Coding]
Security Awareness	The extent to which every member of an enterprise and every other individual who potentially has access to the enterprise's information understand (i) security and the levels of security appropriate to the enterprise; (ii) the importance of security and the consequences of a lack of security; and (iii) their individual responsibilities regarding security (and act accordingly). [ISACA, adapted]
Security Awareness Campaign	A predefined, organized number of actions aimed at improving the security awareness of a special target audience about a specific security problem. Each security awareness program consists of a number of security awareness campaigns. Sometimes referred to as Security Awareness Training. [ISACA, adapted]
Security Awareness Program	A clearly and formally defined plan, structured approach, and set of related activities and procedures with the objective of realizing and maintaining a security-aware culture, and generally consisting of a number of security awareness campaigns. [ISACA, adapted]
Security Categorizations	The process of determining the security category for information or an information system. See Security Category. [NIST IR 7298 r2]
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. [NIST IR 7298 r2]
Security Control	The safeguard or countermeasure prescribed for an organization and/or information system(s) to protect the confidentiality, integrity, and availability of information. [NIST IR 7298 r2, adapted]
Security Control Assessment	Testing and/or evaluation of security controls to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. [NIST IR 7298 r2, adapted]

Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment. [NIST IR 7298 r2]
Security Control Baseline	A set of information security controls that has been established through information security strategic planning activities to address one or more specified security categorizations; this set of security controls is intended to be the initial security control set selected for a specific system once that system's security categorization is determined. [NIST]
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See Common Control. [NIST IR 7298 r2]
Security Event	An observable occurrence within a system, service, or network indicating potential impact to the security of such. [NIST IR 7298 r2, derived from Event]
Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. [NIST IR 7298 r2]
Security Incidents	See Incident. [HITRUST]
Security Official	A designated individual who is responsible for developing and implementing security policies and procedures. [HHS HAS, derived from discussion]
Security Rule	The requirement of appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. [HHS SR, adapted]
Segregation/Separation of Duties (SOD)	A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets, and is commonly used so that no single person is in a position to introduce fraudulent or malicious code without detection. [ISACA, adapted]
Self-Assessment	An evaluation against an objective or standard conducted by an entity without a requisite degree of independence. See Independent. [HITRUST]
Semi-Quantitative Assessment	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. [DHS RL, adapted]
Sender Policy Framework (SPF)	An open standard specifying a technical method to prevent sender address forgery. [SPF]

Sensitive Area	A controlled area within an organization with a medium level of restrictiveness and security (e.g., a wiring closet requiring prior authorization and a badge to access). [HITRUST]
Sensitive Information	See Covered Information. [HITRUST]
Service Level	Measured and reported achievement against one or more service level targets. The term is sometimes used informally to mean service level target. [ITIL]
Service Level Agreements (SLA)	An agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers. [ITIL]
Service Level Target	A commitment that is documented in a service level agreement. Service level targets are based on service level requirements, and are needed to ensure that the IT service is able to meet business objectives. They should be SMART—specific, measurable, achievable, relevant, and timely; and are usually based on key performance indicators. [ITIL, adapted]
Service Provider	An organization supplying services to one or more internal customers or external customers. Service provider is often used as an abbreviation for IT service provider. [ITIL]
Significant Change	The removal or addition of new or upgraded hardware, software, or firmware in the information system or a change in the operational environment, which could potentially degrade the security state of the system. [HITRUST]
Site Security Survey	A review of a facility's security requirements and implemented controls, which is intended to identify and remediate any shortcomings/gaps. [HITRUST]
Smart Card	A credit card-sized card with embedded integrated circuits that can store, process, and communicate information. [NIST IR 7298 r2]
Spam	Unsolicited bulk commercial email messages. [NIST IR 7298 r2]
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge. [NIST IR 7298 r2]
Status Monitoring	Monitoring information security metrics in accordance with the organization's continuous monitoring strategy. [NIST IR 7298 r2, adapted]
Strong Cryptography	Cryptography based on industry-tested and accepted algorithms. [PCI DSS]
Subject of Care	Synonymous with "patient." [HITRUST]
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions. [NIST IR 7298 r2]

Supervisory Authority	An independent public authority that is established by a Member State pursuant to Article 51 of the European Union's General Data Protection Regulation. [EU GDPR, adapted]
Supervisory Control and Data Acquisition (SCADA)	Networks or systems generally used for industrial controls or to manage infrastructure such as pipelines and power systems. [NIST IR 7298 r2]
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See Tailoring. [NIST IR 7298 r2]
Tailoring	The process by which security control baselines are modified by: (i) identifying and designating common controls; (ii) applying scoping considerations on the applicability and implementation of baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to organization-defined security control parameters; (v) supplementing baselines with additional security controls or control enhancements; and (vi) providing additional specification information for control implementation. [NIST SP 800-53 r4]
Technical Controls	The data protection controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [NIST IR 7298 r2]
Telework	The act of conducting work from locations other than the organization's facilities. [NIST, adapted]
Third-Party	A legal entity (individual or company) that is separate and independent from the organization to which the entity is providing service (employing company), that has been authorized for physical and/or logical access to facilities, systems, networks, and data not otherwise under the employing organization's direct control (e.g., business partners, vendors, cloud providers). [HITRUST]
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NIST IR 7298 r2, adapted]
Threat Analysis	The examination of threat sources against vulnerabilities to determine the threats for a particular operational environment. [NIST IR 7298 r2, adapted]
Threat Assessment	Process of formally evaluating the degree of threat to information or the enterprise and describing the nature of the threat. [NIST IR 7298 r2, adapted]
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact. [NIST IR 7298 r2]
Threat Scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. [NIST IR 7298 r2]

Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. [NIST]
Trading Partner	External entity with which business is conducted (e.g., customer). This relationship can be formalized via a trading partner agreement. (Note: a trading partner of an entity for some purposes may be a business associate of that same entity for other purposes.) [HITRUST]
Transaction	A discrete event between a user and a system (including, but not limited to, an online or e-commerce exchange) that supports a business or programmatic purpose, and contains various degrees of exposure (i.e., occurring within a single system, a single network, or externally between two or more separate systems) to which risk is evaluated upon. [NIST, adapted]
Trust Anchor	A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor's public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates. [NIST IR 7298 r2]
Two-Factor Authentication	A type of multi-factor authentication in which only two factors are used. [HITRUST]
Undocumented	A well-understood and consistently-observed policy, procedure, or process that is not supported by written documentation or proof. [HITRUST]
Unsecured Protected Health Information	Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. [HHS HAS]
Urgency	A measure of how long it will be until an incident, problem or change has a significant impact on the business. For example, a high-impact incident may have low urgency if the impact will not affect the business until the end of the financial year. Impact and urgency are used to assign priority. [ITIL]
User	Individual or (system) process authorized to access an information system. [NIST IR 7298 r2]
Validated Assessment	An evaluation conducted against the HITRUST CSF under the CSF Assurance Program, in which the results are (i) checked for accuracy and completeness by a HITRUST Approved Assessor organization; and (ii) undergo a quality assurance review by HITRUST. [HITRUST]
Version	A version is used to identify a specific baseline of a configuration item. Versions typically use a naming convention that enables the sequence or date of each baseline to be identified. For example, payroll application version 3 contains updated functionality from version 2. [ITIL]

Vulnerability	Weakness in an information system, system privacy or security procedures, internal controls, or implementation that could be exploited by a threat source. [NIST IR 7298 r2]
Vulnerability Analysis	See Vulnerability Assessment. [NIST IR 7298 r2]
Vulnerability Assessment	Systematic examination of an information system or product (including its hardware, software, and firmware) to determine the adequacy of privacy and security measures, identify privacy risks and security deficiencies, provide data from which to predict the effectiveness of proposed privacy and security measures, and confirm the adequacy of such measures after implementation. [NIST IR 7298 r2, adapted]
Whole Disk Encryption	See Full Disk Encryption. [HITRUST]
Workforce	Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for an organization, is under the direct control of such organization, whether or not they are paid by the organization. [HHS HAS, adapted]

List of Acronyms

ACL	Access Control List
AES	Advanced Encryption Standard
AICPA	American Institute of Certified Public Accountants
APT	Advanced Persistent Threat
BA	Business Associate
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
CAP	Corrective Action Plan
CCM	Cloud Control Matrix
CE	Covered Entity
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Protection Advisory Council
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMS	Centers for Medicaid and Medicare Services
CMS IS ARS	CMS Information Security Acceptable Risk Safeguards
CNSS	Committee for National Security Systems
CNSSI	CNSS Instruction
CPO	Chief Privacy Officer
CRR	Critical Resilience Review
CSA	Cloud Security Alliance
CVSS	Common Vulnerability Scoring System
DCS	Distributed Control System

DHS	U.S. Department of Homeland Security
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	DNS Security
DoS/DDoS	Denial-of-Service/Distributed Denial-of-Service
DRP	Disaster Recovery Plan
EA	External Assessor
EHNAC	Electronic Healthcare Network Accreditation Commission
EHR	Electronic Health Record
ePHI	Electronic Protected Health Information
ETAP	Education, Training and Awareness Program
EU	European Union
FC	Fully Compliant
FDA	Food and Drug Administration
FDE	Full Disk Encryption
FedRAMP	Federal Risk and Authorization Management Program
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTI	Federal Tax Information
GDPR	General Data Protection Act
HHS	U.S. Department of Health and Human Services
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
HIX	Health Insurance Exchange
IA	Internal Assessor
ICS	Industrial Control System
IEC	International Electrotechnical Commission

InfoSec	Information Security
IP	Internet Protocol
IP	Intellectual Property
IPSEC	IP Security
IRS	Internal Revenue Service
IRT	Incident Response Team
IS	Information System
ISCM	Information Security Continuous Monitoring
ISMP	Information Security Management Program
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MC	Mostly Compliant
NC	Non-Compliant
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NISTIR (or NIST IR)	NIST Interagency Report
OCR	Office of Civil Right
OS	Operating System
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan, Do, Check, Act Cycle
PHI	Protected Health Information
PHR	Personal Health Record
PIA	Privacy Impact Assessments
PII	Personal (or Personally) Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones

PRISMA	Program Review for Information Security Management Assistance
RBAC	Role-based Access Control
RMF	Risk Management Framework
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
SANS	SysAdmin, Audit, Network and Security (ref: SANS Institute)
SC	Somewhat Compliant
SCADA	Supervisory Control and Data Acquisition System
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SMART	Specific, Measurable, Achievable, Relevant and Time-bound
SOD	Segregation/separation of Duties
SOW	Statement of Work
SPF	Sender Policy Framework
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TPO	Treatment, Payment and Operations
VPN	Virtual Private Network
XSS	Cross-Site Scripting

Reference List

AXELOS Limited. (2011). ITIL® Glossary and Abbreviations (ITIL). Retrieved from https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_GB-v1-0.pdf.

Department of Health and Human Services. (n.d.). Personal Health Records and the HIPAA Privacy Rule (HHS PHR). Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

Department of Health and Human Services. (2003). Summary of the HIPAA Privacy Rule (HHS PR). Retrieved from https://www.hhs.gov/sites/default/files/privacysummary.pdf.

Department of Health and Human Services. (2017). The Security Rule (HHS SR). Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/index.html.

Department of Health and Human Services, Centers for Medicare & Medicaid Services. (2016). Framework for the Independent Assessment of Security and Privacy Controls (CMS Assessment). Retrieved from http://mn.gov/buyit/14atm/rfo/RFO0131A1.pdf.

Department of Health and Human Services, Office for Civil Rights. (2013). HIPAA Administrative Simplification (HHS HAS). Retrieved from https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

Department of Homeland Security. (2010). DHS Risk Lexicon, 2010 Edition (DHS RL). Retrieved from https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf.

Department of Labor. (n.d.). Health Plans and Benefits (DOL). Retrieved from https://www.dol.gov/general/topic/health-plans.

European Parliament and the Council of the European Union. (2016). Official Journal of the European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (EU GDPR). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

Food and Drug Administration. (2018). Is the Product a Medical Device? (FDA). Retrieved from https://www.fda.gov/medical-devices/classify-your-medical-device/product-medical-device.

International Association of Privacy Professionals. (2012). Glossary of Privacy Terms (IAPP). Retrieved from https://iapp.org/media/pdf/resource_center/IAPP_Privacy_Certification_Glossary_v2.0.0.2.pdf.

International Information System Security Certification Consortium (ISC)2. (n.d.). CISSP Glossary - Student Guide (ISC)2. Retrieved from https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary.

ISACA. (n.d.). Glossary (ISACA). Retrieved from https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf.

Medscape Education. (2014). Introduction to Health Information Exchange (Medscape). Retrieved from https://www.medscape.org/viewarticle/829539_2.

Merriam-Webster. (n.d.). Dictionary (Merriam-Webster). Retrieved from https://www.merriam-webster.com/.

National Institute of Standards and Technology. (n.d.). Glossary (NIST). Retrieved from https://csrc.nist.gov/Glossary.

National Institute of Standards and Technology. (2013). Glossary of Key Information Security Terms (NIST IR 7298 r2). Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

National Institute of Standards and Technology. (2015). Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82 r2). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

National Institute of Standards and Technology. (2013). Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 r4). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

National Institute of Standards and Technology. (2016). User's Guide to Telework and Bring Your Own Device (BYOD) Security (NIST SP 800-114 r1). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf.

New York State Department of Financial Services. (2017). Cybersecurity Requirements for Financial Services Companies (NYSDFS CS). Retrieved from https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

Palo Alto Networks. (n.d.). What is a denial of service attack (DoS)? (Palo Alto Networks). Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

Public Company Accounting Oversight Board. (2016). Auditing Standard No. 13: The Auditor's Responses to the Risks of Material Misstatement (PCAOB). Retrieved from https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/Auditing_Standard_13.aspx.

Security Standards Council. (2016). Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS): Glossary of Terms, Abbreviations, and Acronyms, Version 3.2 (PCI DSS). Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf.

The Sender Policy Framework Project. (2010). Sender Policy Framework Introduction (SPF). Retrieved from https://web.archive.org/web/20190222070146/http://www.openspf.org/Introduction (Archive of http://www.openspf.org/Introduction–no longer active).

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net