Glossary of Terms and Acronyms

Version 11.3.0

HITRUST

APRIL 2024

Table of Contents

Reader's Cautionary Notes

This publication contains material from HITRUST and other authoritative sources, e.g., ITIL®, and may be subject to multiple copyrights. The source is included within each term definition and is indicated in brackets as [source abbreviation]. The specific citation and full name of the source is cited in the Reference List. Source definitions are used verbatim, unless noted otherwise; grammar and usage may vary.

Some definitions have been altered slightly to make them generally applicable, such as language removed from a NIST definition that is particular to the U.S. Government or otherwise modified to accommodate the HITRUST Risk Management Framework (RMF). Such definitions are indicated by the word "*adapted*" after the source abbreviation. Definitions obtained from a discussion of the term, rather than a glossary, or developed from a similar term (or multiple terms) in a glossary are indicated by the word "*derived*" after the source abbreviation.

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 HITRUST 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 HITRUST Assurance Program.
5.0	Jun 2020	HITRUST	Expanded and updated based on a review of version 9.4 of the HITRUST CSF.
5.1	Jan 2021	HITRUST	Updated definition for Health Information Exchange Updated URL for Department of Homeland Security. (2010). DHS Risk Lexicon, 2010 Edition (DHS RL)
5.2	Dec 2021	HITRUST	Expanded and updated based on a review of version 9.5.2 of the HITRUST CSF.
11.0	Jan 2023	HITRUST	Expanded and updated content based on version 11.0.0 of the HITRUST CSF. Updated to current versions of authoritative source references. Updated Glossary version number to align with HITRUST CSF version.
11.2.0	Oct 2023	HITRUST	Expanded and updated content based on version 11.2.0 of the HITRUST CSF. Minor updates to several existing definitions. Updated Glossary version number to align with HITRUST CSF version.
11.3.0	April 2024	HITRUST	Expanded and updated content based on version 11.3.0 of the HITRUST CSF. Updated Glossary version number to align with HITRUST CSF version.

List of Terms

Term	Definition
Acceptable Risk	The level of risk that has been determined to be a reasonable level of potential loss/disruption for a specific IT system. [NIST SP 800-16, adapted]
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 SP 800-12 Rev. 1, adapted]
Access Control List	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. Also referred to as ACL. [NISTIR 5153, derived]
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 SP 800-12 Rev. 1]
Accounting of Disclosures	A listing of organizations and individuals who have received access to or have been provided with a copy of more than a limited data set of an individual's protected health information under a data use agreement. [HHS, adapted]
Ad Hoc	A security method that ensures users have the minimum, appropriate access level to electronic and physical assets; often undocumented. [HITRUST] Initial level where processes are disorganized and may even be chaotic. Success likely depends on individual efforts and is not considered to be repeatable. This is because processes are not sufficiently defined and documented to enable them to be replicated consistently. [CMU/SEI-93-TR-024, adapted]
Adequate Security	Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [NIST SP 800-30 Rev. 1]

Term	Definition
Agent	Under HIPAA, in relation to group health plans, means a trained insurance professional who can help individuals enroll in a health insurance plan, who must be licensed in their states, and who must have signed agreements to sell Marketplace health plans. Under Ontario PHIPA, in relation to a health information custodian means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated. [PHIPA]
AI System	An engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy. [NIST AI RMF]
Alternate Control	A compensating control that has been submitted and approved for general use by the HITRUST Alternate Controls Committee. See Compensating Security Control. [HITRUST]
Anti-Malware	Software products and technology used to block / contain / quarantine malicious code to prevent a system infection or to remove the malicious code if a system infection has been detected. [NIST SP 800-82 Rev. 2]
Application	A software program hosted by an information system. [NIST SP 800-53 Rev. 5]
Architecture	Description of the fundamental underlying design of the components of the business system or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives. [ISACA, adapted]
Assessment Plan	Set of objectives and associated detailed roadmap of how to conduct security and privacy control assessments, including– a) controls and control enhancements under assessment; b) assessment procedures to be used to determine control effectiveness; and c) assessment environment, assessment team, and assessment roles and responsibilities. [NIST SP 800-53 Rev. 5, adapted]
Assessment Procedure	Set of assessment objectives and an associated set of assessment methods and assessment objects. [NIST SP 800-53A Rev. 4]
Assessor	An individual or organization that conducts control assessments, including HITRUST Authorized Assessors, self-assessors, or independent assessors (e.g., internal/external auditors or third-party assessors). [HITRUST]
Asset	The data and information, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. [NISTIR 8286, adapted]
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 SP 800-60 Vol. 1 Rev. 1, derived from Information System Owner]

Term	Definition
Assurance	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. [NIST SP 800-39]
Attack	Any kind of malicious activity that attempts to observe, surveil, collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [NIST SP 800-12 Rev. 1, adapted]
Attack Vector	Attack can be either inbound/ingress or egress (i.e., data exfiltration), and a successful attack often requires the use of multiple vectors. [ISACA, adapted]
Attest	To affirm to be true or genuine; to authenticate officially. [Merriam-Webster]
Attributes	A characteristic or property of an entity that can be used to describe its state, appearance, or other aspect [NISTIR 8053] A distinct characteristic of an object often specified in terms of their physical traits, such as size, shape, weight, and color, etc., for real -world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address, etc. [NIST SP 800-95]
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. [NIST SP 800-12 Rev.1]
Audit Log	A chronological record of system activities, including records of system accesses and operations performed in a given period. [NIST SP 800-53 Rev. 5]
Audit Trail	Chronological record that traces the sequence of activities surrounding or leading to a specific operation, procedure, or event in security-relevant information involved in a transaction from inception to result, that which, enables examination and reconstruction of activities for the purpose of security incident investigation or forensic artifact preservation and analysis. [NISTIR 7316, derived]
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. [NIST SP 800-53 Rev. 5]
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. [NIST SP 800-37 Rev. 2]
Authoritative Source	A source of data or information that is recognized by members of a large community of interest to be valid or trusted because it is considered to be highly reliable or accurate or is from an official regulation, wherein a set of governing requirements are extracted and applied to comply with or evaluate against. [DoDD 8320.2, adapted]

Term	Definition
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges. [NIST SP 800-53 Rev. 5]
Authorized Access List	Access list used to facilitate the entry of employees, vendors, contractors, and non-agency personnel who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area. [IRS Pub. 1075, 2.B.3.2 Authorized Access List, adapted]
Automated Controls	Controls that have been programmed, configured, and/or embedded within a system. [ISACA]
Availability	Ensuring timely and reliable access to and use of information. [NIST SP 800-53 Rev. 5]
Banner	Display on an information system that sets parameters for system or data use. [CNSSI 4009-2015]
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. [IAPP, 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 data. [IAPP, EU GDPR] See also Natural Person. [HITRUST]
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels). [CNSSI 4009-2015]
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, adapted]
Bring Your Own Device	Use of employees' own personal computing devices for work purposes. Also referred to as BYOD. [IAPP, adapted]
Business Associate	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, adapted]

Term	Definition
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	The documentation of a predetermined set of instructions or procedures that describe how an organization’s mission/business processes will be sustained during and after a significant disruption. [NIST SP 800-34 Rev. 1]
Business Impact Analysis	An analysis of an information system’s requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. [NIST SP 800-34 Rev. 1]
Business Process	An inter-related set of cross-functional activities or events that result in the delivery of a specific product or service to a customer. [ISACA]
Capability	An aptitude, competency or resource that an enterprise may possess or require at an enterprise, business function or individual level that has the potential, or is required, to contribute to a business outcome and to create value. [ISACA]
Care	The process of protecting someone or something and providing what that person or thing needs. [Cambridge Dictionary]
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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. [FIPS 200]
Chain Of Custody	Legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. [ISACA]
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, adapted]
Checklist	A list of items that is used to verify the completeness of a task or goal; as used in quality assurance (and in general, in information systems assessment or audit), to check for compliance with laws, regulations, standards, or other types of requirements. [ISACA, adapted]

Term	Definition
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, adapted]
Clear Desk	An unattended workspace free of confidential or customer information, and if drawers and file cabinets are present, they are locked. [HITRUST]
Cloud Computing	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. [CNSSI 4009-2015, adapted]
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. [NIST SP 800-137]
Communications	The actions and associated activities that are used to exchange information, provide instructions, give details, etc. Communications refers to the full range of activities involved with providing information to support the secure use of IoT devices. Communications include using such tools as phone calls, emails, user guides, in-person classes, instruction manuals, webinars, written instructions, videos, quizzes, frequently asked questions (FAQ) documents, and any other type of tool for such information exchanges. Communication protocols can include FTP, SMTP, TLS, SSL, TELNET, etc. [NISTIR 8259B, adapted]
Compensating Security Control	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. [NIST SP 800-30 Rev. 1]
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive data (e.g., keys, metadata, or other security-related information) or the unauthorized modification of a security-related system, device or process in order to gain unauthorized access. [NIST SP 800-52]
Confidential Information	Information that is not to be disclosed to unauthorized persons, processes, or devices. [NISTIR 7316, adapted from Confidentiality]
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST SP 800-30 Rev. 1]
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, adapted]

Term	Definition
Configuration Baseline	Standard or starting point of reference (benchmark), by which a set of specifications for a system, or a configuration item within a system, which has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control process. [NIST SP 800-53 Rev. 5, adapted]
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 use or disclosure. Consent may be affirmative, i.e., opt-in; or implied, i.e., the individual didn't opt out. (1) Affirmative/Explicit Consent: A requirement that an individual "signifies" their 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. [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). [HITRUST] Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. [NIST SP 800-137]
Contractor	An individual or company hired to perform work or to provide goods at a certain price or within a certain time. [Merriam-Webster, adapted]
Control Effectiveness	A measure of whether a given control is contributing to the reduction of information security or privacy risk. [NIST SP 800-37 Rev. 2]
Control Enhancement	Augmentation of a control to build in additional, but related, functionality to the control; increase the strength of the control; or add assurance to the control. [NIST SP 800-37 Rev. 2]
Control Objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process. [ISACA]
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 an 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 SP 800-53 Rev. 5]
Controlled Unclassified Information	Information that an organization associated with the executive branch of the US Government creates or possesses, or on their behalf, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination security or privacy controls. [32 CFR 2002, adapted]
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. [IAPP, EU GDPR]

Term	Definition
Corrective Action Plan	Prepared by the assessed entity to describe the specific measures planned to correct control gaps identified during the assessment for validation or certification. Also referred to as a CAP. [HITRUST]
Corrective Control	A control designed to correct errors, omissions and unauthorized uses and intrusions once they are detected. [ISACA, adapted]
Covered Entity	Health plans, health care clearinghouses, or health care providers who transmit health information in electronic form or conduct certain financial and administrative transactions electronically for which standards have been adopted by the Secretary of HHS (e.g., electronic billing, fund transfers). [HHS, 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. [NYCRR]
Covered Information	Any type of information (including data) 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. Sometimes referred to as protected or sensitive information. [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 business impact analysis. See also Business Impact Analysis. [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 SP 800-30 Rev. 1, adapted]
Cryptographic Algorithm	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. [NIST SP 800-57 Rev. 1]
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]
Customer	Organization or person that provides consideration to receive a product or service. [NIST SP 800-160, adapted] Also known as second party. [HITRUST]
Cyber Incident	Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. [NIST SP 800-160 Vol. 2]
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks. [NISTIR 8170]
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]

Term	Definition
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. [IAPP, EU GDPR] A subset of protected health information (PHI) as defined under the Health Insurance Portability and Accountability Act (HIPAA). [HITRUST]
Data Custodian	The individual(s) and department(s) responsible for the storage and safeguarding of computerized data. [ISACA]
Data Governance	Set of processes and management oversight that ensures the utility, quality and integrity, safeguarding and lifecycle of information assets are effectively managed and maintained throughout the organization in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidance. [NIST SP 800-53 Rev. 5, derived]
Data Loss Prevention	A system's ability to identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Also referred to as DLP. [CNSSI-4009:2015]
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 Processor	An individual or organization which processes personal data. [EU GDPR], adapted]
Data Subject	The data subject is the person whose personal data are collected, held, or processed. [EU GPPR, adapted]
Data Tag	A non-hierarchical keyword or term assigned to a piece of information which helps describe an item and allows it to be found or processed automatically. [CNSSI 4009-2015]
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, adapted]
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 subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). [NIST SP 800-30 Rev. 1]
De-identification	The process of anonymizing data so that the risk of re-identifying an individual is minimized to an acceptable level. [HITRUST] General term for any process of removing the association between a set of identifying data and the data subject. [NIST SP 800-53 Rev. 5]
Denial-of-Service	The prevention of authorized access to resources or the delaying of time-critical operations. [NIST 800-12 Rev. 1, adapted]
Denial-of-Service Attack	An attack meant to consume resources or shut down a machine or network, depriving legitimate users of the service or resource they expected. Also referred to as DDoS attack. [Palo Alto Networks, derived from discussion]

Term	Definition
Deny-all, permit-by-exception	Process for systematic enforcement of the policy that prevents, by default, the presence or activation of any items unless otherwise specified “Allow or Permit List(ing)” referenced. [NIST SP 800-94, 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, which 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, but not confidentiality protection. [NIST SP 800-63-3]
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. [CNSSI 4009-2015, derived from Disaster Recovery Plan]
Disaster Recovery Plan	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. [CNSSI 4009-2015]
Disclosure	The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. [HHS, adapted]
Documentation	Information that is written, printed, or in electronic form that serves as evidence for practices, capabilities, procedures, maturity or processes performed by an organization. [ISACA, derived]
Downtime	The amount of time that a service or component is disrupted (not operational). [NIST SP 800-34 Rev. 1, derived from Maximum Tolerable Downtime]
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]
Electronic Commerce	A commercial (buying or selling) transaction conducted through an electronic means (e.g., on the Internet). See Transaction. [HITRUST]
Electronic Health Record	Software that's used to securely document, store, retrieve, share, and analyze information about individual patient care. EHRs are hosted on computers either locally (in the practice office) or remotely. Remote EHR systems are described as “cloud-based” or “internet-based.” [HealthIT.gov]
Electronic Signature	The process of applying any mark in electronic form with the intent to sign a data object. See also Digital Signature. [HITRUST]
Encryption	The process of changing plaintext into ciphertext using a cryptographic algorithm and key. [NIST SP 800-57 Part 2 Rev. 1]
Endpoint	Endpoints are physical/virtual devices that connect to a network system, such as mobile devices, desktop computers, virtual machines, embedded devices, and servers. [HITRUST]
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:

Term	Definition
	acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. [NIST SP 800-30 Rev. 1]
Enterprise Architecture	The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. [NIST SP 800-128]
Entity	An individual (person), organization, asset or process. Used interchangeably with "party". [NIST SP 800-102, adapted]
Entropy	A measure of the amount of uncertainty an attacker faces to determine the value of a secret. Entropy is usually stated in bits. [NIST SP 800-63-3]
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]
Exfiltration	The unauthorized transfer of information from an information system. [NIST SP 800-53 Rev. 5]
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 for unauthorized purposes. [HITRUST]
Exposure	The potential loss to an area of business due to the occurrence of an adverse event. [ISACA, adapted]
External Information System	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. [CNSSI 4009-2015]
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. [CNSSI 4009-2015]
External Parties	Contractors, vendors, business partners, or other persons not directly employed by an organization. [HITRUST]
External Service Provider	A provider of external system services to an organization through a variety of consumer-producer relationships, including joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. [NIST SP 800-53 Rev. 5]
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]

Term	Definition
Federal Tax Information	Covered information that pertains to federal tax returns and return information (and information derived from it) created by the taxpayer, received directly from the Internal Revenue Service (IRS), or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement. Also referred to as FTI. [IRS Publication 1075, adapted]
Foreign National	Those individuals, defined by Section 308 of the Immigration and Nationality Act (INA), which confers U.S. nationality but not U.S. citizenship, on persons born in "an outlying possession of the United States" or born of a parent or parents who are non-citizen nationals who meet certain physical presence or residence requirement. Such individuals may apply for a passport in the United States that would delineate and certify their status as a national but not a citizen of the United States. [U.S. Department of State Bureau of Consular Affairs https://travel.state.gov, derived]
Full Disk Encryption	The encryption of each sector of a disk volume. [NIST SP 800-203]
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	An algorithm that maps or translates one set of bits into another (generally smaller) so that a message yields the same result every time the algorithm is executed using the same message as input. It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm or to find two different messages that produce the same hash result using the same algorithm. [ISACA] A (mathematical) function that maps values from a large (possibly very large) domain into a smaller range. The function satisfies the following properties: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output; 2. (Collision free) It is computationally infeasible to find any two distinct inputs that map to the same output. [NIST SP 800-90A Rev. 1]

Term	Definition
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, adapted]
Health Care 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, adapted]
Health Data Institute	Under PHIPA, an entity that analyzes the management, evaluation, or monitoring of the allocation of resources to or planning for all or part of the health system. [Toronto Metropolitan University, Pressbooks]
Health Information	Any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, 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. [HHS, adapted]
Health Information Custodian	A health care practitioner or a person who operates a group practice of health care practitioners, a health service provider or person or entity that is part of an Ontario Health Team and that provides a home and community care service pursuant to funding under section 21 of the Connecting Care Act, 2019, an evaluator, a medical officer of health of a board of health, any other person who has custody or control of personal health information as a result of or in connection with performing duties, or a person who operates one of the following facilities, programs or services: hospital; long-term care home; retirement home; pharmacy; laboratory or specimen collection center; ambulance service; home for special care; center, program, or service for community health or mental health. [PHIPA, adapted]
Health Information Exchange	Allows health care professionals and patients to appropriately access and securely share a patient's medical information electronically. [HealthIT.gov]

Term	Definition
Health Insurance Portability and Accountability Act	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. Also referred to as HIPAA. [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, adapted]
Healthcare	Care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) 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 (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. [HHS, 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 Authorized Assessor	An organization that has been approved by HITRUST for performing assessments and services associated with the HITRUST Assurance Program and the HITRUST CSF. HITRUST Authorized Assessors are critical to HITRUST 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 Assessment	A data protection assessment provided by an assessor to organizations in accordance with the HITRUST Assurance Program. [HITRUST]
HITRUST Assurance Program	The programs and systems of the HITRUST CSF and related 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 that 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 Assessments; (iii) continually maintains their qualifications by participating in continuing education as HITRUST may reasonably require; and (iv) is available to assist in conducting or supervising HITRUST Assessments. [HITRUST]

Term	Definition
HITRUST CSF Submission	The electronic submission to HITRUST of a file/object containing the results of a HITRUST Assessment, either by the assessed entity as a self-assessment or by a HITRUST Authorized Assessor. [HITRUST]
HITRUST 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 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 CSF 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 HITRUST CSF in some way, either as a simple reference for accepted best practices or as a compliance standard. [HITRUST]
HITRUST CSF 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]
Immutable	Not capable or susceptible to change [Merriam-Webster] Not changing or unable to be changed [Cambridge Dictionary]
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [NIST SP 800-60 Vol.1 Rev. 1]
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, acceptable use policies, or standard security practices. [NIST SP 800-61 Rev. 2]
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber attacks against an organization's information system(s). [NIST SP 800-34 Rev. 1, adapted]
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]
Indicators of Attack	An Indicator of Attack (IOA) is a digital artifact, active in nature, focused on identifying a cyberattack that is in process. [Crowdstrike, adapted]
Indicators of Compromise	Evidence of potential intrusions on a system or network. Often seen in system or application event logs or other date/time-stamped media. [HITRUST]
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [NIST SP 800-53 Rev. 5]
Information Exchange	The transfer of data or messages between parties electronically or via an automated system. [Cambridge Dictionary, adapted]
Information Security	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. See Confidentiality. [NIST SP 800-53 Rev. 5]

Term	Definition
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. See Confidentiality. [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 SP 800-12 Rev. 1, adapted]
Information Spill	Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification or different security category. [CNSSI 4009-2015] Also referred to as Information Spillage [HITRUST}
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Also referred to as system or platform. [NIST SP 800-53 Rev. 5, adapted]
Information System Development	See System Development Life Cycle.
Information Technology	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: (i) requires the use of such equipment; or (ii) 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. [FIPS 200]
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner since it was created, transmitted or stored. [NIST SP 800-57 Part 2 Rev. 1]
Interconnection	Point in a system where two components meet and interact or the device or software component within a system that allows for user interaction. [CNSSI 4009-2015, derived from discussion]
Interface	Common boundary between systems or modules where interactions take place. [CNSSI 4009-2015, NIST SP 800-37 Rev. 2, adapted]
Key Performance Indicator (KPI)	A metric that is used to help manage an IT service, process, plan, project or other activity. 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]
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]

Term	Definition
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. [CNSSI 4009-2015]
Logical Access	Access to information and systems related to information processing services by a user (or a process acting on behalf of a user) through electronic or digital means. [HITRUST]
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impacts on the confidentiality, integrity, or availability of an information system. See Confidentiality. [NIST SP 800-53 Rev. 5, adapted]
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. See Confidentiality. [NIST SP 800-137] A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. [NIST SP 800-61 Rev. 2]
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 a system. [NIST SP 800-171 Rev. 2, 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 SP 800-88]
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 (e.g., performance target, threshold), if appropriate, and the procedure to carry out the measurement and the procedure for the interpretation of the assessment over time. [ISACA, adapted]

Term	Definition
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 systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. [NIST SP 800-53 Rev. 5]
Mobile Device	A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers. [NIST SP 800-53 Rev. 5] 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, smartphones, 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 different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). [NIST SP 800-171 Rev. 2]
Natural Person	A human being as distinguished from a person (as a corporation) created by operation of law. [GDPR Art. 4]
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]
Network Access	Logical access to information and systems related to information processing services by a user (or a process acting on behalf of a user) through a network connection (e.g., local area network, wide area network, Internet). [NIST SP 800-53 Rev. 5, adapted]
Non-conformance	Deviation from a standard or evaluative element [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 SP 800-60 Vol. 1 Rev. 1]

Term	Definition
	A transactional property that prevents a participant in an action or process from later denying participation in the act. [HITRUST]
Notice	Information or a warning given about something that is going to happen in the future. [Cambridge Dictionary]
Objectivity	The ability to exercise judgment, express opinions and present recommendations with impartiality. [ISACA]
Offline	Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. [NIST SP 800-53 Rev. 5 Local Access, adapted)
Online Transaction	A transaction that takes place over a computer network or telecommunications system (e.g., the Internet). See Transaction. [HITRUST]
Operational	Operational measures and metrics are prepared by a person or group responsible for the control/requirement / element being measured (e.g., the control owner) or by a person or group influenced by the control owner (a subordinate, a peer reporting to the same department head, etc.). [HITRUST]
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 their information with third parties. [IAPP, adapted]
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, their information will be shared with third parties. [IAPP, adapted]
Overlay	A specification of security or privacy 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 Rev. 5]
Patch	A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component. [CNSSI 4009-2015]
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. [IAPP, EU GDPR]

Term	Definition
Personally Identifying Information	Any information / data about an individual, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linkable to an individual, such as medical, educational, financial, and employment information. Also referred to as PII. [IAPP, Personally Identifiable Information, adapted] Also referred to as Personal Identifying Information [HITRUST]
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for meeting the tasks, and scheduled milestone completion dates Also referred to as POA&M. [NIST SP 800-115]
Plan, Do, Check, Act 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. Also referred to as PDCA. [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 and Removable Media. [HITRUST]
Prescribed Entity	An entity that is authorized to collect, use, and disclose personal information or personal health information for analysis and compiling statistics in relation to the planning and management of the health care system. [IPC, adapted]
Prescribed Organization	An entity that is responsible for developing and maintaining the electronic health record (EHR). [IPC]
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. [HITRUST]
Privacy	Assurance that the confidentiality of, and access to, certain information about an entity is protected. See Confidentiality. [NIST SP 800-130]
Privacy Control	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. [NIST SP 800-53 Rev. 5]
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, 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, derived from discussion]
Privacy Risk	The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur. [NIST Privacy Framework Version 1.0]

Term	Definition
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	A special authorization that is granted to particular users to perform security relevant operations. [NISTIR 5153, adapted]
Privileged User	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. [NIST SP 800-53 rev 5]
Procedure	A detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes. [ISACA, adapted] A documented procedure must address the operational aspects of how to perform the requirement statement. The procedure should be at a sufficient level of detail to enable a knowledgeable and qualified individual to perform the requirement. [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. [IAPP, EU GDPR] See also Natural Person. [HITRUST]
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]
Proprietary Information	Material and information that is not publicly-accessible relating to or associated with an organization's business activities, relationships, products/services, and know-how that has been clearly identified and properly marked by the organization as proprietary information, intellectual property, or company-confidential information. [CNSSI 4009-2015, adapted]

Term	Definition
Protected Health Information	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. Also referred to as PHI. [HHS PR, adapted]
Protocols	A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [NIST SP 800-82 Rev. 2, NISTIR 8183 Rev. 1]
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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. [IAPP, EU GDPR]
Public	Relating to or involving people not employed, contracted or legally partnered with the organization [Cambridge Dictionary, adapted]
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, World Wide Web, or Web). [HITRUST]
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]
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, 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). See Incident. [ISACA, adapted]
Recovery Point Objective	The point in time to which data must be recovered after an outage. Also referred to as RPO. [NIST SP 800-34 Rev. 1, adapted]

Term	Definition
Recovery Time Objective	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. Also referred to as RTO. [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 processes. [NIST SP 800-34 Rev. 1]
Reliability	The ability to produce consistent results under similar conditions. [HITRUST]
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet) [NIST SP 800-171 Rev. 2, adapted]
Remote Access Server	Devices, such as virtual private network gateways and modem servers, that facilitate connections between networks. [NIST SP 800-86] A type of server that provides a suite of services to remotely connected users over a network or the Internet. It operates as a remote gateway or central server that connects remote users with an organization's internal local area network (LAN). [Techopedia]
Remote Maintenance	Maintenance activities conducted by authorized individuals communicating through an external, non-organization-controlled network (e.g., the Internet). [NIST SP 800-171 Rev. 2, adapted]
Remote Work	Work performed using an information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. [NIST SP 800-63-3, adapted]
Removable Media	Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD). [CNSSI 4009-2015]
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-resistant Authentication	Authentication methods that are resistant to a storage and re-use of authentication credentials (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] The ability of different experts to produce the same results from the same data. [NIST SP 800-30 Rev. 1]

Term	Definition
Required by Law	A mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. [LII 45 CFR § 164.103 - Definitions]
Researcher	A person who conducts research, where research is a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing, and evaluation of research. [PHIPA]
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 impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST SP 800-171 Rev. 2]
Risk Acceptance	The formal acceptance of a specific amount of risk by an individual or organization, such that the level of residual risk has been determined to be a reasonable level of potential loss/disruption for a specific IT system. [NIST SP 800-16, derived from discussion]
Risk Analysis	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations resulting from the operation of a system. [NIST SP 800-171 Rev. 2, adapted]
Risk Appetite	The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. [NISTIR 8286]
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 SP 800-30 Rev. 1, adapted]
Risk Factor	A characteristic used in a risk model as an input to determining the level of risk in a risk assessment. [NIST SP 800-30 Rev. 1]
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 SP 800-30 Rev. 1, adapted]
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. A subset of Risk Response. [NIST SP 800-30 Rev. 1]
Risk Register	A central record of current risks, and related information, for a given scope or organization. Current risks are comprised of both accepted risks and risks that have a planned mitigation path. [NISTIR 8170]
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 Risk Treatment. [NIST SP 800-137, adapted]
Risk Tolerance	The level of risk an organization is willing to assume in order to achieve a potential desired result for a specific activity. [NIST SP 800-137]

Term	Definition
Risk Treatment	The process of selection and implementation of measures to modify risk. See Risk Response. [ISACA]
Risk-based	An information security approach that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. [NIST RMF]
Role-Based Access Control	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. Also referred to as RBAC. [NIST SP 800-95, adapted]
Root Cause Analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks. [NIST SP 800-30 Rev. 1]
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 SP 800-12 Rev. 1, adapted]
Sanitize	To render data recorded/stored on any media inaccessible and/or unrecoverable. [NIST SP 800-88 Sanitization, derived from discussion]
Scaling	The act of applying the considerations necessary to select a specific control baseline in control frameworks with multiple baselines. A part of scoping. [HITRUST, derived from NIST SP 800-53 Rev. 4 Tailoring discussion]
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. [HITRUST, derived from NIST SP 800-53 Rev. 4 Tailoring discussion]
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 Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. [NIST SP 800-37 Rev. 2]
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 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 SP 800-30 Rev. 1]

Term	Definition
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. See Confidentiality. [NIST SP 800-53 Rev. 5, adapted]
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. See Confidentiality. [NIST SP 800-128]
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 SP 800-137, adapted]
Security Control Assessor	The individual, group, or organization responsible for conducting a security or privacy control assessment. [NIST SP 800-53 Rev. 5]
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 SP 800-30 Rev. 1]
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 SP 800-30 Rev. 1]
Security Event	An observable occurrence within a system, service, or network indicating potential impact to the security of such. [NIST SP 800-61 Rev. 2, derived from Event]
Security Functions	The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based [NIST SP 800-171 Rev. 2]
Security Official	A person designated by an organization who is responsible for developing and implementing security policies and procedures including development and implementation of policies and procedures to ensure the integrity of electronic Protected Health Information (ePHI). [HHS, adapted]
Security Posture	The security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. [NIST SP 800-128]
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]
Segmentation	Concept of subdividing a system or network into distinct subparts. Segmentation is useful for controlling access and the spread of an attacker's movement/compromise. [HITRUST]

Term	Definition
Segregation / Separation of Duties	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. Segregation/separation of duties is commonly used in IT organizations 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]
Sender Policy Framework	An open standard specifying a technical method to prevent sender address forgery. Also referred to as SPF. [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 Personal Information	A category of personal information that is classified as more sensitive in nature pertaining to an individual natural person, which may be recognized as such by jurisdictional privacy legislation or regulation (e.g., GDPR, CCPA, etc.) as subject to more stringent conditions for safeguarding or permitting authorized access, handling, or disclosure to organizations, persons, or processes other than the individual natural person the information is representative thereof. [HITRUST]
Service	An act or activity performed on behalf of another party in which a combination of people, process, and technology are used to support operations, management, and decision-making. The service can be provided internally or by a third party. Cloud hosting, data backup, or background investigations are each an example of a service in the context of a HITRUST assessment. [HITRUST]
Service Level	Measured and reported achievement against one or more expected performance level targets (e.g., reliability, acceptable quality, and response times). The term is sometimes used informally to mean service level target. [ITIL, adapted]
Service Level Agreements	An agreement between a service provider and a customer. A service level agreement describes the service, documents service level targets, and specifies the responsibilities of the service provider and the customer. A single agreement may cover multiple services or multiple customers. Also referred to as an SLA. [ITIL, adapted]
Service Provider	An organization supplying services to one or more (internal or external) customers. [ISACA]
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 compromise 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. [CNSSI 4009-2015]
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicitedmessages. [NIST SP 800-53 Rev. 5]
Spyware	Software that is secretly or surreptitiously installed into a system to gather and/or surveil information on individuals or organizations without their knowledge; a type of malicious code. [NIST 800-12 Rev. 1, adapted]

Term	Definition
Stakeholder	Party not directly accountable for risk decisions but is affected by such and whose opinions and preferences are considered by the accountable party. [AICPA, derived from discussion]
Standard	A document, established and approved by a recognized body, that provides for common and repeated use rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. [NISTIR 8074 Vol. 2]
Status Monitoring	Monitoring information security metrics in accordance with the organization's continuous monitoring strategy. [NIST SP 800-137, adapted]
Strong Cryptography	Cryptography based on industry-tested and accepted algorithms. [PCI DSS]
Subcontractor	An individual or business firm contracting to perform part or all of another's contract [Merriam-Webster, adapted]
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 SP 800-30 Rev. 1]
Supervisory Authority	An independent public authority which is established by a Member State pursuant to Article 51 of the European Union's General Data Protection Regulation. [IAPP, EU GDPR adapted]
Supervisory Control and Data Acquisition	Networks or systems generally used for industrial controls or to manage infrastructure such as pipelines and power systems. Also referred to as SCADA. [HITRUST]
Supplier	Entity (organization or person) that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain. [NISTIR 7622 under Supplier ISO/IEC 15288, adapted]
Supply Chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. [NIST SP 800-37 Rev. 2]
Supply Chain Risk	The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system. [CNSSI 4009-2015, adapted]
System Boundary	Defined physical and/or logical perimeter (or demarcation) that contains all components of a system affected by the security or privacy controls. [CNSSI 4009, adapted]
System Development Life Cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation (except in the case where the underlying business service operating on that system is discontinued or retired). [NIST SP 800-137, adapted]
System Owner	Person or organization with responsibility and accountability of the business/financial entitlement, lifecycle management (e.g., development, acquisition, integration, modification, operation, and maintenance, and final disposition), and the security and resiliency of the system or other technology asset. [NIST SP 800-161, derived from discussion]

Term	Definition
System Security Plan	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-137]
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See Tailoring. [NIST SP 800-30 Rev. 1]
Tailoring	The process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. [NIST SP 800-37 Rev. 2]
Technical Controls	The security 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 SP 800-137]
Telework	The act of conducting work from locations other than the organization's facilities. [HITRUST]
Third Country	A country that is not an EU member. [HITRUST]
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 SP 800-12 Rev. 1, adapted]
Threat Agent	Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability. [NIST SP 800-18 Rev. 1]
Threat Analysis	Formal description and evaluation of threat to an information system. [NIST SP 800-53 Rev. 5]
Threat Assessment	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. [CNSSI 4009-2015]
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact. [NIST SP 800-12 Rev. 1]
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, or a system 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 SP 800-63-3. adapted]

Term	Definition
Trust Anchor	An authoritative entity for which trust is assumed. In a public key infrastructure (PKI), a trust anchor is a certification authority, which is represented by a certificate that is used to verify the signature on a certificate issued by that trust-anchor. The security of the validation process depends upon the authenticity and integrity of the trust anchor's certificate. [NIST SP 800-57 Part 1 Rev. 5, adapted]
Two-Factor Authentication	A type of multi-factor authentication in which specifically two factors are used. [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, adapted]
User	Individual, or (system) process acting on behalf of an individual, authorized to access a system. [NIST SP 800-53 Rev. 5]
Validation	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. [NIST SP 800-160 Vol. 1]
Vendor	Supplier of commercial products or services. [NISTIR 4734, adapted]
Vendor Risk Management	See Supply Chain Risk.
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. [HITRUST]
Virtual Machine	Virtual simulation of a complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications running on a single host. May be referred to as a VM. [NIST SP 800-125A, adapted]
Virtual Private Network	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line. Also referred to as a VPN. [CNSSI 4009-201, adapted]
Virtualization	Methodology for emulating or abstracting the simulation of hardware computing resources to enable the complete execution of software stacks that are run on it. [NIST SP 800-125A, adapted]
Voice over Internet Protocol	A term used to describe the transmission of packetized voice using the internet protocol (IP) and consists of both signaling and media protocols. [CNSSI 4009-2015; NIST SP 800-53 Rev.5] A technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers. Also, while some VoIP services only work over your computer or a special VoIP phone, other services allow you to use a traditional phone connected to a VoIP adapter. [https://www.fcc.gov/consumers/guides/voice-over-internet-protocol-voip, derived]
Vulnerability	Weakness in an information system, system privacy or security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [NIST SP 800-53 Rev. 5, adapted]

Term	Definition
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 SP 800-53 Rev. 5, adapted]
Vulnerability Scan	A technique used to identify hosts/host attributes and associated vulnerabilities. [NIST SP 800-115]
Workforce	Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. [HHS, adapted]

List of Acronyms

Acronym	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
AAL	Authorized Access List
AO	Authorizing Official / Agency Official
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	Cybersecurity Incident Response Team
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMS	Center for Medicare and Medicaid Services
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
DDoS	Distributed-Denial-of-Service
DHS	U.S. Department of Homeland Security
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	DNS Security
DoS	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
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
IEC	International Electrotechnical Commission
InfoSec	Information Security
IP	Internet Protocol Intellectual Property
IPSEC	IP Security
IRS	Internal Revenue Service
IRT	Incident Response Team
IS	Information System
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	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
PIA	Privacy Impact Assessments
PII	Personal Identifying Information (also 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
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
SSR	Safeguard Security Report
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
XSS	Cross-Site Scripting

Reference List

Association of International Certified Professional Accountants (AICPA). (n.d.) [AICPA].

https://www.aicpa.org/about/landing/about

AXELOS Limited. (2011). ITIL® ITIL4 Glossary of terms (pdf). [ITIL].
https://www.axelos.com/resource-hub/glossary/ITIL-4-glossaries-of-terms

Cambridge Dictionary. (n.d.) [Cambridge Dictionary].
https://dictionary.cambridge.org/us/

Code of Federal Regulations (CFR). (2022) Title 32, National Defense. [32 CFR].
https://www.ecfr.gov/current/title-32

Crowdstrike. IOA vs IOC. (2022) [Crowdstrike].
https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ioa-vs-ioc/

Department of Defense (DoD). (2020) Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense. Directive 8320.2. (pdf) [DoDD 8320.2].
https://irp.fas.org/doddir/dod/i8320_02.pdf

Department of Health and Human Services. (n.d.) Summary of the HIPAA Privacy Rule. Also related FAQs. [HHS, HHS.gov; HHS PR).
https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Department of Health and Human Services. (n.d.) Summary of the HIPAA Security Rule. Also related FAQs. [HHS, HHS.gov; HHS SR].
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Department of Health and Human Services, Centers for Medicare & Medicaid Services. (2018) Framework for the Independent Assessment of Security and Privacy Controls (pdf) [CMS Assessment].
https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents/ede_security_privacy_assessment_framework_v1.2_2018-03-06.pdf

Department of Labor (DOL). (n.d.) Health Plans and Benefits [DOL]
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).
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1670021121704

European Parliament and the Council of the European Union. (2022) Official Journal of the European Union: Regulation (EU) 2016/679. Document Summary. (EU GDPR).
https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32016R0679&qid=1670021121704

Federal Communications Commission. (n.d.) Consumer Guides.
https://www.fcc.gov/consumers/guides

Flexera (n.d.). Technopedia – an IT Taxonomy. What does Remote Application Server Mean?
https://.technopedia.com/defintionHealthIT.gov. (Expires 9/30/2023) Health IT and Health Information Exchange Basics, FAQ: What is an electronic health record? [HealthIT.gov].
https://www.healthit.gov/faq/what-electronic-health-record-her

HealthIT.gov. (n.d.) Health IT and Health Information Exchange Basics, Health Information Exchange. [HealthIT.gov].
https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/health-information-exchange

International Association of Privacy Professionals (IAPP). (n.d.) Glossary of Privacy Terms [IAPP].
https://iapp.org/resources/glossary/

Internal Revenue Service (IRS). (2021) Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information. (pdf) [IRS Publication 1075].
https://www.irs.gov/pub/irs-pdf/p1075.pdf

ISACA. (n.d.) ISACA Resources Glossary [ISACA].
https://www.isaca.org/resources/glossary

ISC^2. (n.d.) Student Glossary [ISC^2]
https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary#

Legal Information Institute (LII). (n.d.) 45 CFR § 164.103 Definitions. [LII 45 CFR § 164.103 - Definitions].
https://www.law.cornell.edu/cfr/text/45/164.103

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

National Institute of Standards and Technology (NIST). (n.d.). Information Technology Laboratory Computer Security Resource Center (CSRS) Glossary. (Includes Special Publications (SP), Incident Response (IR), and Committee on National Security Systems Instruction (CNSSI)). [NIST], [NISTIR], or [CNSSI], respectively.
https://csrc.nist.gov/glossary

National Institute of Standards and Technology Privacy Framework. (n.d.) [NIST Privacy Framework].
https://www.nist.gov/privacy-framework

National Institute of Standards and Technology (NIST). (n.d.). Information Technology Laboratory Computer Security Resource Center (CSRS) NIST Risk Management Framework RMF. [NIST RMF]

https://csrc.nist.gov/projects/risk-management/about-rmf

National Institute of Standards and Technology (NIST). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). [NIST AI RMF]

https://www.nist.gov/itl/ai-risk-management-framework

New York State Department of Financial Services. (2021). Adoption of an Affiliate's Cybersecurity Program Footnote 1. 23 NYCRR §500.1(c). [NYCRR]

https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211022_affiliates_cybersecurity_program

Ontario, Canada CanLII Consolidated Statutes (n.d.). Personal Health Information Protection Act, 2004, SO 2004 Chapter 3, Schedule A [PHIPA]
https://www.canlii.org/en/on/laws/stat/so-2004-c-3-sch-a/latest/so-2004-c-3-sch-a.html

Ontario, Canada Information and Privacy Commissioner of Ontario (n.d.). FAQs (Frequently Asked Questions) [IPC]
https://www.ipc.on.ca/decisions/three-year-reviews-and-approvals/faqs/

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

Security Standards Council. (n.d.) Payment Card Industry (PCI) Security Standards Council Glossary, Abbreviations, and Acronyms. [PCI DSS]

https://www.pcisecuritystandards.org/glossary/

Software Engineering Institute (1993). Capability Maturity Model for Software (Version 1.1). Carnegie Mellon University. [CMU/SEI-93-TR-024]

http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=11955

University of Toronto, Pressbooks (n.d.). Documentation in Nursing: 1st Canadian Edition, Privacy, Confidentiality, and Security.

https://pressbooks.library.torontomu.ca/documentation/chapter/privacy-confidentiality-and-security/

U.S. Department of State Bureau of Consular Affairs (n.d.). Certificates of Non Citizen Nationality.

https://travel.state.gov

THANK YOU

855.HITRUST (855.448.7878)

www.HITRUSTAlliance.net

HITRUST®