Glossary

A

acceptable use policy (AUP) A formal statement of policy signed by management, acknowledged by the user with their signature, and typically enforced by the Human Resources department. The policy should state prohibited uses such as those related to religion or topics of questionable use and that computing resources are for company business only. The AUP should also state the prohibition of administrative system utilities and related system tools not specifically authorized as contraband. This eliminates any excuses or misunderstanding and enforces separation of duties.

access control lists (ACLs) An access control list (ACL) specifies which users or system processes have access to a specific object, such as an application or process, in addition to what operations they can perform.

Advanced Encryption Standard (AES) AES is a symmetric block type of cipher used to encrypt information. It is currently the standard for the U.S. government in protecting sensitive and secret documents. It is the gold standard of encryption when implemented properly.

Amazon EC2 Amazon EC2 is a web service that provides scalable computing capacity in the cloud. It is an example of IaaS.

annual loss expectancy (ALE) The amount an organization should expect to lose on an annual basis due to incidents. It is typically calculated by multiplying the annual rate of occurrence (ARO) by the single loss expectancy (SLE).

$$ALE = ARO \times SLE$$

annual rate of occurrence (ARO) The annual rate of occurrence (ARO) of an event or security incident is how many times you could expect this event to occur in any given 12-month period.

anonymization Anonymization is the act of permanently and completely removing personal identifiers from data, such as converting personally identifiable information (PII) into aggregated data.

Anything-as-a-Service (AaaS or XaaS) Anything-as-a-Service, also known as AaaS or XaaS, refers to the growing diversity of services available over the Internet via cloud computing as opposed to residing locally or on premises.

Apache CloudStack An open source cloud computing and Infrastructure as a Service (IaaS) platform developed to help IaaS make creating, deploying, and managing cloud services easier by providing a complete stack of features and components for cloud environments.

API gateway A device that filters API traffic. It can be either a proxy or a specific part of your application stack that comes into play before data is processed. Additionally, it can implement access controls, rate limiting, logging, metrics, and security filtering.

Application Normative Framework (ANF) A subset of an organizational normative framework (ONF) that contains only the information required for a specific business application to reach the targeted level of trust. There is a many-to-one relationship between ANFs and ONFs.

application programming interfaces (APIs) APIs are sets of routines, standards, protocols, and tools for building software applications to access a web-based software application or web tool. The two most widely used API formats include REST and SOAP.

application security management process (ASMP) ISO/IEC 27034-1 defines an ASMP used to manage and maintain ANFs created in five steps:

- Specifying the application requirements and environment
- Assessing application security risks
- Creating and maintaining the ANF
- Provisioning and operating the application
- Auditing the security of the application

application virtualization Application virtualization is a software technology that allows for encapsulation of application software execution on an underlying operating system.

auditability Auditability refers to something being in the state of readiness for auditing. In the context of cloud computing, it refers to the ability of an organization to obtain specific information regarding reporting and actions, controls, and processes.

Australian Privacy Act of 1988 APA, enacted in 1988, is an Australian regulation detailing individual privacy safeguards. It includes laws and rules governing the collection, use, storage, and disclosure of personal information, as well as access to and correction of that information.

authentication The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, it is a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

authorization The granting of right of access to a user, program, or process.

availability Refers to the availability of services and or data. It also represents one leg of the three legs of the CIA Triad: confidentiality, integrity, and availability.

B

Big Data Big Data is a term used to describe extremely large datasets used to reveal trends and otherwise undetectable patterns. Big Data is often computationally analyzed using cloud infrastructure and applications due to their scalability and access to large datasets.

bit splitting The technique of splitting up and storing encrypted information across different cloud storage services. This poses challenges to both disaster recovery (DR) and forensics due to the geographical dispersion. Data may reside in different jurisdictions, making forensic eDiscovery difficult or impossible. When trying to accomplish DR activities, the same geographical dispersion may cause problems with timely retrieval of information.

business continuity and disaster recovery (BC/DR) BCP and DR are strategies designed to assist organizations in recovering from activities that disrupt normal functions such as sales and manufacturing. They can cover both short-term and long-term strategies. Additionally, the BIA influences the BCP and DR in guiding the building of the BC strategy.

business requirements Business requirements are what you need to do to enable the implementation of and compliance with business rules.

business rules Business rules are lists of statements that tell you whether you may or may not do anything or that give you the criteria and conditions for making a decision.

business impact analysis (BIA) An exercise that determines the impact of losing the support of any resource (availability) to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems.

C

central processing unit (CPU) A CPU is the core brain of any system. It handles all of the basic I/O instructions as they originate from the software, whether it is in the form of an application or the operating system.

chain of custody The practice and methods of documenting control of evidence from the time it was collected until it is presented to the court. Must be thorough, exhaustive, and detailed, as well as accurate.

cloud administrator This individual is typically responsible for the implementation, monitoring, and maintenance of the cloud within the organization or on behalf of an organization (acting as a third party).

cloud app (cloud application) Short for cloud application, cloud app is the phrase used to describe a software application never installed on a local computer but only accessed via the Internet.

cloud application architect Typically responsible for adapting, porting, or deploying an application to a target cloud environment.

cloud application management platform (CAMP) A specification designed to ease management of applications—including packaging and deployment—across public and private cloud computing platforms.

cloud architect A cloud architect will determine when and how a private cloud meets the policies and needs of an organization's strategic goals and contractual requirements (from a technical perspective).

cloud backup Cloud backup, or cloud computer backup, refers to backing up data to a remote, cloud-based server. As a form of cloud storage, cloud backup data is accessible from multiple distributed and connecting resources that comprise a cloud.

cloud backup service provider A third-party entity that manages and distributes remote, cloud-based data backup services and solutions to customers from a central datacenter.

cloud backup solutions Cloud backup solutions enable enterprises or individuals to store their data and computer files on the Internet using a storage service provider rather than storing the data locally on a physical disk, such as a hard drive or tape backup.

cloud computing Cloud computing is a type of computing, comparable to grid computing, that relies on sharing computing resources rather than having local servers or personal devices to handle applications.

cloud computing accounting software Accounting software hosted on remote servers.

cloud computing reseller A company that purchases hosting services from a cloud server hosting or cloud computing provider and then resells them to its own customers is a cloud computing reseller.

cloud data architect Ensures the various storage types and mechanisms utilized within the cloud environment meet and conform to the relevant SLAs and that the storage components are functioning according to their specified requirements.

cloud database A database accessible to clients from the cloud and delivered to users on demand via the Internet.

cloud developer Cloud developers focus on development for the cloud infrastructure itself. This role can vary from client tools or solutions engagements to systems components. Although developers can operate independently or as part of a team, regular interactions with cloud administrators and security practitioners will be required for debugging, code reviews, and relevant security assessment remediation requirements.

cloud enablement Cloud enablement is the process of making available one or more of the following services and infrastructures to create a public cloud-computing environment: cloud provider, client, or application.

cloud management A term used to describe software and technologies designed for operating and monitoring the applications, data, and services residing in the cloud. Cloud management tools help to ensure a company's cloud computing–based resources are working optimally and properly interacting with users and other services.

cloud migration The process of transitioning all or part of a company's data, applications, and services from on-site premises behind the firewall to the cloud. This enables information to be provided over the Internet on an on-demand basis.

cloud OS A phrase frequently used in place of Platform as a Service (PaaS) to denote an association to cloud computing.

cloud portability The ability to move applications and associated data between one cloud provider and another or between public and private cloud environments.

cloud provider A service provider who offers customers storage or software solutions available via a public network, usually the Internet.

cloud provisioning A term used to describe the deployment of a company's cloud computing strategy, which typically first involves selecting which applications and services will reside in the public cloud and which will remain on-site behind the firewall or in the private cloud.

Cloud Security Alliance (CSA) The CSA is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud-computing environment.

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) The Cloud Security Alliance Cloud Controls Matrix (CCM) provides the fundamental security principles that guide cloud vendors. It is designed to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

cloud server hosting A type of hosting in which hosting services are available to customers on demand via the Internet. Rather than being provided by a single server or virtual server, multiple connected servers that comprise a cloud server provide the hosting environment.

cloud services broker A third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple cloud service providers. It acts as a liaison between cloud services customers and cloud service providers, selecting the best provider for each customer and monitoring the services.

cloud storage The storage of data online in the cloud, wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

cloud testing A term used to describe load and performance testing conducted on the applications and services provided via cloud computing, particularly the capability to access these services in order to ensure optimal performance and scalability under a wide variety of conditions.

cloud washing The act of adding the name "cloud" to a non-cloud service and selling it as a cloud solution.

Common Criteria The *Common Criteria* for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard for computer security certification under ISO/IEC standard 15408. It allows vendors to make certain security claims if their products meet the standard.

community cloud A specific community of organizations with shared concerns (e.g., mission, security requirements, policy, and compliance considerations) provisions this type of cloud infrastructure for exclusive use. One or more of the organizations in the community, a third party, or some combination thereof, community clouds own, manage, and/or operate the environment, and may exist on or off premises.

compute As it applies to cloud computing, the term compute refers to the manipulation of some sort of data by a CPU and associated application such as a calculator performing multiplication on both a variable and an operand.

confidentiality Refers to the concept of keeping secret information from anyone other than someone with authorized access.

content delivery network (CDN) A CDN is a service that replicates data across the global Internet.

control Controls act as mechanisms designed to restrict a list of possible actions to allowed or permitted actions.

converged networking model Optimized for cloud deployments and utilizes standard perimeter protection measures. The underlying storage and IP networks are converged to maximize the benefits for a cloud workload.

corporate governance Describes the relationship between shareholders and other stakeholders in the organization versus the senior management of the corporation.

criminal law A body of rules and statutes that defines prohibited conduct by the government and is set out to protect the safety and well-being of the public.

cross-site scripting (XSS) XSS occurs when an application receives untrusted data and then sends it to a web browser without proper validation. This can allow attackers to execute scripts in the user's browser, hijacking sessions, or other malicious behaviors.

crypto-shredding The process of deliberately destroying encryption keys used to encrypt the data, rendering the data unreadable by anyone.

D

data loss prevention (DLP) Describes the controls put in place by an organization to ensure that certain types of data (structured and unstructured) remain under organizational control, in line with policies, standards, and procedures.

data masking A method of creating a structurally similar but inauthentic version of an organization's data, typically used for purposes like software testing and user training.

database activity monitoring (DAM) A database security technology for monitoring and analyzing database activity that operates independently of the database management system

(DBMS) and does not rely on any form of native (DBMS-resident) auditing or native logs such as trace or transaction logs.

Database as a Service (DBaaS) A cloud-based managed database service.

degaussing Refers to the practice of using strong magnets for scrambling data on magnetic media such as hard drives, tapes, or any other form of magnetic media.

demilitarized zone (DMZ) Because of trustless network access and exposure to external attacks, a demilitarized zone isolates network elements such as email servers that would otherwise be vulnerable.

Desktop as a Service (DaaS) A cloud-based desktop service.

Digital Rights Management (DRM) Focuses on security and encryption to prevent unauthorized copying and limitation of distribution to only those who pay.

Doctrine of the Proper Law When a conflict of laws occurs, the Doctrine of the Proper Law will determine in which jurisdiction the dispute will be heard.

Domain Name System (DNS) A hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as Internet Protocol (IP) addresses. DNS allows you to use friendly names, such as `www.isc2.org`, as opposed to IP addresses in the location of computers and other resources on a TCP/IP-based network.

Domain Name System Security Extensions (DNSSEC) A suite of extensions that adds security to the Domain Name System (DNS) protocol by enabling DNS response validation. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks.

Dynamic Application Security Testing (DAST) In application testing, DAST is a black-box test, where the tool must discover individual execution paths. Unlike SAST, which analyzes code "offline" (when the code is not running), DAST is used against applications in their running state.

E

EC Directive 95/46 The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive adopted in 1995, which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law

eDiscovery Refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

elliptical curve cryptography (ECC) An approach to public-key cryptography using algebraic elliptic curves. ECC requires smaller keys compared to non-ECC cryptography to provide the same level of security as other forms of cryptography.

encryption An overt secret writing technique that uses a bidirectional algorithm in which humanly readable information (referred to as plain text) is converted into humanly unintelligible information (referred to as cipher text).

encryption key A special mathematical code that allows encryption hardware or software to encode and then decipher an encrypted message.

enterprise application The term used to describe applications or software that a business would use to assist the organization in solving enterprise problems.

enterprise cloud backup Enterprise cloud backup solutions typically add essential features such as archiving and disaster recovery to cloud backup solutions.

enterprise DRM An integration plan designed by Digital Equipment Corp. to provide an operation platform for multivendor environments.

enterprise risk management (ERM) The set of processes and structure used in managing risks in the enterprise.

ephemeral storage This type of storage is relevant for IaaS instances and exists only as long as its instance is up. Swap files and other temporary storage needs are examples, all of which will terminate with the instance.

ePHI A term used to describe electronic Protected Health Information.

EU General Data Protection Regulation 2012 This regulation that introduced many significant changes for data processors and controllers, such as

- The concept of consent
- Transfers abroad
- The right to be forgotten
- Establishment of the role of the data protection officer
- Access requests
- Home state regulation, increased sanctions

Eucalyptus An open source cloud computing and Infrastructure as a Service (IaaS) platform for enabling private clouds.

F

Federal Information Security Modernization Act (FISMA) A piece of legislation that defines a comprehensive framework designed to protect U.S. government information, operations, and assets against natural or fabricated threats.

Federal Risk and Authorization Management Program (FedRAMP) A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Federated Identity Management (FIM) An arrangement that can be made among multiple enterprises that allows subscribers to use the same identification data to obtain access to the networks of all enterprises in the group.

federated single sign-on (SSO) SSO systems allow a single-user authentication process across multiple IT systems or even organizations. SSO is a subset of federated identity management, as it relates only to authentication and technical interoperability.

FIPS 140-2 A federal standard for accrediting and distinguishing secure and well-architected cryptographic modules produced by private sector vendors who seek to or are in the process of having their solutions and services certified for use in U.S. government departments and regulated industries (this includes financial services and healthcare) that collect, store, transfer, or share data that is deemed to be "sensitive" but not classified (i.e., Secret/Top Secret).

firewall A type of network device designed to allow only authorized traffic to cross through its interfaces. A DMZ is one part of firewalls.

G

Generally Accepted Accounting Practices (GAAP) GAAP is an AICPA term that stands for Generally Accepted Accounting Practices. These are the industry standards, also recognized by the courts and regulators, that accountants and auditors must adhere to in professional practice. Many of these deal with elements of the CIA Triad, but they also include aspects such as conflict of interest, client privacy, and so forth.

governance The term *governance* relating to processes and decisions defines actions, assigns responsibilities, and verifies performance. The same can be said and adopted for cloud services and environments where the goal is to secure applications and data when in transit and at rest. In many cases, cloud governance is an extension of existing organizational or traditional business process governance, with a slightly altered risk and controls landscape.

Gramm-Leach-Bliley Act (GLBA) A federal law enacted in 1999 by the United States to allow banks to own insurance companies (and vice-versa). Included in its provisions are stipulations regarding the handling of customer information, largely involving privacy.

H

hardware security module (HSM) A device that can safely store and manage encryption keys used in servers, data transmission, log files, and so forth.

Health Insurance Portability and Accountability Act (HIPAA) of 1996 Defines the national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. Protected health information can be stored via cloud computing under HIPAA.

homomorphic encryption Enables processing of encrypted data without the need to decrypt the data. It allows the cloud customer to upload data to a cloud service provider for processing without the requirement to decipher the data first.

honeypot A honeypot consists of a computer, data, or a network site that appears to be part of a network but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

host intrusion-detection system (HIDS) Monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected.

heating, ventilation, and air conditioning (HVAC) HVAC systems provide air management that separates the cool air from the heat exhaust of servers. Many methods provide air management, including racks with built-in ventilation or alternating cold/hot aisles. The best design choice will depend on space and building design constraints.

hybrid cloud This cloud infrastructure consists of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

hybrid cloud storage A combination of public cloud storage and private cloud storage, where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

hypervisor A hypervisor, sometimes also called a virtual machine manager, is a program that allows multiple operating systems to share a single hardware host. These hypervisors come in two basic varieties:

- Type 1, which uses a minimal piece of software to manage the underlying hardware resources such as RAM, CPU, and storage
- Type 2, which has an operating system installed on the hardware and then the virtual machine manager software, or hypervisor, installed on it.

I

identity and access management (IAM) The security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

identity provider An identity provider is responsible for (a) providing identifiers for users looking to interact with a system, (b) asserting to such a system that such an identifier

presented by a user is known to the provider, and (c) possibly providing other information about the user that is known to the provider. This can be achieved via an authentication module, which verifies a security token that can be accepted as an alternative to repeatedly explicitly authenticating a user within a security realm.

information gathering Refers to the process of identifying, collecting, documenting, structuring, and communicating information from various sources in order to enable educated and swift decision making to occur.

information security management system (ISMS) A set of policies concerned with information security management or IT-related risks. The idioms arose primarily out of BS 7799.

Infrastructure as a Service (IaaS) A model of cloud computing that provides a complete infrastructure (e.g., servers and internetworking devices) and allows companies to install software on provisioned servers and control the configurations of all devices.

integrity One of the legs of CIA, integrity ensures that data has not been altered by an unauthorized entity.

Internet Engineering Task Force (IETF) An international organization of network designers and architects who work together in establishing standards and protocols for standardization of the Internet.

interoperability Defines the ease of ability with which application components are moved and reused elsewhere—regardless of the provider, platform, OS, infrastructure, location, storage, or the format of the data or APIs.

ISO/IEC 27001:2013 Helps organizations establish and maintain an ISMS. An ISMS is a set of interrelated elements that organizations use to manage and control information security risks and to protect and preserve the confidentiality, integrity, and availability of information.

ISO/IEC 27018 Addresses the privacy aspects of cloud computing for consumers and is the first international set of privacy controls in the cloud.

ISO/IEC 27034-1 Represents an overview of application security. It introduces definitions, concepts, principles, and processes involved in application security.

ITIL ITIL, formerly known as the Information Technology Infrastructure Library, is a set of practices that focus on aligning IT services with business needs.

K

Key management Includes the generation, storage, distribution, deletion, archiving, and application of keys in accordance with a formal security policy.

L

legacy Refers to traditional types of IT tools and technologies.

local area network (LAN) LANs are the backbone of infrastructure. They are a logical grouping of devices that allow traffic to be contained and operate at high speeds.

logical design A part of the design phase of the SDLC in which all functional features of the system chosen for development in analysis are described independently of any computer platform.

long-term storage Write Once, Read Many (WORM) is a type of long-term storage, meaning it is written to initially and only used for read purposes thereafter.

M

managed service provider An IT service provider where the customer dictates both the technology and operational procedures.

management plane Controls the entire infrastructure. Independent of network location and always partially exposed to customers, it is therefore a prime resource to protect.

masking A weak form of confidentiality assurance that replaces the original information with asterisks or X's.

mean time between failures (MTBF) MTBF represents the mean or average time between the time a device is brought into service and the time it will typically fail or require repair.

mean time to repair (MTTR) MTTR represents the average time required to repair a device that has failed or requires repair.

Microsoft Azure A Microsoft cloud service offering that provides Platform as a Service (PaaS), allowing developers to create cloud applications and services.

middleware A term used to describe software that works between an operating system and another application or database of some sort. Typically, middleware operates above the transport layer and below the application layer.

mobile cloud storage A form of cloud storage that applies to storing an individual's mobile device data in the cloud and providing the individual with access to the data from anywhere.

multifactor authentication (MFA) A method of access control in which a user can pass by successfully presenting authentication factors from at least two of the three following categories:

- Knowledge factors ("things only the user knows"), such as passwords
- What the user has (security token)
- What the user is (biometric verification)

multitenancy Datacenter networks logically divided into smaller, isolated networks. They share the physical networking gear but operate on their own network without visibility into the other logical networks.

N

network intrusion-detection system (NIDS) A device or software application that monitors networks or systems for malicious activities or policy violations and produces electronic alerts and/or reports to a management station.

NIST 800-14 NIST 800-14, entitled *Generally Accepted Principles and Practices for Securing Information Technology Systems*, provides a baseline that organizations can use to establish and review their IT security programs.

NIST 800-53r4 NIST 800-53r4, entitled *Security and Privacy Controls for Federal Information Systems and Organizations*, describe ways to ensure the proper application of appropriate security requirements and security controls to all U.S. federal government information and information management systems.

NIST 800-123 NIST 800-23, entitled *Guide to General Server Security*, assists organizations in understanding the fundamental activities performed as part of securing and maintaining the servers that provide services over network communications as a main function.

NIST 800-145 NIST 800145, entitled *Definition of Cloud Computing*, outlines both the cloud computing deployment and service models and their definitions.

NIST 800-146 NIST 800-146, entitled *Cloud Computing Synopsis and Recommendations*, reprises the NIST-established definition of cloud computing, describes cloud computing benefits and open issues, presents an overview of major classes of cloud technology, and provides guidelines and recommendations on how organizations should consider the relative opportunities and risks of cloud computing.

nonrepudiation The assurance that a specific author actually did create and send a specific item to a specific recipient and that it was successfully received. With assurance of nonrepudiation, the sender of the message cannot later credibly deny having sent the message, nor can the recipient credibly claim not to have received it.

O

obfuscation The convoluting of code to such a degree that even source code is not easily decipherable.

object storage Objects (files) are stored with additional metadata (content type, redundancy required, creation date, etc.). These objects are accessible through APIs and potentially through a web user interface.

online backup Online backups leverage the Internet and cloud computing to create an attractive off-site storage solution with little hardware requirements for any business of any size.

OpenID OpenID is one form of authentication used to enable SSO. It enables the user to log into more than one application or website using the same credentials.

Open Web Application Security Project (OWASP) The Open Web Application Security Project (OWASP) is a 501(c) (3) worldwide not-for-profit charitable organization focused on improving the security of software.

operational-level agreement (OLA) A contract that defines how various IT groups within a company plan to deliver a service or set of services.

organizational normative framework (ONF) A framework of so-called containers for all components of application security best practices catalogued and leveraged by the organization. It contains at least one, but often more, application normative frameworks (ANFs). Therefore, there is a one-to-many relationship between an ONF and ANFs.

oversubscription Occurs when more users connect to a system than can be fully supported simultaneously.

P

Payment Card Industry Security Standards Council (PCI Council) The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection.

penetration test A test or attack designed to test system(s) or network(s) or web application(s) for vulnerabilities that would allow an attacker to gain control over said system, network, or application.

personal cloud storage A form of cloud storage that applies to storing an individual's data in the cloud and providing the individual with access to the data from anywhere.

personal data Any information relating to an identified or identifiable natural person data subject; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity.

personal health information (PHI) As defined by DHHS, PHI is any information about health status, provision of healthcare, or payment for healthcare that is created or collected by a "covered entity."

personally identifiable information (PII) Information that can be traced back to an individual user, such as your name, postal address, or email address. Personal user preferences tracked by a website via a cookie are also considered personally identifiable when linked to other personally identifiable information provided by you online.

Platform as a Service (PaaS) PaaS is a way for customers to rent hardware, operating systems, storage, and network capacity over the Internet from a cloud service provider.

portability A phrase used to describe the ability to move applications and associated data between one cloud provider and another or between public and private cloud environments.

privacy level agreement (PLA) An agreement whereby the cloud provider states the level and types of personal data protection(s) in place.

private cloud A private cloud infrastructure is provisioned for exclusive use by a single organization consisting of multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on- or off-premises.

private cloud project Enables its IT infrastructure to become more capable of quickly adapting to continually evolving business needs and requirements.

private cloud security A private cloud implementation aims to avoid many of the objections regarding cloud computing security. Because a private cloud setup is implemented safely within the corporate firewall, it remains under the control of the IT department.

private cloud storage A form of cloud storage where the enterprise data and cloud storage resources both reside within the enterprise's datacenter and behind the firewall.

public cloud A public cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

public cloud storage A form of cloud storage where the enterprise and storage service provider are separate and the data is stored outside of the enterprise's datacenter.

public key encryption A form of public key infrastructure (PKI) is a framework of programs, procedures, communication protocols, and public key cryptography that enables a diverse group of individuals to communicate securely.

Q

qualitative assessment (QA) QA typically employs a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels (e.g., very low, low, moderate, high, very high).

quality of service (QoS) QoS refers to the capability of a network to provide better service to selected network traffic over various technologies, including frame relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

quantitative assessment Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers. This type of assessment most effectively supports cost–benefit analyses of alternative risk responses or courses of action.

R

random access memory (RAM) A form of high-speed volatile computer storage used by application and operating systems.

record A data structure or collection of information that is retained by an organization for legal, regulatory, or business reasons.

reduced sign-on (RSO) Not to be confused with single sign-on (SSO) or federated single sign-on. Reduced sign-on refers to not having to sign into each piece of data or store once authorization has been granted.

redundant array of inexpensive disks (RAID) Instead of using one large disk to store data, you can use many smaller disks (because they are cheaper). An approach to using many low-cost drives as a group to improve performance, yet also provides a degree of redundancy that makes the chance of data loss remote.

Remote Desktop Protocol (RDP) A protocol that allows for separate channels for carrying presentation data, serial device communication, licensing information, and highly encrypted data (keyboard, mouse activity).

Representation State Transfer (REST) REST relies on stateless, client-server, cacheable communications. It is a software architecture style consisting of guidelines and best practices for creating scalable web services.

request for proposal (RFP) An RFP is generally part of initial vendor management process when a company first asks vendors to reply with a proposal to meet some type of need.

Restatement (Second) of Law The restatement of law refers to situation where there is no such local legislative directive in a case. When no such factor exists, the factors relevant to the choice of the applicable rule of law are used.

return on investment (ROI) A term used to describe a profitability ratio. It is generally calculated by dividing net profit by net assets.

return point objective (RPO) A term used in BCP/DR describing the maximum allowable amount of data that might be lost due to an outage before severe (and usually unrecoverable) consequences are experienced. The RPO is the point at which recovery becomes extremely difficult or even impossible.

return time objective (RTO) A term used in BCP/DR describing a point in time after which an outage has occurred, beyond which recovery becomes extremely difficult or even impossible.

reversibility Refers to the ability to back out of a transaction or event such as an upgrade or patching of a system. Is the user able to “reverse” the event and return the system(s) to its former state?

S

sandboxing Sandboxing refers to a system(s) ability to cordon off or protect certain aspects of the compute environment such as processing, memory, and other resources needed in the compute transaction. It can be used for testing untested applications or carving out resources that cannot then touch other parts of the same system as part of a security strategy to isolate those operations.

Sarbanes-Oxley Act (SOX) SOX was enacted after several large company accounting scandals such as that of Enron and WorldCom involved large accounting errors of judgement. Named after the bill's authors, Sen. Paul Sarbanes (D-MD), and Rep. Michael G. Oxley (R-OH, and formerly known as the *Public Company Accounting Reform and Investor Protection Act*, SOX was enacted in 2002.

Secret Sharing Made Short (SSMS) SSMS is a method of bit splitting that uses a three-phase process consisting of encryption, use of an information dispersal algorithm (IDA), and splitting of the encryption key using the secret sharing algorithm. The fragments are then signed and distributed to different cloud storage services, making it impossible to decrypt without both arbitrarily chosen data and encryption key fragments.

Security Assertion Markup Language (SAML) SAML is an XML-based, open standard data format designed for the exchange of authentication and authorization data between parties. IT utilizes the services of both an identity provider and a service provider.

security information and event management (SIEM) Often used interchangeably with SIM, SIEMs deal with real-time security event monitoring. These solutions generally log and sort thousands to millions of logs in real time, generating usable reports that assist security professionals in making better informed and earlier security decisions.

sensitive data Sensitive data can be many things—Social Security number, DOB, address, and so forth. Each business must make decisions about what is sensitive in its operations in order to develop and apply appropriate controls for the protection of that information.

service-level agreement (SLA) A formal, legal, agreement between two or more organizations that may or may not contain incentives and/or penalties. One use of the SLA is to determine whether a customer is actually receiving the services outlined in the SLA.

Service Organization Controls 1 (SOC 1) SOC 1 reports are one of the reports on controls at service organizations focusing on the user entity's internal control over financial reporting.

Service Organization Controls 2 (SOC 2) SOC 2 reports are relevant to a user entity's internal controls over the five security principles of security, processing, integrity, confidentiality, and privacy.

Simple Object Access Protocol (SOAP) A messaging protocol specification designed for exchanging structured information in web services. It allows programs to operate independently of the client operating system.

single loss expectancy (SLE) The amount of expected damage or loss incurred by any single security incident.

single sign-on (SSO) SSO allows a user to access multiple applications with a single set of credentials for authentication and authorization. It is often tied to federated SSO and often confused with reduced sign-on (RSO).

Six Sigma Six Sigma is used to identify defects in processes so that the processes can be improved upon.

Software as a Service (SaaS) SaaS offers the user the capability of using the vendor's or cloud provider's application solution on their existing infrastructure.

software defined networking (SDN) The idea of separating the network control plane from the actual network forwarding plane. This allows for greater control over networking capabilities and for the integration of such things as APIs.

software development life cycle (SDLC) The concept of establishing clear phases and methodologies as part of software development.

solid-state drive (SSD) SSDs are widely used in cloud computing today because of their reduced cost and high speed. They can typically operate at much greater speeds than traditional spinning drives and use less power and generate less heat.

static application security testing (SAST) Generally considered a white-box test, wherein examination of application code for problems occurs without executing the binary.

storage cloud The collection of multiple distributed and connected resources responsible for storing and managing data online in the cloud.

storage clusters The use of two or more storage servers working together to increase performance, capacity, or reliability. Clustering distributes workloads to each server, manages the transfer of workloads between servers, and provides access to all files from any server regardless of the physical location of the file

Stored Communications Act (SCA) The SCA, enacted in the United States in 1986 as part of the Electronic Communications Privacy Act, provides electronic communication and computing services privacy protections from unauthorized access or interception.

STRIDE Threat Model First developed by Microsoft and derived from an acronym for the following six threat categories: **S**poofing identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege.

T

TCI reference architecture A methodology and a set of tools that enables security architects, enterprise architects, and risk management professionals to leverage a common set of solutions that fulfill their common needs to be able to assess where their internal IT and their cloud providers are in terms of security capabilities and to plan a roadmap to meet the security needs of their business.

threat modeling The idea of identifying specific points of vulnerability and then implementing countermeasures to protect or thwart those points from successful exploitation.

tokenization The process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security.

tort law A body of rights, obligations, and remedies that sets out reliefs for persons suffering harm as a result of the wrongful acts of others.

traditional network model These models use a layered approach with physical switches at the top layer and logical separation at the hypervisor level.

V

vendor lock-in Refers to the idea of a cloud provider or solution not allowing the customer to move their applications or data in the event they need or want to do so.

vertical cloud computing Refers to the optimization of cloud computing and cloud services for a particular vertical (e.g., a specific industry) or specific-use application.

virtual machine introspection (VMI) An agentless means of ensuring a VM's security baseline does not change over time. It examines such things as physical location, network settings, and installed OS to ensure that the baseline has not been inadvertently or maliciously altered.

virtualization In cloud computing, virtualization refers to creating a virtual (a logical vs. a physical) version of something, including virtual computer hardware platforms, operating systems, storage devices, and computer network resources. Computer hardware virtualization is a way of improving overall efficiency. It involves CPUs that provide support for virtualization in hardware, and other hardware components that help improve the performance of a guest environment.

virtualization technologies These technologies enable cloud computing to become a real and scalable service offering due to the savings, sharing, and allocations of resources across multiple tenants and environments.

volume storage Volumes that are attached to virtual storage that behave just like a physical drive or array.

vulnerability assessment A vulnerability assessment or scan is designed to identify known vulnerabilities in applications, operating systems, or network devices.

W

web application firewall (WAP) An appliance, server plug-in, or filter that applies a set of rules to an HTTP conversation. Generally these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.

X

XML gateway XML gateways transform how services and sensitive data are exposed as APIs to developers, mobile users, and the cloud. They can be either hardware or software, and they can implement security controls such as DLP, AV, and antimalware services.