C848 – MANAGING CLOUD SECURITY (CCSP)

Contents

Chapter 1 – Architectural Concepts

Existing State – evaluate and understand the business processes, assets, and requirements; after collecting sufficient data, a detailed analysis is necessary; a BIA (business impact analysis) takes place.

- **BIA (Business Impact Analysis):** an assessment of the priorities given to each asset and process within the organization; analysis considers the effect (impact) any hard or soft loss might mean to the organization overall; identify critical paths and single points of failure; determine the costs of compliance (legislative and contractual requirements mandated).

- **Metered service:** the organization only pays for what it uses.

- **Rapid Elasticity**: excess capacity available to be apportioned to cloud customers.

- **Cloud bursting:** organizations to use hosted cloud service to augment internal, private data center capabilities with managed services during times of increased demand; an organization can rent the additional capacity as needed from an external cloud provider (crisis situation, heavy holiday shopping periods); Rapid scalability allows customers to dictate the volume of resources.

Cloud service benefits: reduction in personnel costs (data management); reduction in capital expenditure (metered service, rapid elasticity, cloud bursting); reduction in operational costs; transfer of some regulatory costs; reduction in costs for data archival and backup services.

- **ROI (Return on Investment):** term related to cost-benefit measures; used to describe a profitability ratio; calculated by dividing net profits by net assets

- **Elasticity**: customers can contract cloud providers to use virtualization to flexibly allocate only the needed usage of each resource to the organization while holding costs while maintaining profitability; allow users to access their data from diverse platforms and locations, increasing portability, accessibility, and availability.

- **Simplicity**: allow a user to seamlessly use the service without frequently interacting with the cloud service provider.

- **Scalability**: increasing or reducing services can be easily, quickly, and cost-effectively accomplished.

Cloud Computing Service Models

- **IaaS (Infrastructure as a Service):** most basic service; allows customers to install all software and OSs on hardware housed and connected by the cloud vendor; can be considered a warm site for BC/DR purposes; optimal for organizations wanting control over the security of their data and limited cloud vendor assistance (BC/DR or archiving); least expensive option; customer retention of IT staffing.
    - When to use: website or application hosting; virtual data centers; data analysis.

- **PaaS (Platform as a Service):** includes services from IaaS and OSs (offers a selection for customers to use, Windows, Linux, Mac, etc.); vendor is responsible for patching, administering, and updating the OS; customer can install any software; useful for customers involved in software development (they can test on multiple OS platforms); <u>includes cloud-based database engines</u> and services "big data" style services (data warehousing and datamining); provider offers access to back-end engine/functionality, while customer can create/install apps/APIs to access the backend.

    - When to use: reduce development time; support for different programming languages; easy collaboration for remote or distributed teams; high development capabilities without additional staff.
    - Data storage types used: structured and unstructured.
    - **Unstructured Data Types**: qualitative data; natural-language text; incorporate media (audio, video, images); contains JSON, XML, and binary objects (images encoded as text strings); important for data analytic strategies; noSQL.
    - **Structured Data Types**: quantitative data; organized and decipherable by **machine learning** algorithms; SQL (relational) can be used to quickly input, search, and manipulate data; used by **machine learning** algorithms.

- **SaaS (Software as a Service):** includes everything from IaaS and PaaS with the addition of software programs; vendor is responsible for administering, patching, and updating everything; also takes care of all infrastructure, compute, and storage needs as well as providing OSs and applications; customer is only involved in uploading and processing data in a full production environment; application is a shared responsibility of all parties.
    - When to use: (personal) email services (gmail), cloud storage services (dropbox), cloud-based file management (Google Docs); (business) gmail, collaboration tools (Trello), CRM (Salesforce), ERP.

Cloud Deployment Models

- **Public** Cloud: resources are owned and operated by a vendor and sold, leased, or rented to anyone; multitenant environments; multiple customers will share resources; EX: The customer might be using an AM that resides on the same hardware that hosts another VM as their competitor, but they do not know the entities using the same resources. Rackspace, Microsoft's Azure, and AWS (Amazon Web Services)

- **Private** Cloud: resources dedicated to a single customer; might be owned and maintained by the entity that is the sole customer (the organization might own and operate a data center that serves as the cloud environment for the organization's users); might be a set of resources (racks, blades, software packages) owned by the single customer but located and maintained at the provider's data center; the provider might offer physical security, admin services, and utilities (power, Internet) for customers (referred to as a co-located environment).

- **Community** Cloud: features infrastructure and processing owned and operated by or for an affinity group; organizations come together to perform joint tasks and functions; gaming communities; ownership is spread throughout the various members of the community; can be provisioned by a third party (FedRAMP service, only used by US federal government).

- **Hybrid** Cloud: contains elements of other models; organizations might want to retain some private cloud resources (remote user access) but lease some public cloud space (the PaaS function for software development and testing).

Roles/Responsibilities

- A cloud broker is a company that purchases hosting services from a provider and resells them to its own customers.

- **CASB (Cloud Access Security Broker):** third-party entity offering independent IAM (identity and access management) services to CSPs and cloud customers; can be SSO, certificate management, or cryptographic key escrow

- **Regulators**: ensure organizations are in compliance with the regulatory framework for which they are responsible; HIPAA, GLBA, PCI DSS, ISO, SOX, etc. Regulators include the FTC, SEC, and auditors.

Definitions

- **Cost-Benefit Analysis**: comparing the potential positive impact (profit, efficiency, market share) of a business decision to the potential negative impact (expense, detriment to production, risk) and weighing the two as equivalent or not (potential positive or negative).

- **FIPS 140-2**: NIST document that describes the process for accrediting and cryptosystems for use by the federal government; lists only approved cryptographic tools

- **NIST 800-53: A** guidance document with the primary goal of ensuring appropriate security requirements and controls are applied to all US federal government information in management systems

- **TCI (Trusted Cloud Initiative)** Reference Model: a guide for cloud providers, allowing them to create a holistic architecture that customers can purchase (including the physical and logical layout of the network and the processes necessary to utilize both).

- **Vendor Lock-In**: situation where a customer is unable to leave, migrate, retrieve, or transfer data to an alternate provider due to technical or nontechnical constraints; use portability for a level of ease when transporting data; ensure contract states so; avoid proprietary formats (requires specific software to read data); check for regulatory constraints; detrimental contract terms or technical limitations

- **Vendor Lock-Out**: when a customer is unable to recover or access their own data due to the provider going into bankruptcy or leaving the market

- **Blockchain: an** open means of conveying value using encryption technologies and algorithms (cryptocurrency); a transactional ledger where all participants can view every transaction, making it extremely difficult to negatively affect the integrity of past transactions; each record (block) is distributed among all participants in a distributed or cloud-based manner.

- **Containers**: logical segmentation of memory space in a device, creating two or more abstract areas that cannot interface directly; commonly used in BYOD environments; distinguishing two distinct partitions (one for work functions or data and the other for personal functions or data).

- **Quantum computing is an** emerging technology that allows IT systems to operate beyond binary math. Instead of using the presence of electrons for calculations (electrons are either present or not), quantum computing may use subatomic characteristics (electron spin, charm, etc.) to offer computing on an exponentially larger scale.

- **Homomorphic encryption is a** theoretical phenomenon that allows the processing of encrypted material without needing to first decrypt it; it can allow cloud customers to upload encrypted data and still utilize data without sharing keys with the provider or having to accommodate decryption as part of the process.

- **STRIDE** Threat Model: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

- **Apache cloud stack**: open source cloud computing software for creating, managing, and deploying infrastructure cloud services; uses existing hypervisor platforms.

- **Business Requirement**: operational driver for decision-making and input for risk management

Chapter 2 – Design Requirements

Business Requirements Analysis – inventory of all assets; valuation of each asset (BIA, data owners determine value; head of department); determination of critical paths (made by senior management; SPOFs), processes, and assets; clear understanding of risk appetite (set by senior management)

SPOFs (Single Points of Failure) methods to reduce – adding redundancies; creating alternative processes; cross-training personnel; back up data; load sharing/balancing for IT assets

- **Quantitative** Risk Assessment: use specific numerical values such as 1,2, and 3; employ a set of methods, principles, or rules for assessing risk
- **Qualitative** Risk Assessment: use nonnumerical categories that are relative in nature; high, medium, and low; employ a set of methods, principles, or rules for assessing risk
- **Risk**: likelihood an impact will be realized; can be reduced, never eliminated; orgs can accept a level of risk that allows operations to continue in a successful manner; legal and defensible to accept risks higher than the norm/greater than your competitors (except risk to health and human safety, must be addressed to industry standard/regulatory scheme)

There are four main ways to address risk

- **Avoidance**: risk that exceeds the organization's appetite; leaving business opportunity because risk is too high and cannot be compensated for with adequate control mechanisms; response to cost-benefit analysis; don't conduct the risk at all; halts business functions
- **Acceptance**: opposite of avoidance; falls within the org's risk appetite; org continue operations without any additional efforts
- **Transference**: org pays someone else to accept the risk, at a lower cost (insurance); normally with low probability of occurring but a high impact if they do

- **Mitigation**: org take steps to decrease the likelihood/impact of the risk; form of controls/countermeasures, where security practitioners are involved
- **Residual Risk**: when risks are mitigated by applying countermeasures and controls the remaining leftover risk is residual risk; task of security program is to reduce until it falls within the acceptable level according to org's risk appetite (senior management dictates the appetite)

Security Considerations for Cloud – the cloud customer is always legally liable for any loss of data, even if cloud provider demonstrates negligence or malice

- IaaS Considerations – customer has the most responsibility and authority; provider is responsible for building, land, connectivity, power, and hardware assets; makes auditing difficult because they cannot set up network monitoring for policy and regulatory compliance, but customers can collect and review event logs from the software (OS too)
- PaaS Consideration – same as IaaS but provider controls the OSs; customer can still monitor and review software events because the programs running on the OS belongs to them
- SaaS Consideration – customer only supplies and process data; security controls are limited because provider supplies all needs of customer
- To demonstrate due care – ensure cloud provider performs strict background checks, continual monitoring of all personnel with access to data center, extreme physical security measures, encryption of data processed and stored, assignment of contractual liability to the provider, etc.

Chapter 3 – Data Classification

Data Ownership: assign responsibilities according to who has possession and legal ownership of that data; roles are assigned to allocate this

- **Data Owner:** org that collected/created the data; usually department head/business unit manager; cloud customer is usually the data owner (international treaties/frameworks refer to as the data controller)
    - Data owners remain legally responsible for all data they own
- **Data Custodian:** person or entity tasked with the daily maintenance/administration of the data; role of proper security controls and processes as directed by the data owner; sometimes a database admin
- **Data Processor**: any org or person who manipulates, stores, or moves the data on behalf of the data owner; cloud provider is a data processer (international law)

    - Data processors do not necessarily all have direct relationships with data owners; processors can be third parties or further removed down the supply chain

Data Lifecycle – understand it in order (Create > Store > Use > Share > Archive > Destroy)

- **Create**: data owner will be identified in this first phase; data security and management responsibilities require action; data owner will categorize the data
- Data Categorization:
    - **Regulatory Compliance**: can categorize by specific datasets (GLBA, PCI, SOX, HIPAA, GDPR, other international, national, and local compliance)
    - Business Function: different use of data (billing, marketing, operations)
    - Functional Unit: department or office with its own category and data controls
    - By Project: define datasets by projects associated with as means of creating discrete, compartmentalized projects
    - **Data Classification**: responsibility of the data owner; assigned by the org's policy based on characteristics of dataset
        - Sensitivity: used by the US military; assigned to the sensitivity of the data, based on negative impact an unauthorized disclosure would cause
        - Jurisdiction: geophysical location of the source/storage point of the data might determine how the data is handled; PII gathered from citizens from EU is subject to the EU privacy laws
        - Criticality: data deems critical to org survival classified in a manner distinct from trivial, basic operational data; BIA helps determine this
    - **Data Mapping**: data between organizations (or departments) normalized and translated so it is meaningful to both parties; in classifications, mapping is necessary so data that is sensitive must be protected in one org must be recognized by the receiving org
    - **Data Labeling**: when data owner creates, categorizes, and classifies the data, it also must be labeled; should indicate who the data owner is (office or role, not name or identity); should take any form to be enduring, understandable, and consistent; Ex: labels on hardcopy data might be printed headers/footers, labels on electronic files might be embedded in the filename/nomenclature; labels should be evident and communicate pertinent concepts without disclosing data they describe; labels may include:
        - Date of creation; Date of scheduled destruction/disposal; Confidentiality level; Handling directions; Dissemination/distribution instructions; Access limitations; Source; Jurisdiction; Applicable regulation
- **Data Discovery**: used to refer several kinds of tasks to determine and accurately inventory the data under its control; org is attempting to create an initial inventory of data it owns, org is

involved in electronic discovery (e-discovery), and can modern the use of datamining tools to discover trends and relations in the data already in the org's inventory

    - **E-Discovery**: legal term for how electronic evidence is collected as part of an investigation/lawsuit

- **Label-Based Discovery**: labels created will aid in any data discovery efforts; org can determine what data it controls and amounts of each kind; labels are useful when the discovery effort is undertaken in response to a mandate with specific purpose (court order/regulatory demand); can easily collect and disclose all appropriate data if labeled
- **Metadata-Based Discovery**: data about data, a listing of traits and characteristics about specific data elements/sets; can be useful for discovery purposes; data discovery uses metadata the same way as labels to scan field for particular terms for certain purposes
- **Content-Based Discovery**: discovery tools can be used to located and identify specific kinds of data by delving into the content of datasets (even without labels/metadata); basic term searches or sophisticated pattern-matching technologies

Data Analytics: technological options to provide additional findings and assigning types to data; modern tools create new data feeds from sets of data that already exist within the environment; modes used are real-time analytics, datamining, and agile business intelligence

- **Datamining**: an outgrowth of the possibilities offered by regular use of the cloud (big data); when org collects data streams and run queries across the feeds, the org can detect and analyze previously unknown trends and patterns that can be useful
- **Real-Time Analytics**: tools can provide datamining functionality concurrently with data creation and use; the tools rely on automation and require efficiency to perform properly
- **Agile Business Intelligence**: state-of-the-art datamining involves recursive, iterative tools and processes that can detect trends and identify more oblique patterns in historical and recent data

Jurisdictional Requirements

- United States: address privacy with industry-specific legislation (GLBA for banking/insurance, HIPAA for medical care, etc.) or with contractual obligations (PCI); granular data breach notification laws exist that are enforced by states and localities (New York/California); strong protections for intellectual property
- Europe: has massive, exhaustive, comprehensive personal privacy protections (EU General Data Protection Regulation); good intellectual property protection
- Asia: data privacy protection levels differ by country; with its Act on the Protection of Personal Information, Japan and Singapore adheres to the EU model, China has a legal requirement the opposite of privacy (all IT traffic and communications in China must be accessible by the Chinese government); disparate levels of intellectual property protection

- South/Central America: most countries lack privacy protection frameworks; Argentina is an exception; their Personal Data Protection Act is in direct correlation with the EU legislation; has various intellectual property mechanisms
- Australia/New Zealand: has the Australian Privacy Act mapping directly to the EU statutes; provide strong intellectual property protections and strong privacy protections

IRM (Information Rights Management) – managing information in accordance with who has rights to it; can be **DRM** (digital/data rights management), ERM (enterprise); uses a variety of tools to enforce intellectual property rights such as support-based licensing, local agent enforcement, and media-present checks.

Intellectual Property Protections – intangible; assets of the mind

- **Copyright**: legal protection for expressions of ideas; in the US, granted to anyone who first creates an expression of an idea (literary works, films, music, software, and artistic works); does not cover ideas, specific words, slogans, recipes, formulae; lasts for 70 years after the author's death/120 years after the first publication of a work for hire; creator is the only entity legally allowed to do the following: perform the work publicly, profit from the work, make copies of the work, make derivative works from the original, import or export the work, broadcast the work, sell/assign the rights
- **Trademarks**: : intended to be applied to specific words and graphics; representations of an org – its brand; can be the name of an org, logo, phrase, color, sound, or combo of these
- **Patents**: legal mechanism for protecting intellectual property in the form of inventions, processes, materials, decorations, and plant life; lasts about 20 years from time of patent application
- **Trade Secrets:** has same aspects as patented material (processes, formulas, commercial methods, etc.); includes aggregations of information (list of clients/supplies)

IRM Tool Traits – material protected by IRM solutions need some form of labeling/metadata associated with the material for the IRM tool to function properly

- **Rudimentary Reference Checks:** content itself can check for proper usage/ownership; Ex: vintage games will pause in operation until player entered information acquired with the purchase of a licensed copy of the game (word/phrase from manual shipped with game)
- **Online Reference Checks**: Microsoft software packages (Windows OS/Office programs) requiring product key at installation; program will check against online database when connected to the Internet
- **Local Agent Checks**: user installs reference tool that checks the protected content against the user's license; Ex: Steam when installing games purchased, agents check user's system against online license database to ensure games are not pirated

- **Presence of Licensed Media**: disks for example, is required to be present when the content is being used; IRM engine is on the media, often installed with a cryptographic engine that identifies the unique disk and the licensed content and allowing usage based on that relationship
- **Support-Based Licensing**: predicted on the need of continual support for content (production software); vendor can prevent unlicensed versions from getting support (updates/patches)

IRM in the Cloud Complications

- **Replication Restrictions**: IRM often prevent unauthorized duplication, the cloud may create, close, and replicate virtualized host instances; IRM might interfere with automatic resource allocation processes
- **Jurisdictional Conflicts**: cloud extends across boundaries and borders, often pose problems when intellectual property rights are restricted by locale.
- **Agent/Enterprise Conflicts**: IRM solutions that require local installation of software agents for enforcement purposes might not always function properly in the cloud environment, virtualization engines, or various platforms used in BYOD enterprise
- **Mapping IAM (Identity and Access Management) and IRM**: the extra layer of access control (ACLs) will cause a conflict between IRM IAM and enterprise/cloud IAM; more possible if these functions are outsourced to a third party (CASB)
- **API Conflicts**: IRM tool is often incorporated into the content, usage of material might not offer the same level of performance across different applications (content readers/media players)

IRM Functions Provided (regardless of type of content/format)

- **Persistent Protection**: follow the content it protects regardless of location, if it's duplicated or original file, or how it's being utilized
- **Dynamic Policy Control**: should allow content creators and data owners to modify ACLs and permissions for the protected data under their control
- **Automatic Expiration:** because of the nature of legal protections of intellectual property, a significant amount of digital content will not be protected in perpetuity; protection should cease when legal protections cease; licenses also expire, access and permissions for protected content should expire
- **Continuous Auditing**: allow for comprehensive monitoring of the content's use and access history
- **Replication Restrictions**: purpose of IRM is to restrict illegal or unauthorized duplication of protected content; IRM solutions should enforce restrictions across the many forms of copying that exist (screen-scraping, printing, electronic duplication, email attachments)

- **Remote Rights Revocation**: owner of rights to intellectual property should have ability to revoke rights at any time; used because of litigation/infringement

Data Control – protect data other than in the CREATE lifecycle phase; each aspect of data management (retention, audit, disposal) will need a specific policy addressing it

Data Retention Policy

- **Retention Periods**: length of time organization should keep data; data being archived for long-term storage, reduce data footprint, reduce duplicate data; not being used in production; expressed in number of years, set by regulation/legislation; can be mandated/modified by contractual agreements
- **Applicable Regulation**: can be mandated by statute/contract; policy should refer to all applicable regulatory guidance
- **Retention Formats**: contain description of how data is actually archived (type of media storage, handling specifications); Ex: some types of data are required to be encrypted while in storage, policy should include description of encryption engine, key storage and retrieval procedures, and reference to regulation(s).
- **Data Classification:** org can use classification level of data to determine how long specific datasets/types of data need to be retained
- **Archiving and Retrieval Procedures**: mandate the creation of a detailed description of the processes both for sending data into storage and recovery; usually attach to policy or mentioned by reference, usually kept separate
- **Monitoring, Maintenance, and Enforcement**: list in detail how often it will be reviewed, amended, by whom, consequences for failure to adhere to policy, and which entity is responsible for enforcement
- **Legal Hold**: supersede org's retention/destruction policies; when law enforcement/regulatory/private entity is commencing litigation against the org, they must suspend all relevant data destruction activities until fully resolved (only relevant data); concept is dictated by the Federal Rules of Evidence (HIPAA); considered temporary paramount retention period

Data Audit – org need to regularly review, inventory, and inspect usage and condition of data it owns; should have policy for conducting audits and include audit periods; scope; responsibilities (internal/external); processes/procedures; applicable regulations; monitoring, maintenance, and enforcement; audit is predicated on logging (event; security; traffic); data audit policy addresses activities that take place in all phases of the data lifecycle

Data Destruction/Disposal – because of the cloud environment, hardware destruction or overwriting storage area is nearly impossible; crypto-shredding will be the sole pragmatic option for data disposal in the cloud; must include in the policy the process for data disposal, regulations, clear directions of when data should be destroyed; addresses activities in the DESTROY phase of data lifecycle

- **Crypto-Shredding (Cryptographic Erasure):** encrypt the data with a strong encryption engine, take the keys generated and encrypt them with a different encryption engine, then destroying the resulting keys of the second round of encryption

Chapter 4 – Cloud Data Security

Data Lifecycle: Create > Store > Use > Share > Archive > Destroy

Create– defines classification levels:

- Data created remotely – data created by the user should be encrypted before uploading to the cloud; protects against MIIM attacks/insider threats at cloud data center; connection should be secure too (IPsec or TLS VPN solution)
- Data created within the cloud – should be encrypted upon creation; allows both read and process functions to be performed

Store – usually refer to near-term storage; this phase will happen when the data is created (occurs simultaneously); encryption at rest/transit should happen before this phase begin

Use – platforms used to connect to data in the cloud needs to be secure (VPN, IRM, DLP); for BYOD, a holistic approach should be used; data owners should restrict permissions; logging and audit trails are important when data are manipulated; on provider's side, strong protections should be implemented, ensure virtualized data can't be read/detected by other hosts on the same device

Share – craft sharing restrictions based on jurisdiction; limit/prevent data being sent to certain locations (export/import controls); implement some form of egress monitoring; uses content delivery networks

- Export/Import Restrictions
  - **ITAR** (International Traffic in Arms Regulations – US): State department prohibit defense-related exports (includes cryptography systems)
  - **EAR** (Export Administration Regulations – US): Department of Commerce prohibits dual-use items (technologies used for both commercial/military purposes)
  - Cryptography (Various): many countries restrict on importing cryptosystems/materials that has been encrypted
  - **The Wassenaar Arrangement:** group of 41 members have agreed to mutually inform each other about conventional military shipments to nonmember countries; not a treaty, not legally binding, may require org to notify government to stay within compliance

Archive – phase for long-term storage; cryptography is the essential consideration; key management is important, if lost, can lead to exposure or total loss; weigh in the risk of physical security (location, format, staff, procedure

Destroy – crypto shredding is the only feasible and thorough means available:

Cloud Storage Architectures

Volume Storage: customer is allocated storage space; represented as an attached drive to user's VM; can take forms of file-based/block storage/raw disk storage; includes bit splitting and erasure coding, a means of implementing data protection solutions similar to RAID arrays; often associated with IaaS; user/admin can install/run programs

- Threats: since it's a drive space, all traditional data storage threats remain; malware, deletion of data, and physical disk failure; since data is stored in the cloud, MiiM exists
- **Block Storage:** provides low latency and high-performance values; useful for structured storage; blank volume customer can put anything into; allow more flexibility and higher performance, requires greater amount of administration, installation of an OS or app to store, sort, and retrieve the data; better suited for a volume and purpose that includes data of multiple types and kinds (enterprise backup services)
- **File Storage** (File-Level Storage/File-Based Storage): data stored/displayed with a file structure in a traditional environment (files/folders) with same hierarchical and naming functions; popular with big data analytical tools/processes

Object-Based Storage: best used for large unstructured data when durability, unlimited storage, scalability, and metadata management are factors for overall performance; customers are given access to parts of the hierarchy; include actual production content, metadata describing the content/object, and unique address identifier for locating object across entire storage space; allow for significant level of description (marking, labels, classification, categorization); enhances opportunities for indexing capabilities, data policy enforcement (IRM, DLP), and centralization of data management functions; stores ***presentations, documents, audio files***; usually associated with IaaS

- Threats: object storage doesn't have a runtime environment; risk of malware is reduced but parasitical viruses can infect specific files; loss due to physical disk failure; ransomware attacks

Ephemeral Storage: temporary resource used for processing; referred to as *instance store* volumes; provided by devices directly connected to a host machine; analogous to RAM for cloud VM

- Threats: data will be lost if VM instance is shut down or physical drive fails

Long-Term Storage: durable data storage capacity; offered at low cost and large amounts; used for archiving/backups; not used for production environments or installing/running programs; can run queries and analyze data stored

- Threats: insider threat; intermediary (MiiM attacks); ransomware; vendor lock-in

SAN (Storage Area Network): dedicated high-speed network that interconnects and deliver shared pools of storage devices on multiple servers

- **iSCSI**: makes it possible to set up a shared-storage network where multiple servers and clients can access central storage resources; creates a SAN

NAS (Network Attached Storage): remote storage accessed; hosted by 3rd party service provider

Databases – provide some structure for stored data; arranged according to characteristics and elements in the data itself (trait required to file the data know, primary key); usually backend storage in the data center, accessed by users utilizing online apps/APIs through a browser; PaaS and SaaS

CDN (Content Delivery Network): used for large amounts of data that require time-sensitive communication and low latency; a form of data caching, usually near geophysical locations of high use/demand, for copies of data commonly requested by users; Ex: online multimedia streaming services, improves bandwidth and delivery quality

- Threats: intermediaries; insider threats; malware

Cloud Data Security Foundational Strategies

Key Management – how and where encryption keys are stored can affect the risk of data; keys must be secured at the same level of control (level of protection); must have key recovery (usually multiple people with access to a portion of the key); key distribution; key revocation; key escrow (copies of keys by trusted third party); outsourcing key management

- **HSM** (Hardware Security Module): device that safely store and manage encryption keys; used in servers, data transmission, and log files; far stronger than saving/storing in software

Key Protection Methods: Masking, Obfuscation, Anonymization, and Tokenization

- When to use it?: Test environments; enforcing least privilege; secure remote access
- How to perform these activities?:
    - **Randomization**: replace part/all of the data with random characters
    - **Hashing**: one-way cryptographic function to create a digest of the original data
    - **Shuffling**: using different entries from within the same data set to represent the data
    - **Masking**: hiding data with useless characters; XXX-XX-1234
        - **DDM (Dynamic Data Masking):** replace sensitive data in transit leaving original at-rest data unaltered
        - **SDM (Static Data Masking):** permanently replaces sensitive data by altering data at rest
    - **Nulls**: deleting raw data from display before represented or displaying null sets

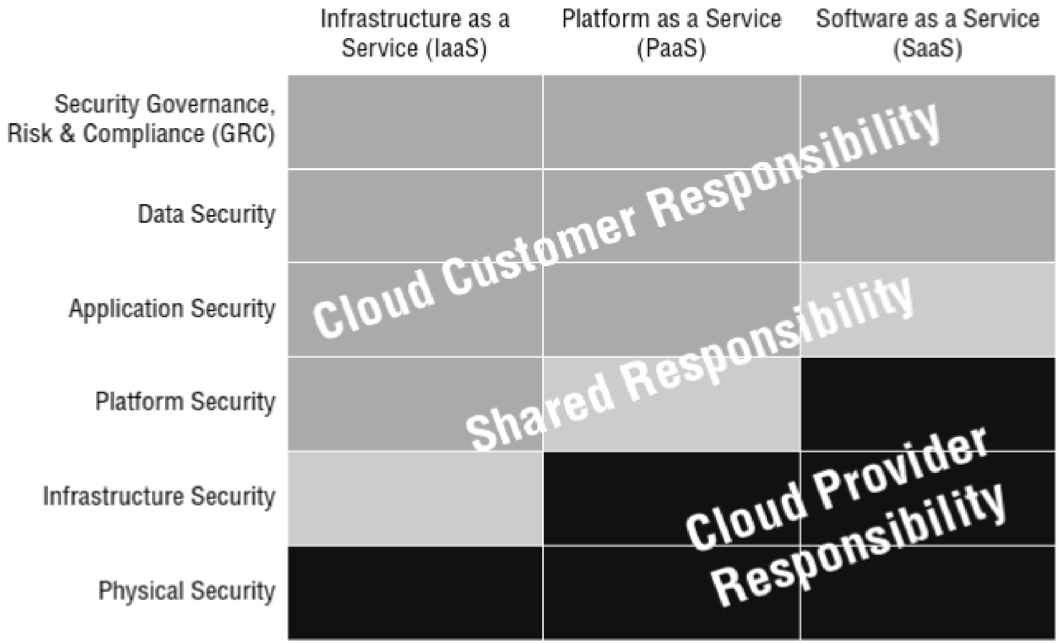
- **Obfuscation**: the application of any of the above techniques to make the data less meaningful, detailed, or readable to protect the data; can be done in static/dynamic matter
- **Anonymization** (Deidentification): can be difficult, sensitive data must be recognized and marked as sensitive when created, determining sensitivity might not be simple since data is input into open fields; mark creates metadata which can be valuable to attackers
- **Tokenization**: practice of having two distinct databases: one with live, actual sensitive data; one with nonrepresentational tokens mapped to each piece of that data; user/program is authenticated by the token server; adds significant overhead but creates extra degree of security (relieve org dependence on encryption); placing sensitive data with **unique identification symbols**; a **way of hiding or concealing sensitive data by representing it with unique identification symbols/addresses, retains essential information w/o compromising security**

SIEM (security information and event management): goals implementation of SIEM are to centralize collection of log data; enhance analysis capabilities; dashboarding; automated response

Egress Monitoring (DLP) – examining data as it leaves the production environment (DLP – data loss, leak prevention, and protection); some major goals are, additional security; policy enforcement; enhanced monitoring; regulatory compliance; can be added to IRM tools to control intellectual property

Chapter 5 – Security in the Cloud

FIGURE 5.1 Responsibilities according to service model



	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Security Governance, Risk & Compliance (GRC)	▓	▓	▓
Data Security	▓	▓	▓
Application Security	▓	▓	░
Platform Security	▓	░	█
Infrastructure Security	░	█	█
Physical Security	█	█	█

Cloud Customer Responsibility
Shared Responsibility
Cloud Provider Responsibility

Private Cloud – distributed computing environment with only one customer

- Risks: personnel threats; natural disasters; external attacks; regulatory noncompliance; malware

Community Cloud – resources are shared and dispersed among an affinity group

- Risks: resiliency through shared ownership; shared costs; no need for centralized administration for performance and monitoring

Public Cloud – offer services to any entity that wants to become a cloud customer

- Risks:
  - **Vendor Lock-In**: customer is unable to retrieve data; use portability for a level of ease when transporting data, ensure contract states so, avoid proprietary formats, check for regulatory constraints; detrimental contract terms or technical limitations
    - **Data Portability**: used to avoid lock-in; the ease of moving data from cloud provider to another
  - **Vendor Lock-Out**: provider goes out of business, bought out by another business, or ceases operation

Hypervisor:

- **Type 1**: also called bare-metal/hardware hypervisor; resides on host machine as bootable software
- **Type 2**: software hypervisor; runs on top of the OS that runs on a host device
- **Guest Escape / VM Escape**: allow a user to leave their own virtualized instance; user will be able to access other virtualized instances on the same host, view, copy, or modify data stored, access host itself affecting all instances on the machine
    - **Host Escape**: user can leave the host machine, accessing other devices on the network
- **VMI** (Virtual Machine Introspection): agentless means of ensuring VM's security baseline does not change by examining the physical address, network settings, and installed OS
- **NFV (Network Functions Virtualization)**: replacement of network appliance hardware with VMs; uses a hypervisor to run networking software and processes such as routing and load balancing

SDN (Software Defined Networking): approach to networking that uses software-based controllers or APIs to communicate with underlying hardware infrastructure and direct traffic on a network; allow network admins to perform the following:

- Reroute traffic based on current customer demand
- Create logical subnets without having to change any actual physical connections
- Filter access to resources based on specific rules or settings

Chapter 6 – Responsibilities in the Cloud

- **SOC** reports: part of the SSAE reporting format by the AICPA; recognized as being acceptable for regulatory purposes, specifically designed for SOX
    - **SOC 1**: reports for the auditing of financial reporting instruments of a corporation; there are 2 subclasses (Type 1 and Type 2)
    - **SOC 2**: report audits of any controls on an org's security, availability, processing integrity, confidentiality, and privacy
        - **Type 1**: not useful for determining security and trust of an org; only reviews the design of controls, not how they are implemented / maintained / functioned
        - **Type 2**: useful for getting true assessment of org's security posture; extremely detail, usually not shared unless NDA is signed
    - **SOC 3**: reports designed to be shared with the public; "seal of approval"; has no data about the security controls, an assertion the audit was conducted and passed

Chapter 7 – Cloud Application Security

- **Forklifting**: moving an entire application to the cloud without significant changes; often self-contained stand-alone applications
- **Cloud-Secure SDLC** (Software Development Lifecycle):
    - **Defining**: during this phase, the focus is to identify the business requirements of the application (accounting, database, or customer relationship management); describe aspects of the business needs; do not choose tools/technologies at this phase
    - **Designing**: this phase begins to develop user stories (what user want to accomplish and how to do it), what the interface will look like, and will it require use/development of any APIs
    - **Development**: phase where the code is written
    - **Testing**: activities of initial penetration testing and vulnerability scanning against the application; use techniques/tools for both DAST (Dynamic application security testing) and SAST (static); at least two types of tests take place, functional and security testing
        - **Functional testing**: ensures the software performs whatever tasks it was intended for, completely and accurately, in a manner resistant to loss/interruption
        - **Security testing**: ensures whatever controls were included in the software are working effectively and accomplishing their purpose
    - **Secure Operations**: phase begins when thorough testing is complete and environment is secure
    - **Disposal**: when software reaches end of life or replaced by newer application, it must be securely disposed
- **QA** (Quality Assurance): management/inspection to reduce possibility of introducing errors or harming the end product
- **ISO/IEC 27034-1 Standards for Secure Application Development**: created an approach orgs can use for tracking security controls used in software; provides overview of application security that introduces definitive concepts, principles, and processes; describes two documents, ONF and ANFs
    - **ONF** (Organizational Normative Framework): framework for all components of application security controls and best practices cataloged and leveraged by the org
    - **ANF** (Application Normative Framework): subsets of ONF for each specific application; shares the applicable parts of the ONF needed to achieve an application's required level of security and level of trust desired
    - ANF-to-ONF relationship is one-to-one, every application has an ANF that maps back to the ONF; ONF-to-ANF relationship is one-to-many, ONF has many ANFs, but AND has only one ONF
- **IAM** (Identity and Access Management): about the people, processes, and procedures used to create, manage, and destroy identities

- **Identity Management**: process where individuals are given access to system resources by associating user rights with a given identity
    - **Provisioning**: first phase of IM; each subject is issued a unique identity assertion (ex: user ID); during the process, user is given a password to authenticate the identity assertion
- **Access Managemen**t: part of the process that deals with controlling access to resources once they have been granted; identifies who a user is and what they are allowed to access, accomplished through authentication, authorization, policy management, federation, and identity repositories
- Identity Repositories: store of information or attributes of identities
- Directory Services: how identities and attributes are managed; X.500 and LDAP; Microsoft AD; Novell eDirectory; Metadata replication and synchronization
- **Federated Identity Management (Federation):** used to manage identities across disparate orgs; a SSO for multiple orgs; two types of federation; web of trust and use of 3rd party identifier (CASB)
    - **Web of Trust Model**: each member of the federation has to review and approve each other member for inclusion; doesn't scale well, can be costly
    - In a trusted third-party model of federation (CASB), each member organization outsources the review and approval task to a third party they all trust. This makes the third party the ***identifier*** (it issues and manages identities for all users in all organizations in the federation), and the various member organizations are the ***relying parties*** (the resource providers that share resources based on approval from the third party).
- **SAML** (Security Assertion Markup Language): a federation standard; XML-based and consists of a framework for communication authentication, authorization or entitlement information, and attribute information across orgs; a means for users from outside orgs to be verified as authorized users
    - **SAML 2.0**: standard used to pass security assertions across the internet (user IDs and authenticating credentials)
- **WS-Federation**: uses the term realms in explaining its capabilities to allow orgs to trust each other's identity information across orgs
- **OAuth**: used in authorization with mobile apps; provides 3rd party applications limited access to HTTP services
- **OpenID Connect**: interoperable authentication protocol based on OAuth 2 specification; allows developers to authenticate users across websites and applications without having to manage us/pw
- **Stateful Packet Inspection**: allow firewalls to prevent inbound traffic from entering unless connection has been initiated from inside the network
- **WAFs (Web Application Firewall)**: deployed in addition to network firewall; protect specific web-based applications like PCI DSS; can protect against DoS/DDoS attacks; function at Layer 7 in OSI model

    - **DAM (Database Activity Monitoring)**: protects the DB from unusual requests or activity; can be agent (host)/network based; function at Layer 7 in OSI model
    - **API Gateways**: impose controls as an API proxy to not directly expose the API; implement access control; limit connections for bandwidth to be available for all applications (helps with internal DoS attack); API logging; gathering metrics from access logs; additional API security filtering; function at Layer 7 in OSI model
    - **XML Gateway**: works around how sensitive data and services are exposed to APIs; software/hardware based and can implement types of DLPs
    - **XACML (eXtensible Access Control Markup Language)**: attribute-based access control policy language or XML-based language, designed to express security policies and access requests to information; can be used for web services, digital rights management, enterprise security applications
- **APIs (Application Programming Interface)**: coding components that allow applications to communicate through web interface in a safe and secure manner; two types of APIs in cloud-based applications
    - **RESTful APIs (Representational State Transfer)**: relies on stateless, client-server, cacheable communications. It is a software architecture consisting of guidelines and best practices for creating scalable web service
        - Characteristics: low processing; uses simple URLs/URIs; not reliant on a single programming language; scalable; offers outputs in many formats (CVS, JSON); efficient
        - Situations where REST works well: when bandwidth is limited; stateless operations are used; caching is needed
        - **SCIM (System for Cross-domain Identity Management)**: open standard designed to manage user identity information; provides a defined schema for representing users and groups, and a RESTful API to run CRUD operations on those user and group resources
    - **SOAP (Simple Object Access Protocol)**: protocol specification providing for the exchange of structured information or data in web services; works over other protocols like SMTP, FTP, and HTTP
        - Characteristics: standards-based; reliant on XML; highly intolerant of errors; slower; built-in error handling; more accurate
        - Situations where SOAP works well: asynchronous processing; format contracts; stateful operations
    - **SDK (Software Developmental Kits)**: collection of software development tools in one installable package; facilitate creation of applications by having a compiler, debugger, and software framework; kit that facilitates usages of an API
- **TLS (Transport Layer Security)**: protocol to ensure privacy when communication between applications, servers, or client
- **SSL (Secure Socket Layer)**: same use as TLS, replaced by TLS
- **Whole-Instance Encryption (Whole-Disk)**: encrypt all system’s data at rest in one instance

- **STRIDE Model**: standardized way of describing threats by their attributes; Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of Privilege
- **CSRF (Cross-Site Request Forgery)**: manipulates a logged-on user's browser to send a forged HTTP request along with cookies to force the victim's browser to generate a request that a vulnerable application thinks is a legitimate request from the user
- **White-Box Testing SAST (Static Application Security Testing)**: reviewing the source code
- **Black-Box Testing DAST (Dynamic)**: testing the program as it functions in runtime; source code is not reviewed; team use inputs and results of application itself as it's running
- **Application Orchestration**: when two or more applications must interact in order to successfully complete a business process/transaction; two approaches we can take:
    - Link elements of the applications directly, so out of one is input of another; can lead to additional problems; creating unnecessary dependencies, increasing difficulty of version control, testing
    - Abstract the functions of the applications so input/output can be handled distinctly from the way the programs work; often with another code/software; preferable option; known as application orchestration
- **Authentication**: confirms the identity assertion belongs to the entity presenting it

Chapter 8 – Operations Elements

- Industry service standard for uptime is *five nines* (99.999%), less than 6 downtime minutes a year
- **Conditioning**: involves adjusting the voltage on the line; includes surge protectors
- **Uptime Institute (UI)**: advisory org to publish standards related to data center redundancy in pursuit of continuous operations, matters related to IT services, and certifies data centers for compliance
    - **Tier 1**: simplistic with little to no redundancy and labeled *Basic Site Infrastructure*; lists minimum requirements for a data center; dedicated space for IT systems, UPS system for line conditioning and backup purposes, sufficient cooling systems to serve all critical equipment, power generator for extended electrical outages with at least 12 hours of fuel to run the generator; useful for orgs to use as a backup, private cloud, cheaper to operate, a hot/warm/cold site
    - **Tier 2**: named *Redundant Site Infrastructure Capacity Components*; good for orgs looking to operate in the public cloud environment and maintaining low overhead
    - **Tier 3**: known as *Concurrently Maintainable Site Infrastructure*; has added benefit of multiple distribution paths; there are dual power supplied for all IT systems; critical operations can continue even if any single component is out of service

  - **Tier 4**: *Fault-Tolerant Site Infrastructure* is premium data center offering; redundancy in both IT and electrical components; facility will feature automatic response capabilities for infrastructure control systems
- **TPM (Trusted Platform Module)**: specialized chip on a computer designed to secure hardware with integrated cryptographic keys; helps prove user's identity and authenticate devices; provide security against firmware and ransomware attacks
- **Tightly Couped Cluster Storage**: all storage devices are directly connected to a shared physical backplane; confined to restrictive design parameters; enhance performance as it scales
- **Loosely Coupled Cluster**: allow greater flexibility; each node of the cluster is independent; logically connected and do not share same proximate physical framework

Resiliency: two general ways for disk data protection in a cloud storage cluster: RAID and data dispersion

- **RAID** (Redundant Array of Independent Disks): all data is stored across various disks known as *striping*; allows data to be recovered if one drive fails; in some schemes (0-10) parity bits are added to raw data to aid in recovery after a drive failure
- **Data Dispersion**: data is sliced into chunks (shards) that are encrypted with parity bits (erasure coding in cloud data dispersion) and written to various drives in the cloud cluster; the parity bits/erasure coding allows recovery of partial data lost by recreating the lost data from remaining data plus parity bits/erasure code; can be seen equivalent to RAID array in a cloud environment; often referred to as *bit splitting;* uses parity bits, data chunks, and encryption
- **SSMS** (Secret Sharing Made Short): method of bit splitting using 3 phases: encryption, using information dispersal algorithm, and splitting encryption key using secret sharing algorithm; fragments are signed and distributed to different cloud storage services

Chapter 9 – Operations Management

- **OS Logging**: integral toolsets for monitoring performance and events; set OS logs to alert admins when usage approaches a level of capacity utilization, performance degradation, CPU usage, memory usage, disk space, disk I/O timing (slow writing/reading to/from disk)
- **ASHRAE** Recommended Range for data centers:
  - Temperature: 64-81 degrees F
  - Humidity: Dew point 42-59 degrees F; 60% relative humidity
- **Maintenance Mode:** all operational instances are removed from the system/device before entering this mode; prevent all new logins; ensure logging is continued; begin enhanced logging
- **CI/CD** (Continuous Integration/Continuous Delivery): incorporates heavy use of automation to shorten software delivery pipeline; includes administrative and technical controls

- **ISO/IEC 20000-1, Information technology** – Service Management: defines a set of operational controls and standards orgs can use to manage IT services; used to manage ITSM using approaches of ITIL and ISACA COBIT framework
    - **ITSM (IT Service Management)**: goal is to identify user needs, design IT service to meet those needs, deploy it, then enter a cycle of continuous improvements
- **BC/DR (Business Continuity and Disaster Recovery)**:
    - **Business continuity** efforts are concerned with maintaining critical operations
    - **Disaster Recovery** efforts are focused on resumption of operations due to disaster
    - **Event**: unscheduled impact to operating environment; impact lasts three days or less, disasters last longer, an event can become a disaster
    - The most important planning and efforts is health and human safety; notification, evacuation, protection, and egress will need to be prioritized
    - **MAD (Maximum Allowable Downtime)**: how long an interruption will stop operations; referred to as MTD (maximum tolerable downtime)
        - **MTTR (mean time to repair)**: average amount of time it takes to repair a system/device that is down
    - **RTO (Recovery Time Objective)**: BC/DR goal for recovery of operation, measured in time; must be less than the MAD
    - **RPO (Recovery Point Objective)**: BC/DR goal for limiting loss of data from unplanned event, measured in time; example – org resumes critical operations at alternate operating site with last full backup (if they backup every day, RPO will be 24 hours), RPO for org will be loss of no more than one day's worth of data; tolerable/acceptable amount of data that might be lost due to an outage before severe consequences are experienced.
    - **RSL % (Recovery Service Level)**:
    - **ALE (Annual Loss Expectancy)**: amount an org should expect to lose annually based on any one type of incident; ARO x SLE = ALE
        - **ARO (Annual Rate of Occurrence)**: rate of occurrence of a specific event/incident
        - **SLE (Single Loss Expectancy)**: amount of expected damage/loss from any single specific security incident
    - UPS should last long enough for graceful shutdown of affected system, can provide line conditioning, adjusting power to optimize for the devices it serves and smooth power fluctuations; battery backup should only be relied on to provide immediate and near-term power supply; longer power supply should be provided by generators (short-term contingency)
        - Generators: supply close to immediate power when utility electricity is interrupted and have automatic transfer switches (not a viable replacement for an UPS); minimum of 12 hours of fuel for all generators
    - Testing:

- **Tabletop Testing**: essential participants work together at a scheduled time; InfoSec equivalent of role-playing games; least impact on production of testing alternatives
- **Dry Run**: whole org takes part in a scenario at a scheduled time; impacts productivity
- **Full Test**: entire org takes part in an unscheduled, unannounced practice scenario, performing full BC/DR activities; includes system failover, facility evacuation, used for detecting shortcomings in the plan; greatest impact on productivity

Chapter 10 – Legal and Compliance Part I

- **Criminal Law**: all legal matters where the government is in conflict with person, group, or org that violates statutes (state and federal legislated by lawmakers); includes federal court system; punishments can be monetary fines, imprisonment, death; enforcement is called prosecution
- **State Laws**: laws enacted by a state legislature; federal laws supersede this
- **Federal Laws**: laws that affect the entire country; issues of jurisdiction and prosecution are negotiated between law enforcement and course prior to prosecution
- **Civil Law**: body of law, statutes, and so on that deals with personal and community-based law such as marriage/divorce; set of rules that govern private citizens and disputes; parties involved are strictly private entities; cases are called lawsuits/litigations; has restitution of monetary damages or perform actions but not imprisonment
- **Contracts**: agreement between parties; in a breach of contract, a party within the agreement can sue to get court-ordered relief in money or other considerations (property or other agreements made before); SLAs / PCI DSS contracts
- **Common Law**: existing set of rulings/decisions made by courts, informed by cultural mores and legislation; this creates precedents, each party will cite in course as means to sway the court
- **Administrative Law**: laws not created by legislatures but by executive decisions and function; federal agencies can create, monitor, and enforce their own administrative law

US Laws:

- **ECPA (Electronic Communication Privacy Act)**: laws restricting government from putting wiretaps on phone calls and electronic communication in the form of data
- **GLBA (Graham-Leach-Bliley Act)**: aka *Financial Services Modernization Act of 1999*; allow banks to merge with insurance companies and financial institutions; customer

account information is kept secure and private; customers may opt out of any information-sharing arrangements from bank/insurer

- **SOX (Sarbanes-Oxley Act)**: transparency in publicly traded corporation's financial activities; includes provisions for securing data and expressly names the traits of CIA; US legislation enacted to protect shareholders and the public from enterprise accounting errors and fraudulent practices
- **HIPAA (Health Insurance Portability and Accountability Act)**: protect patient records and data; known as ePHI
- **FERPA (Family Educational Rights and Privacy Act)**: prevent academic institutions from sharing student data with anyone other than parents or students (after age 18)
- **DMCA (Digital Millennium Copyright Act)**: provisions to protect owned data; cracking of access controls on copyrighted media a crime and enables holders to require any site to remove content
- **CLOUD Act (Clarifying Lawful Overseas Use of Data)**: allows US law enforcement and courts to compel American companies to disclose data stored in foreign data centers
- **FedRAMP**: not a law, but a US federal program that mandates standardized approach to security assessments, authorization, and continuous monitoring of cloud products/services; FedRAMP certification is required for cloud hosting services provided to a US government agency or contractor

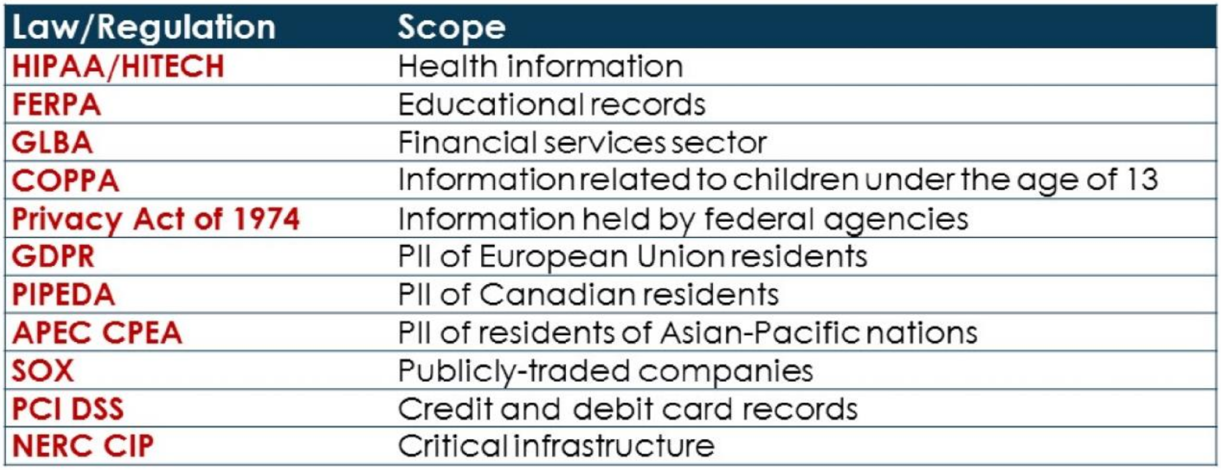
PII:

- **Direct Indicators**: data elements that immediately reveal a specific individual; mobile phone number, IP address, SSN, birthday, home address, name; depends on jurisdiction
- **Indirect Indicators**: characteristics/traits of an individual can reveal the identity of a person; not sensitive data but collect enough of it will reveal a person; location, birthplace, pets, industry, etc. Ex: a man born in Wisconsin, living in New Orleans, owns a dog, works in security
- **Anonymization**: removing identifiers; certain jurisdictions, laws, and standards require this for both indirect/direct identifiers

- Federal PII law that complies with the EU Privacy Regulation: The EU, Australia, and New Zealand, Argentina, EFTA (Switzerland, Norway, Iceland, Lichtenstein), Israel, Japan, Canada; The USA does ***NOT***; USA has an opt-out approach and EU has opt-in
  - **GDPR (General Data Protection Regulation)**: the EU's has the most significant and powerful privacy law in the world; describes handling of personal/private information of all EU citizens; codifies 7 principles:
    - Notice: individual must be informed about PII being gathered or created
    - Choice: individual can choose to disclose PII; need explicit agreement

  - Purpose: individual must be told specific use of information
  - Access: individual is allowed copies of PII
  - Integrity: individual is allowed to correct information
  - Security: entity holding PII is responsible for protecting PII and liable
  - Enforcement: entities holding PII understand they are subject to enforcement actions by EU authorities
  - **Privacy Shield**: program for American companies to comply with GDPR within the EU; voluntarily agree to comply; administered by the DoC (Department of Commerce) a federal enforcement entity in the US; companies must agree to auditing and enforcement with fines assessed for violations
  - **Data Subject**: individual whom PII refers; human being
  - **Data Controller**: entity collecting/creating PII; the cloud customer; responsible for any unauthorized disclosure of PII (with GDPR) regardless of fault
  - **Data Processor**: entity acting on behalf of data controller; performing any manipulation, storage, or transmission of PII; cloud service provider
  - **Cloud Carrier**: intermediary who provides connectivity and transport of cloud services between cloud providers and cloud consumers
  - Australian Privacy Act of 1988; Canada's PIPEDA (Personal Information Protection and Electronic Documents Act); EFTA and Switzerland; APEC (Asia-Pacific Economic Cooperation) Privacy Framework
- **ISMSs** (Information Security Management Systems): holistic overview of the entire security program within an org; detailed in ISO **27001**; provides a standardized international model for development and implementation of policies, procedures, and standards in a top-down approach in addressing and managing risk in an org
- **ISO/IEC 27017: 2015**: set of standards regarding the guidelines for information security controls applicable to the provision and use of cloud services and customers; standard for providing cloud services and how customer information/privacy should be controlled
  - **ISO/IEC 27018: 2019**: focuses on code of practice and security techniques for processing PII in cloud services
- **Laws**: legal rules created by government entities/legislatures
- **Regulations**: rules created by governmental agencies
- **Standards**: dictate reasonable level of performance; created by an org (internal) or industry bodies/trade groups (external); following standards can reduce liability and compliance represents due care
- **eDiscovery**: process of identifying and obtaining electronic evidence for prosecutorial or litigation purposes; ISO 27050 is the industry standard and guidance
- ISO Global Digital Forensic Standards:
  - ISO/IEC **27037**: 2012: guide for collecting, identifying, and preserving electronic evidence
  - ISO/IEC **27041**: 2015: guide for incident investigation

  - ISO/IEC **27042**: 2015: guide for digital evidence analysis
  - ISO/IEC **27043**: 2015: incident investigation principles and processes
  - ISO/IEC **27050**-1: 2016: overview and principles for eDiscovery



Law/Regulation	Scope
HIPAA/HITECH	Health information
FERPA	Educational records
GLBA	Financial services sector
COPPA	Information related to children under the age of 13
Privacy Act of 1974	Information held by federal agencies
GDPR	PII of European Union residents
PIPEDA	PII of Canadian residents
APEC CPEA	PII of residents of Asian-Pacific nations
SOX	Publicly-traded companies
PCI DSS	Credit and debit card records
NERC CIP	Critical infrastructure

Chapter 11 – Legal and Compliance Part II

- **KRIs (Key Risk Indicators)**: metrics used by an org to inform management of impending negative impact to operations; involves algorithms and rating systems ascribed to factors selected by analysts and management for an early-warning system; *forward-looking*, helps an org understand risks/events already occurred and impacted the business
  - **KPIs (Key Performance Indicators)**: backward-looking; metrics to gauge business critical initiatives, objectives, or goals; measurable benchmarks against defined goals
- **Risk Appetite/Tolerance**: how the org views risks; senior management dictates the amount of risk an org is willing to take
- **Risk Profiles**: comprehensive analysis of the possible risks to the org; include a survey of various operations the org is engaged in, public perception, pending legislation, stability of countries where org operates
- **Physical Controls**: physical access to assets that reduces the impact of a physical event; locks, fire suppression, fences, guards
- **Technical Controls**: aka logical controls; controls that enhance the CIA triad; encryption, ACLs, audit trails, logs
- **Administrative Controls**: processes and activities that provide aspects of security; background checks, scheduled log reviews, mandatory vacations, robust/comprehensive security policies/procedures, designing business processes
- **Risk Management Framework (RMF)**:

  - **ISO 31000: 2018**: international standard focusing on design, implementing, and reviewing risk management processes and practices
  - **NIST SP 800-37 (Guide for Implementing the RMF)**: a methodology for handing all organizational risk in a holistic, comprehensive, and continual manner; relies on automated solutions
  - **ENISA (EU Agency for Network and Information Security)**: EU counterpart to NIST; standard and model developed in EU; responsible for producing Cloud Computing: Benefits, Risks, and Recommendations for Information Security; identifies top eight security risks based on likelihood and impact
  - **COBIT**
  - **ISO/IEC 31010: 2009**: RM techniques
- **Risk Management Metrics**:
  - 5 – Critical; 4 – High; 3 – Moderate; 2 – Low; 1 – Minimal
- **ISO/IEC 15408-1: 2009 (Common Criteria Assurance Framework)**: provide assurances for security claims by vendors; assurance for security products customers purchase have been thoroughly tested by 3rd party testers and meets requirements
- **ISO 28000: 2007**: applies to security controls in supply chains
- **CSA STAR (Security, Trust, and Assurance Registry)**: single consistent framework for evaluating cloud providers; registry of security controls provided; designed for users to assess cloud providers, security providers, and advisory and assessment service firms as part of their vendor management due diligence while choosing providers
  - **CCM (Cloud Controls Matrix)**: list of security controls and principles appropriate for cloud environment, cross-referenced to other control frameworks (COBIT, ISO, NIST, FedRAMP, PIPEDA); aids in selecting/implementing appropriate controls for regulatory frameworks; an inventory of cloud service security controls that are arranged into separate security domains
  - **CAIQ (Consensus Assessments Initiative Questionnaire)**: self-assessment by cloud providers, detailing evaluation of practice areas and control groups
  - **CSA STAR Program** – Open Certification Framework:
    - Level One: Self-Assessment: requires release and publication of due diligence assessment against CSA's CAIQ/CCM
    - Level Two: CSA STAR Attestation: requires release and publication of available results of assessment from 3rd party based on CSA CCM and ISO 27001: 2013 or AICPA SOC 2
    - Level Three: CSA STAR Continuous Monitoring: requires release and publication of results of continuous monitoring by certified 3rd party

ETC:

- **PKI**: framework of programs, procedures, communication protocols, and public key cryptography that enables a diverse group of individuals to communicate securely

- **OWASP (Open Web Application Security Project)**: an international nonprofit that focuses on identifying software vulnerabilities and educating developers in the practice of secure coding
    - Broken Access Control; Cryptographic Failures; Injection; Insecure Design; Security Misconfiguration; Vulnerable and Outdated Components; Identification and Authentication Failures; Software and Data Integrity Failures; Security Logging and Monitoring Failures; Sever-Side Request Forgery (SSRF)
- Joint Operating Agreements: provide nearby relocation sites so disruption is limited to the org's own facility/campus and can be addressed at a different location
- OSI Model: Physical; Data Link; Network; Transport; Session; Presentation; Application (Please Do Not Throw Sausage Pizza Away)
- SSO: allows a user to access multiple *applications* with a single set of credentials for authentication and authorization
- **Cross-Certification Model**: every participating org has to review and approve every other org; does not scale well
- **FPE (Format-Preserving Encryption)**: technique used to scramble contents of data using mathematical algorithm *while keeping the structural arrangement of the data*
- Logging Levels: OFF > FATAL > ERROR > WARN > INFO > DEBUG > TRACE > ALL
    - OFF: used to turn off logging
    - FATAL: application is about to stop a serious problem/corruption; the situation is catastrophic; application is unable to connect to the data store
    - ERROR: inability to access a service/file; failure of something important in the application; when a severe issue is stopping functions within the application from operating efficiently, will continue to run but will need to be addressed
    - WARN: detected an unexpected application problem
    - INFO: normal behavior of applications
    - DEBUG: diagnostic information in a detailed manner; fetch information to diagnose, troubleshoot, or test an application
    - TRACE: captures all details about behavior of application; used when you need to see events within application and what happened in 3rd party libraries; use to query parameters in the code or interpret algorithm's steps
    - ALL: shows all or customed logged defined
- **Management Plane**: technology that allows an admin to remotely manage a fleet of servers; logical infrastructure design used to configure cloud resources; launching VMs or configuring virtual networks
- **Information Commissioner**: responsible for enforcing UK's GDPR and offering advice and assistance to both the council and individual groups whose information is being held
- **NIS Directive** (EU2016/1148): first piece of EU-wide cybersecurity legislation; must notify competent authorities or CSIRT
- **NIST 800-145**: The NIST definition of Cloud Computing; a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources

(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- **NIST 800-146**: document 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.
- **Functional requirements**: Those performance aspects of a device, process, or employee that are necessary for the business task to be accomplished. Example: A salesperson in the field must be able to connect to the organization's network remotely.
- **Nonfunctional requirements**: Those aspects of a device, process, or employee that are not necessary for accomplishing a business task but are desired or expected. Example: The salesperson's remote connection must be secure
- **DFD (Data Flow Diagrams):** useful in systems/software engineering to establish functional requirements before selection of technology takes place
- **Eucalyptus**: computer software building AWS-compatible private/hybrid cloud computing environment; multitenancy
- **ISO/IEC 17788**: overview of cloud computing and a set of terms and definitions
- **NIST 500-292**: adoption of cloud computing into the Federal Government
- **Metastructure**: protocols and mechanisms that provide the interface between the infrastructure layer and other layers; the glue that ties technologies between management and configuration
- **PRE (Proxy Re-Encryption)**: allows a proxy (3rd party) to convert a ciphertext encrypted under one key into an encryption of the same message under another key; place as little trust and reveal as little information to the proxy to allow it to perform its translations
- **Software-Defined Infrastructure**: technical computing infrastructure entirely under the control of software with no operator or human intervention
- **Chaos Engineering**: method of testing software that deliberately introduces failure and faulty scenarios to verify resilience
- **Microsoft's (SDL) Security Development Lifecycle**: software development process based on the spiral model; help developers create applications/software while reducing security issues, resolving security vulnerabilities, and reducing development and maintenance costs; training, requirements, design, implementation, verification, release, response
- NIST 800-92: log management
- NIST 800-40: enterprise patch management planning
- **Backup Types**:
    - Full
    - Copy
    - **Differential**: all data changed since last full backup; if a full back up was done on a Sunday, a differential backup will be done on Monday for only the files that changed since Sunday, Tuesday you back up only files that changed since Sunday (adding);

quicker than a full backup but storage space will be used until another full back up is done

- **Incremental**: backs up data that changed since last backup; time consuming to restore data

Laws, Regs, Orgs

(ISC)2 -: International Information System Security Certification Consortium: A security certification granting organization that has a long history of certifications that were difficult to get. This difficulty has made their certificates seen as having higher value in the industry.

(ISC)2 Cloud Secure Data Life Cycle: Based on CSA Guidance.: : : : : : : 1. **Create**; 2. **Store**; 3. **Use**; 4. **Share**; 5. **Archive**; 6. **Destroy**.:

(SAS) 70: Statement on Auditing Standards (SAS) No. 70 was a recognized standard of the American Institute of Certified Public Accountants (AICPA) in response to the issues that also lead to Sarbanes-Oxley (SOX). Deprecated in 2011 by the Statement on Standards for Attestation Engagements (**SSAE) No. 16**.

AICPA -- American Institute of Certified Public Accountants which established SAS 70 and later SAAE 16.

Application Normative Framework (ANF), **Organizational Normative Framework** (ONF) are concepts of ISO 27034.: There is only one ONF for an organization but potentially as many ANF's as applications.

ASHRAE - American Society of Heating, Refrigerating and Air-Conditioning Engineers is an American professional association seeking to advance heating, ventilation, air conditioning and refrigeration systems design and construction.:

Biba - an access control model designed to preserve data integrity.: It has 3 goals.: Maintain internal and external consistency; prevent unauthorized data modification even by authorized parties; prevent data modification by unauthorized individuals.

Capability Maturity Model (CMM) is a development model where the maturity relates to the formality and optimization of processes.: When applied to cloud security it would focus on those aspects as they relate to cloud security.

Child Online Protection Act (COPA) - An attempt to restrict access by minors to material defined as harmful to minors. A permanent injunction against the law in 2009.

Cloud Access Security Brokers (CASBs) monitors network activity between users and cloud applications and enforces security policy and blocking malware.

Cloud Security Alliance (CSA) publishes the **Notorious Nine**: 1) Data breaches; 2) Data Loss; 3) Account service traffic hijacking; 4) Insecure Interfaces and APIs; 5) Denial of Service; 6) Malicious Insiders; 7) Abuse of Cloud Services; 8) Insufficient Due Diligence; 9) Shared technology Vulnerabilities. There are also implications and controls associated with each.

Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) or **CSA STAR** -- uses the Consensus Assessments Initiative Questionnaire (CAIQ),: Cloud Controls Matrix (CCM), and GDPR Self-Assessment as inputs to certify an organization to Level 1.: Level 2 integrates the CSA Cloud Controls Matrix and the AICPA Trust Service Principles - AT 101 for STAR attestation.: STAR Certification for level to uses the CSA Cloud Controls Matrix and the requirements of the ISO/IEC 27001: 2013 management system standard together with the CSA Cloud Controls Matrix. Certification certificates follow normal ISO/IEC 27001 protocol for a 3rd party assessment: : :

Cloud Security Alliance Cloud Controls Matrix (CSA CCM): Composed of 17 domains covering key elements of cloud.: It contains 170 objectives within the domains.: They integrate with the STAR program**.**

COBIT: or Control Objectives for Information and Related Technologies is a framework for IT governance and management.: Initially used to achieve compliance with Sarbanes-Oxley and focused on IT controls.: Since 2019 the emphasis has shifted to information governance. It is focused on these 5: principles: : 1: Meeting Stakeholder Needs;: 2: Covering the Enterprise End-to-End; 3: Applying a Single Integrated Framework; 4: Enabling a Holistic Approach; and 5: Separating Governance from Management.

Common Criteria and the EAL rating: : An EAL rating is assigned to an IT product after it has been evaluated by an independent lab.: The level indicates the degree and type of testing with 1 the least and 7 the most.: Common criteria contain 60 functional requirements in 11 classes and is an accepted standard among the military organizations of the US and many allies.

Consensus Assessments Initiative Questionnaire (CAIQ): is an initiative of the Cloud Security Alliance to provide an industry-accepted documentation of security controls and as of 2020 is combined with the Cloud Controls Matrix.: They can be used as evidence for entry to the CSA STAR registry.

Digital Millennium Copyright Act (DMCA): -- and occasionally controversial act intended to align the US copyright act with the requirements of treaties and the World Intellectual Property Organization.:

DLP: -- Data Los Prevention is ensured by a set of tools, procedures, and policy to ensure sensitive, proprietary, and PII is not lost or misused.: It helps to provide compliance with numerous laws and compliance requirements by enforcing preventative and detective measures in the organization.

ENISA: - European Union Agency for Cybersecurity is a Cyber Security awareness association that provides support, information, and collaboration on security issues.: They also publish a top x threats each year.: The last few years they have included 15 threats each year.

EU Data Directive: regulates the processing of PII in the EU.: Since it is a directive, each country must pass the laws that establish how each country will enforce the directive.: It includes the 7 principles governing the OECD's recommendations for protection of personal data.**:**

Eurocloud Star Audit Certification (ESAC) is nonprofit organization that maintains information security standards or best practices and provides assessments and certification of compliance.

European Union Agency for Network and Information Security (ENISA): see ENISA above.

Family Education Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. It applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Federal Information Processing Standard (FIPS) 140-2 is mandatory for all US government, military, contractors doing business with the government and regulated industries such as financial and health-care institutions.: IT is being succeeded by FIPS 140-3.: FIPS 140-2 has four levels with 1 being the lowest level of security through 4 as the highest.: Testing under FIPS 140-2 is done by 23 accredited Cryptographic Module Testing laboratories.

Federal Information Systems Management Act (FISMA) is a US law that makes mandatory requirements for federal agencies to develop, document, and implement management cyber security.: NIST plays a major role in implementing FISMA and has promulgated numerous security standards and guidelines.**:** One key guideline is the Risk Management Framework (RMF).: Office of Management and Budget (OMB) monitors compliance with NIST programs.

Fiber Channel: : is a data transfer protocol used to connect servers to Storage Area Networks (SAN) in data centers.: It typically runs on fiber optic cables but can also run on copper.: Data rates range from 1 to 128 gigabit/sec.

Fiber Channel over Ethernet (FCoE): : encapsulates Fiber Channel frames over Ethernet networks.: This technology can support speeds of up to: 10Gigabit/sec.: Using FCoE can allow network and storage traffic to connect using a wider range of networks and storage devices.

FIPS 140-2: Used for protecting sensitive but unclassified information by the federal government.: The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4.: The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography-based standards such as CMVP. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries.:

GDPR – General Data Protection Regulation gives individuals control over their personal data.: It also simplified regulation by forcing all member states to comply with a single regulation.: GDPR specifies rights of the data subject, including access rectification, erasure, object to use of PII.: It poses requirements on data controllers and data processors.**:**

Generally Accepted Privacy Principles described by the AICPA (GAPP): The generally accepted principles and practices (GAPP), were agreed upon by 23 countries in response to investors and regulators concerned about transparency, independence, and governance of the accounting industry.: It was based on 24 principles in the areas of legal, institutional, and investment and risk.

Gramm-Leach-Bliley Act (GLBA): requires companies that offer financial products or services to safeguard sensitive data about customers and inform the customers of those requirements.

Health Insurance Portability and Accountability Act (HIPAA) modernized healthcare information and stipulated how PII kept by healthcare and healthcare insurance industries should be protected.: The act was vague: **:**

HITECH act motivated the implementation of electronic health records (HER) and the supporting technology. Some penalties for non-compliance of HIPAA were increased under HITEC, as well as establishing breach notification to impacted patients.:

IDCA or **International Data Center Authority** is attempting to be "the ultimate standardization, education, and certification body for the Application Ecosystem and its supporting digital infrastructure, helps deliver comprehensive, effective, up-to-date and uniquely innovative data compliance audits. The Application Ecosystem and digital infrastructure audits.": Auditors certified by IDCA will engage with cloud providers to assess their compliance to IDCA Grade Levels.

International Standards Organization (ISO) is an international standards body composed of representatives from various standards organizations.

Internet Small Computer System Interface (iSCSI) is a storage networking standard used to link data storage to systems using the Internet Protocol (IP).

ISACA's COBIT: see COBIT

ISO/IEC 27001: Standard on managing Information Security.: It includes requirements for establishing , implementing, maintaining, and continually improving information management.

ISO/IEC 27002: provides best practices on information security controls for those attempting to be ISO/IEC 27001.

ISO/IEC 27017 created to supplement ISO/IEC 27002 to provide additional security controls for the **cloud**.**:**

ISO/IEC 27018: 2014 ISO/IEC 27018: 2019: IT Security techniques.: Code of practice for ***protection of PII*** in public clouds.

ISO/IEC 27034-1 mandates a framework for application security within an organization. According to the standard, each organization should have a(n) ___________, and each application within the organization should have its own ____________.

ISO/IEC 28000: 2007: is a standard for ensuring security assurance in the supply chain.

ISO/IEC 31000: 2009: is a standard providing industry independent principles and guidelines on risk management.: It does not intend or attempt to achieve uniformity but rather the most appropriate risk management for each organization for its objectives, context, structure, operations, processes, functions, services, or assets employed.

Key risk indicators (KRI): critical predictors of risks or adverse events that can impact and organization.

Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a Distinguished name (DN)

Mean time between failure (MTBF): is the predicted time between failures of a system during normal system operation.: It applies only to unplanned maintenance and excludes scheduled maintenance, inspection, recalibration, or prevent parts replacement.

Mean time to repair (MTTR): is the mean time it takes to repair a system.: It includes both the repair time and testing time.

NFPA: National Fire Protection Association.: This is a nonprofit organization attempting to eliminate death, injury, property, and economic loss due to fire, electrical and related hazards.

NIST National Institute of Standards and Technology is an agency of the Department of Commerce whose mission is to promote innovation and industrial competitiveness. It also creates numerous standard and requirements for the DoD, Federal Government, and government contractors relating to Cyber security.**:**

NIST SP 800-37 establishes the Risk Management Framework using a life cycle approach for security and privacy.: "The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels. The RMF also promotes near real-time risk management and ongoing information system and common control authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make efficient, cost-effective, risk management decisions about the systems supporting their missions and business functions; and incorporates security and privacy into the system development life cycle."

NIST SP 800-53 provides security and privacy controls for information systems and organizations.

NIST SP 800-92: Guide to Computer Security Log Management "seeks to assist organizations in understanding the need for sound computer security log management. It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in this publication covers several topics, including establishing log management infrastructures, and developing and performing robust log management processes throughout an organization. The publication presents logging technologies from a high-level viewpoint."

NIST 800-161 – entitled "Supply Chain Risk Management Practices for Fed Info Sys and Orgs" is concerned with the supply chain risk management.

Open Web Application Security Project (OWASP): is a nonprofit organization working to improve the security of software.: They are known for their top 10 most critical security concerns for web application security.: See https: //owasp.org/www-project-top-ten/

Organization for Economic Cooperation and Development (OECD): produced 7 principals to govern the protection of data.: They are:

1. **Notice**—data subjects should be given notice when their data is being collected;
2. **Purpose**—data should only be used for the purpose stated and not for any other purposes;
3. **Consent**—data should not be disclosed without the data subject's consent;
4. **Security**—collected data should be kept secure from any potential abuses;
5. **Disclosure**—data subjects should be informed as to who is collecting their data;
6. **Access**—data subjects should be allowed to access their data and make corrections to any inaccurate data
7. **Accountability**—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

Organizational Normative Framework (ONF), Application Normative Framework (ANF): The Organizational Normative Framework (ONF) is a framework which contains multiple application security best practices know as Application Normative Frameworks (ANFs).: One ONF per organization with as many ANFs as needed.

OSHA: is a large regulatory agency of the United States Department of Labor that originally had federal visitorial powers to inspect and examine workplaces.

Payment Card Industry Data Security Standard (PCI DSS): is an industry requirement that imposes on anyone who processes or accepts credit cards.: The PCI can impose fines on violators if they fail to meet PCI DSS requirements.: Depending on the size of the vendor, external, independent audits can be required in addition to higher requirements.

Personal Information Protection and Electronic Documents Act (PIPEDA): is a Canadian data privacy law that protects the PII of individuals.: It provides for individuals to inspect the data held by and organization and challenge its accuracy.: It also requires an organization to obtain the consent of an individual when collecting, using, and disclosing that PII.

Privacy Level Agreement (PLA) is and agreement set to contract how a third-party provider will ensure the confidentiality of information an organization might permit them to access.

Recovery time objective (RTO) is the duration of time and specified service level to which a business process must be restored to.:

Risk Management Framework (RMF): is a set of: standards and guidelines to develop a risk-based approach to Information Security.: It helps and organization **prepare** for risk management, **categorize** systems and information based on impact studies, **select** appropriate controls based on risk assessments, **implement** and document the controls, **assess** how well the controls work, authorize the system to operate, and **monitor** controls and changes to the risks to the system.

RPO Recovery Point Objective refers to how much data can be lost before that loss causes significant harm to the business.: This often drives backup and real-time duplication requirements.

RTO is the maximum time after an outage of a computer or other resource to resume normal business operations.

SABSA stands for Sherwood Applied Business Security Architecture, which is a framework for enterprise security architecture and service management.:

Sarbanes-Oxley Act (SOX): : A law passed to increase independence in audit practices and require the retention and accuracy of financial records as a result of financial and stock scandals associated with Enron.

SAS 70: Statement on Auditing Standards (SAS) No. 70 was a recognized standard of the American Institute of Certified Public Accountants (AICPA) in response to the issues that also lead to Sarbanes-Oxley (SOX).: Deprecated in 2011 by the Statement on Standards for Attestation Engagements (**SSAE) No. 16**.

SEC is the US Securities and Exchange Commission whose primary purpose is to combat market manipulation.: It also enforces the Sarbanes-Oxley Act.

Secure Sockets Layer (SSL): :

Sherwood Applied Business Structure Architecture (SABSA) see SABSA

SIEMs are Security Event and Incident Managers.: They collect, clean, and correlate

SOC 1 Report: : This report focuses on controls associated with financial services. DOES NOT INCLUDE ANY INFORMATION TECHNOLOGY AND IS USELESS TO A CLOUD CUSTOMER

SOC 2 Report – review controls relevant to data security, availability, processing integrity, confidentiality, or privacy***. This is the report of the most useful cloud customers*** (to determine the suitability of cloud providers)

SOC 2 Type 1 Report – only reviews controls as designed, at a particular moment in time. Audit examines the controls chosen by the target. Not useful for a CCSP

SOC 2 Type 2 Report –: a realistic view of the provider's security posture and overall program. the SOC 2 reports are composed of five principles: confidentiality, processing integrity, availability, privacy, and security.

SOC 3 Report is an attestation report or can be called a seal of approval.: It lacks financial or security data but only attests that an audit was performed.

SRE stands for Site Reliability Engineering which is a set of practices and principles whose goal is to produce scalable and highly reliable software systems.: Closely related to DevOPS,: which are practices that combine software develop SRE and IT operations.

SSAE 16: and subsequent SOC reports are the successors of the SAS 70.:

Standard Application Security (SAS), Application Normative Framework (ANF)

Statement on Standards for Attestation Engagements (SSAE) auditing standard and certifies auditors for that standard?

Statement on Standards for Attestation Engagements 16 (SSAE 16) Service Organization Control (SOC) reports are audit tools promulgated by the American Institute of Certified Public Accountants (AICPA).

Storage area networks (SAN) is a dedicated, high-speed network that connects shared pools of storage to multiple servers.

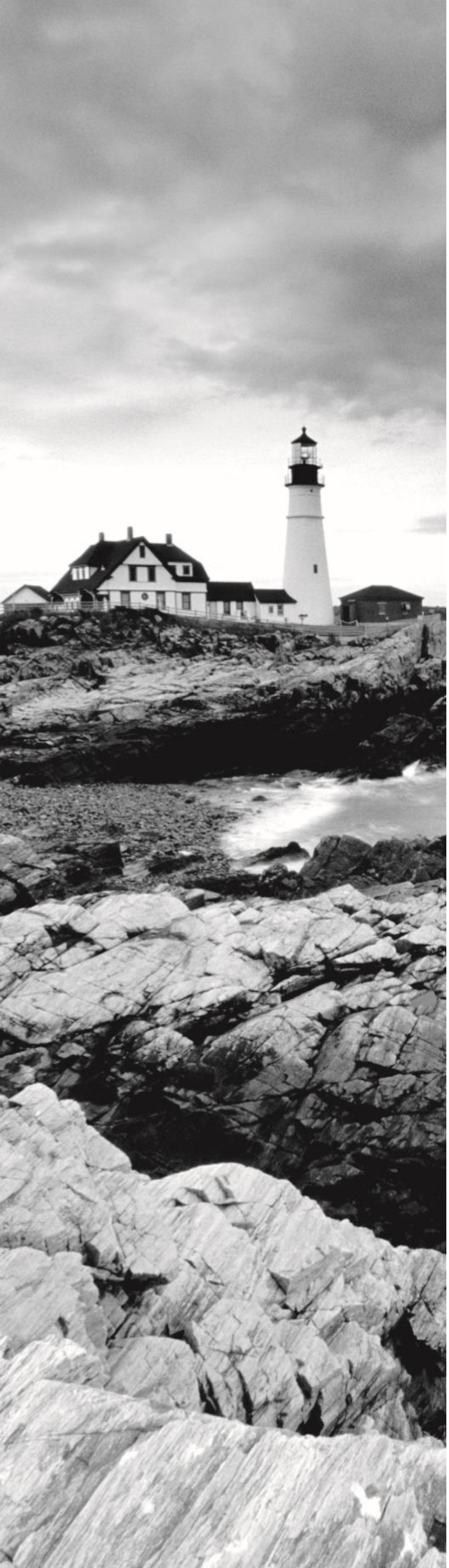
STRIDE Model: STRIDE is a threat model while DREAD is a risk assessment model.: STRIDE stands for **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of service, **E**levation of privilege.:

System and Organization Controls (SOC) reports help companies establish trust and confidence in service delivery and controls.: The reports are produced by third party certified public accountants.

US Office of Management and Budget (OMB) is a component of the Executive branch.: Of import to us, they manage FedRAMP and direct it's used for the Federal Governments use of the Cloud.

Uptime Institute has created and promoted the Tier Standard which guides the design, construction, and operation of sites world-wide.: A data center can be rated from Tier 1, the lowest to: Tier 4 based on built-in redundancy, distribution paths, concurrent maintenance, fault tolerance, compartmentalization, and cooling.:

USPTO is the US Patent and Trademark Office which registers both.



CCSP Textbook Glossary (WGU C838: Managing Cloud Security)

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 Access Security Broker (CASB): A solution/provider who handles secure access methodologies between the cloud customer and cloud service provider. Services can include cryptographic management/key escrow, and login solutions (such as federation/identity tokens).

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.

Containers/containerization: Technology that allows the virtualization of a runtime environment such that the cloud customer can install/operate an application without needing an entire virtual machine/operating system. Also offers compartmentalization of data.

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. Also known as 'cryptographic erasure'.

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. Satellite

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.

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.

Digital Rights Management (DRM): Focuses on security and encryption to prevent unauthorized copying and limitation of distribution to only those who pay. Sometimes referred to as Enterprise Rights Management (ERM) or Information Rights Management (IRM).

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 blackbox 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 string 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

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 wellarchitected 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. A theoretical technology.

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-based 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 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. Currently described by ISO 27001.

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.

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-based 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

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 threephase 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).

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.

STRIDE Threat Model: First developed by Microsoft and derived from an acronym for the following six threat categories: Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege.

T

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.

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 crosssite 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.