**0. General Information**

**Definitions, Translations & Links**

* **VOCABULARY**
  + Ubiquitous = allgegenwärtig
  + Inadvertent = versehentlich
  + Insurmountable = unüberwindlich
* **GLOSSARY**
  + GRC = Governance Risk Management and Compliance
  + ISMS = Information Security Management System
* **DOCUMENTS**
  + Privacy Act 1988 (Australia)
  + NIST SP 800-145 / ISO 17788 (Core Definition of Cloud)
  + NIST SP 800-146 / ISO 17789 (Extended Definition of Cloud)
  + ISO 15408 (Common Criteria for testing security products)
  + CSA TCI Reference Architecture
  + SABSA
  + ITIL
  + Jericho
  + CSA Security as a Service Category 8 Encryption
  + ISO 27001 (Information Security Management Systems)
  + ISO 27002 (Code of practice for information security management)
  + ISO 27017 (Cloud Security)
  + ISO 27018 (Code of practice for protecting PII in public Clouds acting as PII processors)
  + ANZ4360 (Australia New Zealand) Qualitative (RISK)
  + ISO 31000 / 27031 (RISK)
  + ENISA
  + CSA STAR
  + NIST RISK management Framework
  + CSA CCM (Cloud Controls Matrix)
  + NIST 800-53 (like ISO 27002 but for federal agencies)
  + NIST 800-137 (continuous monitoring ISCM)
  + ISO 27037:2012 (collect evidence)
  + FIPS 140-2 (physical IT security)
  + Security as a Service Category 2
  + AICPA SAS-70 (replaced by SSAE16) SSAE18 newer Version
    - SOC 1-3 reports
  + NIST SP 800-63 A/B/C
  + GLBA
  + ITAR
  + Safe Harbor
  + NIST SP 500-299 Security Reference Architecture
  + ISO 15408 Common Criteria
    - P = Category of Product
    - To = Actual Product
    - ST = Security Target = Condition of Test
    - EAL (Evaluation Assurance Level) 1-7
      * 1: functional
      * 2: structurally
      * 3/4: methodically
      * 5/6: semi-formally
      * 7: formally
  + ISO 27034-1 (organizational normative framework)
  + ISO 28000 Supply Chain Standard
  + NIST SP 800-14 (Securing IT Systems)
  + NIST SP 800-123 (General Server Security)

* **Important for EXAM PREP**
  + Exam dates back to 2015
  + Weight: see CCSP Exam Outline
    - Domain 1: 19%
    - Domain 2: 20%
    - Domain 3: 19%
    - Domain 4: 15%
    - Domain 5: 15%
    - Domain 6: 12%
  + Essential Docs:
    - CSA guide need to know
      * All SecAAS good to know
      * TCI Reference Architecture
      * STAR
      * Cloud Controls Matrix
  + Essential Standards:
    - ISO 27001/2
    - ISO 270017/18
    - FIPS-140-2
      * 4 Levels
    - NIST800-53
      * FedRamp
    - Common Criteria
      * EAL1-7
    - SAS-70 (replaces by SSAE16)
      * SOC-1-3
  + Essential Laws:
    - Privacy Act 1988
    - SOX/GBLA
    - APEC
    - Safe Harbour
    - HIPPA
  + Essential Contractual Regulation
    - PCI-DSS

**1. Architectural Concepts and Design Requirements**

**Roles, characteristics, and technologies**

* **MODELS**
  + NIST (SP 800-145): Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

* **CHARACTERISTICS**
  + Broad Network Access
  + Resource Pool
  + On demand (Self service)
  + Measured Service / Pay per use
  + Rapid Elasticity

* **DRIVERS**
  + Costs associated with the ownership of their current IT infrastructure solutions
  + The desire to reduce IT complexity
  + Risk reduction: Testing solution before investments
  + Scalability
  + Elasticity
  + Consumption-based pricing
  + Virtualization: Single view of resources
  + Cost: The pay-per-usage model / Shift from CapEx to OpEx
  + Business agility
  + Mobility: Access from around the globe (ubiquitous)
  + Collaboration/Innovation: Work simultaneously

* **SECURITY/RISKS AND BENEFITS**
  + Managing reputational risk
    - Strategic alignment
    - Effective board oversight
    - Integration of risk into strategy setting and business planning
    - Cultural alignment
    - Strong corporate values and a focus on compliance
    - Operational focus
    - Strong control environment
  + Compliance (Legal, Regulatory)
  + Privacy
  + Distributed/Multi Tenant Security Environment

* **DEFINITIONS**
  + Anything as a Service (XaaS): The growing diversity of services available over the Internet via cloud computing as opposed to being provided locally, or on-premises.
  + Apache CloudStack: An open source cloud computing and Infrastructure as a Service (IaaS) platform developed to help make creating, deploying, and managing cloud services easier by providing a complete “stack” of features and components for cloud environments.
  + Business Continuity: The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
  + Business Continuity Management: A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and that provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.
  + Business Continuity Plan: The creation of a strategy through the recognition of threats and risks facing a company, with an eye to ensure that personnel and assets are protected and able to function in the event of a disaster.
  + Cloud App (Cloud Application): Short for cloud application, cloud app describes a software application that is never installed on a local computer. Instead, it is accessed via the Internet.
  + Cloud Application Management for Platforms (CAMP): CAMP is a specification designed to ease management of applications—including packaging and deployment—across public and private cloud computing platforms.
  + 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 stored in and accessible from multiple distributed and connected 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: 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: Cloud computing accounting software is accounting software that is hosted on remote servers. It provides accounting capabilities to businesses in a fashion similar to the SaaS (Software as a Service) business model.
  + Cloud Computing Reseller: A company that purchases hosting services from a cloud server hosting or cloud computing provider and then re-sells them to its own customers.
  + Cloud Database: A database accessible to clients from the cloud and delivered to users on demand via the Internet. Also referred to as Database as a Service (DBaaS)
  + Cloud Enablement: The process of making available one or more of the following services and infrastructures to create a public cloud computing environment: cloud provider, client, and application.
  + Cloud OS: A phrase frequently used in place of Platform as a Service (PaaS) to denote an association to cloud computing.
  + Cloud Portability: In cloud computing terminology, this refers to the ability to move applications and their associated data between one cloud provider and another—or between public and private cloud environments.
  + 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, where the information can be provided over the Internet on an on-demand basis.
  + Cloud Provider: A service provider who offers customers storage or software solutions available via a public network, usually the Internet. The cloud provider dictates both the technology and operational procedures involved.
  + Cloud Provisioning: 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.
  + Enterprise Application: Describes applications—or software—that a business uses to assist the organization in solving enterprise problems.
  + Cloud Server Hosting: A type of hosting in which hosting services are made available to customers on demand via the Internet.
  + Cloud Storage: “The storage of data online in the cloud,” whereby a company’s data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.
  + Cloud Testing: 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.
  + Desktop as a Service (DaaS): A form of virtual desktop infrastructure (VDI) in which the VDI is outsourced and handled by a third party.
  + Enterprise Cloud Backup: Enterprise-grade cloud backup solutions typically add essential features such as archiving and disaster recovery to cloud backup solutions.
  + Eucalyptus: An open source cloud computing and Infrastructure as a Service (IaaS) platform for enabling private clouds.
  + Event: A change of state that has significance for the management of an IT service or other configuration item.
  + Hybrid Cloud Storage: A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise’s private cloud and other data is stored and accessible from a public cloud storage provider.
  + Incident: An unplanned interruption to an IT service or reduction in the quality of an IT service.
  + Infrastructure as a Service (IaaS): IaaS is defined as computer infrastructure, such as virtualization, being delivered as a service.
  + Managed Service Provider: An IT service provider where the customer dictates both the technology and operational procedures
  + Mean Time Between Failure (MTBF): The measure of the average time between failures of a specific component, or part of a system.
  + Mean Time To Repair (MTTR): The measure of the average time it should take to repair a failed component, or part of a system.
  + 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.
  + Multi-Tenant: In cloud computing, multi-tenant is the phrase used to describe multiple customers using the same public cloud.
  + Online Backup: In storage technology, online backup means to back up data from your hard drive to a remote server or computer using a network connection.
  + 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.
  + Platform as a Service (PaaS): The process of deploying onto the cloud infrastructure consumer-created or acquired applications that are created using programming languages, libraries, services, and tools supported by the provider.
  + 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.
  + Problem: The unknown cause of one or more incidents, often identified as a result of multiple similar incidents.
  + 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.
  + Storage Cloud: Refers to the collection of multiple distributed and connected resources responsible for storing and managing data online in the cloud.
  + Vendor Lock-in: customer might be unable to leave, migrate, or transfer to an alternate provider due to technical or non-technical constraints
  + Vendor Lock-out: occurs when a customer is unable to recover access their own data (e.g. bankruptcy of the provider)

* **ROLES**
  + Cloud Customer: An individual or entity that utilizes or subscribes to cloud-based services or resources.
  + Cloud Provider: A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations and/or individuals, usually for a fee, otherwise known to clients “as a service.”
  + Cloud Backup Service Provider: A third-party entity that manages and holds operational responsibilities for cloud-based data backup services and solutions to customers from a central datacenter.
  + Cloud Services Broker (CSB): Typically 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.
  + Cloud Service Auditor: Third-party organization that verifies attainment of SLAs (service level agreements).
  + Regulators: entities that ensure organization are in compliance with regulatory framework for which they are responsible. Can be government agencies certification bodies, or parties to a contract. Regulations include:
    - HIPPA
    - GLBA
    - PCI-DSS
    - ISO
    - SOX
    - FTC
    - SEC

* **CHARACTERISTICS**
  + On-Demand Self-Service: The cloud service(s) provided that enables the provision of cloud resources on demand
  + Broad Network Access: The cloud, by its nature is an “always on” and “always accessible” offering for users to have widespread access to resources, data, and other assets.
  + Resource Pooling
  + Rapid Elasticity: Allows the user to obtain additional resources, storage, compute power, and so on, as the user’s need or workload requires.
  + Measured Service: Cloud computing offers a unique and important component that traditional IT deployments have struggled to provide—resource usage can be measured, controlled, reported, and alerted upon

* **ACTIVITIES**
  + Cloud Administrator: This individual is typically responsible for the implementation, monitoring, and maintenance of the cloud within the organization
  + Cloud Application Architect: This person is typically responsible for adapting, porting, or deploying an application to a target cloud environment.
  + Cloud Architect: This role 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 Data Architect: This individual is similar to the Cloud Architect; the Data Architect’s role is to ensure 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 Developer: This person focuses on development for the cloud infrastructure itself.
  + Cloud Operator: This individual is responsible for daily operational tasks and duties that focus on cloud maintenance and monitoring activities.
  + Cloud Service Manager: This person typically responsible for policy design, business agreement, pricing model, and some elements of the SLA
  + Cloud Storage Administrator: This role focuses on relevant user groups and the mapping, segregations, bandwidth, and reliability of storage volumes assigned.
  + Cloud User/Cloud Customer: This individual is a user accessing either paid for or free cloud services and resources within a cloud.

* **CATEGORIES**
  + **IaaS**, “the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).”
  + **PaaS**, “the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.”
  + **SaaS**, “The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including networks, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.”

* **DEPLOYMENT MODELS**
  + ***PUBLIC CLOUD***
    - “the 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.”
  + ***PRIVATE CLOUD***
    - “the cloud infrastructure is provisioned for exclusive use by a single organization comprising 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.”
  + ***HYBRID CLOUD***
    - “the cloud infrastructure is a composition 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).”
  + ***COMMUNITY CLOUD***
    - “the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.”

**Architecture Design principles**

* **FRAMEWORKS**
  + Business Operation Support Services BOSS
    - Sherwood Applied Business Security Architecture (SABSA)
  + Information Technology Operation and Support ITOS
    - IT Infrastructure Library (ITIL)
  + Presentation, Application, Information, Infrastructure Services
    - The Open Group Architecture Framework (TOGAF)
  + Security and Risk Management
    - Jericho/Open Group The Jericho forum now is part of the Open Group Security Forum.

* **KEY PRINCIPLES**
  + Define protections that enable trust in the cloud,
  + Develop cross-platform capabilities and patterns for proprietary and open source providers.
  + Facilitate trusted and efficient access, administration, and resiliency to the customer/consumer.
  + Provide direction to secure information that is protected by regulations.
  + The architecture must facilitate proper and efficient identification, authentication, authorization, administration, and auditability.
  + Centralize security policy, maintenance operation, and oversight functions.
  + Access to information must be secure yet still easy to obtain.
  + Delegate or federate access control where appropriate.
  + Must be easy to adopt and consume, supporting the design of security patterns.
  + The architecture must be elastic, flexible, and resilient, supporting multi-tenant, multi-landlord platforms.
  + The architecture must address and support multiple levels of protection, including network, operating system, and application security needs.

* **KEY REQUIREMENTS**
  + Interoperability: Interoperability defines how easy it is to move and reuse application components regardless of the provider, platform, OS, infrastructure, location, storage, and the format of data or APIs.
    - Investments do not become prematurely technologically obsolete.
    - Organizations are able to easily change cloud service providers to flexibly and cost-effectively support their mission
    - Organizations can economically acquire commercial and develop private clouds using standards-based products, processes, and services.
  + Portability: Portability is a key aspect to consider when selecting cloud providers since it can both help prevent vendor lock-in and deliver business benefits by allowing identical cloud deployments to occur in different cloud provider solutions, either for the purposes of disaster recovery or for the global deployment of a distributed single solution.
  + Availability: Systems and resource availability defines the success or failure of a cloud-based service.
  + Security: the ability to measure, obtain assurance, and integrate contractual obligations to minimum levels of security are the keys to success.
  + Privacy: Challenge - no uniform or international privacy directives, laws, regulations, or controls exist, leading to a separate, disparate, and segmented mesh of laws and regulations being applicable depending on the geographic location where the information may reside (data at rest) or be transmitted (data in transit).
  + Resiliency: represents the ability to continue service and business operations in the event of a disruption or event.
  + Performance: In order for optimum performance to be experienced through the use of cloud services, the provisioning, elasticity, and other associated components should always focus on performance.
  + Governance: The term “governance” relating to processes and decisions looks to define actions, assign responsibilities, and verify performance.
  + Service Level Agreements (SLAs): Key benefits when compared with traditional-based environments or “in-house IT.” These include downtime, upgrades, updates, patching, vulnerability testing, application coding, test and development, support, and release management. Many of these require the provider to take these areas and activities very seriously, as failing to do so will have an impact on their bottom line.
  + Auditability: Auditability allows for users and the organization to access, report, and obtain evidence of actions, controls, and processes that were performed or run by a specified user.
  + Regulatory Compliance: Organization’s requirement to adhere to relevant laws, regulations, guidelines, and specifications relevant to its business, specifically dictated by the nature, operations, and functions it provides or utilizes to its customers.

**Security concepts**

* **KEY SECURITY COMPONENTS**
  + Network Security and Perimeter
    - Key elements
    - Different meanings Network perimeter under different guises and deployment models.
  + Cryptography
    - Encryption
    - Key Management
  + IAM and Access Control
    - Provisioning and de-provisioning
    - Centralized directory services
    - Privileged user management
    - Authentication and access management: In the event that one of the activities mentioned above is not carried out regularly as part of an ongoing managed process, this can weaken the overall security posture.
  + Data and Media Sanitization
    - Vendor lock-in
    - Cryptographic erasure
    - Data overwriting
  + Virtualization Security
    - Hypervisor
      * Type 1: running directly on hardware
      * Type 2: running on host OS
    - HV Security types

* **COMMON THREATS**
  + Data Breaches
    - the nature of cloud deployments and multi-tenancy, virtual machines, shared databases, application design, integration, APIs, cryptography deployments, key management, and multiple locations of data all combine to provide a highly amplified and dispersed attack surface, leading to greater opportunity for data breaches.
    - the rise of smart devices, tablets, increased workforce mobility, BYOD
  + Data Loss
    - Does the provider/customer have responsibility for data backup?
    - In the event that backup media containing the data is obtained, does this include all data or only a portion of the information?
    - Where data has become corrupt, or overwritten, can an import or restore be performed?
    - Where accidental data deletion has occurred from the customer side, will the provider facilitate the restoration of systems and information in multi-tenancy environments or on shared platforms?
  + Account or Service traffic hijacking
    - Means
    - Attackers goals
  + Insecure Provider interfaces and APIs
  + Denial of Service
  + Malicious insiders
  + Abuse of Cloud Services
  + Insufficient Due Diligence
    - Due diligence is the act of investigating and understanding the risks a company faces.
    - Due care is the development and implementation of policies and procedures to aid in protecting the company, its assets, and its people from threats.
  + Shared Technology Vulnerabilities: providers should implement a layered approach to securing the various components, and a defense-in-depth strategy should include compute, storage, network, application, and user security enforcement and monitoring.

* **OPEN WEB APPLICATION SECURITY PROJECT (OWASP) TOP TEN SECURITY THREATS**
  + A1—Injection: Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
  + A2—Broken Authentication and Session Management: Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities.
  + A3—Cross-Site Scripting (XSS): XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim’s browser, which can hijack user sessions, deface websites, or redirect the user to malicious sites.
  + A4—Insecure Direct Object References: A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
  + A5—Security Misconfiguration: Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
  + A6—Sensitive Data Exposure: Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
  + A7—Missing Function Level Access Control: Most web applications verify function-level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
  + A8—Cross-Site Request Forgery (CSRF): A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
  + A9—Using Components with Known Vulnerabilities: Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
  + A10—Unvalidated Redirects and Forwards: Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

* **SECURITY CONSIDERATIONS FOR DIFFERENT CLOUD CATEGORIES**

* **IAAS**
  + Virtual Machine Attacks
  + Virtual Network: The virtual network contains the virtual switch software that controls multiplexing traffic between the virtual NICs of the installed VMs and the physical NICs of the host.
  + Hypervisor Attacks: Hackers consider the hypervisor a potential target because of the greater control afforded by lower layers in the system.
  + VM-Based Rootkits (VMBRs): These rootkits act by inserting a malicious hypervisor on the fly or modifying the installed hypervisor to gain control over the host workload. In some hypervisors such as Xen, the hypervisor is not alone in administering the VMs.
  + Virtual Switch Attacks: The virtual switch is vulnerable to a wide range of layer II attacks such as a physical switch. These attacks include virtual switch configurations, VLANs and trust zones, and ARP tables.
  + Denial-of-Service (DoS) Attacks: Denial-of-service attacks in a virtual environment form a critical threat to VMs, along with all other dependent and associated services.
  + Co-Location: Multiple VMs residing on a single server and sharing the same resources increase the attack surface and the risk of VM-to-VM or VM-to-hypervisor compromise.
  + Multi-Tenancy: Different users within a cloud share the same applications and the physical hardware to run their VMs.
  + Workload Complexity: Server aggregation duplicates the amount of workload and network traffic that runs inside the cloud physical servers, which increases the complexity of managing the cloud workload.
  + Loss of Control: Users are not aware of the location of their data and services, and the cloud providers run VMs and are not aware of their contents
  + Network Topology: The cloud architecture is very dynamic, and the existing workload changes over time because of creating and removing VMs. In addition, the mobile nature of the VMs that allows VMs to migrate from one server to another leads to non-predefined network topology.
  + Logical Network Segmentation: Within IaaS, the requirement for isolation alongside the hypervisor remains a key and fundamental activity to reduce external sniffing, monitoring, and interception of communications and others within the relevant segments.
  + No Physical Endpoints: Due to server and network virtualization, the number of physical endpoints (e.g., switches, servers, NICs) is reduced. These physical endpoints are traditionally used in defining, managing, and protecting IT assets.
  + Single Point of Access: Virtualized servers have a limited number of access points (NICs) available to all VMs.

* **PAAS**
  + System/Resource Isolation: PaaS tenants should not have shell access to the servers running their instances
  + User-Level Permissions: Each instance of a service should have its own notion of user-level entitlements (permissions)
  + User Access Management: key emphasis is placed on the agreement, implementation of the rules, and organizational policies for access to data and assets
  + Protection Against Malware/Backdoors/Trojans

* **SAAS**
  + Data Segregation: As a result of multi-tenancy, multiple users can store their data using the applications provided by SaaS. Within these architectures, the data of various users will reside at the same location or across multiple locations and sites.
  + Data Access and Policies: The challenge associated with this is to map existing security policies, processes, and standards to meet and match the policies enforced by the cloud provider.
  + Web Application Security: cloud services rely on a robust, hardened, and regularly assessed web application to deliver services to its users. The fundamental difference with cloud-based services versus traditional web applications is their footprint and the attack surface that they will present.

* **CLOUD SECURE DATA LIFECYCLE**
  + Create: New digital content is generated or existing content is modified.
  + Store: Data is committed to a storage repository, which typically occurs directly after creation.
  + Use: Data is viewed, processed, or otherwise used in some sort of activity (not including modification).
  + Share: Information is made accessible to others—users, partners, customers, and so on.
  + Archive: Data leaves active use and enters long-term storage.
  + Destroy: Data is permanently destroyed using physical or digital means.

* **INFORMATION/DATA GOVERNANCE TYPES**
  + Information Classification: High-level description of valuable information categories (e.g., highly confidential, regulated).
  + Information Management Policies: What activities are allowed for different information types?
  + Location and Jurisdictional Policies: Where can data be geographically located? What are the legal and regulatory implications or ramifications?
  + Authorizations: Who is allowed to access different types of information?
  + Custodianship: Who is responsible for managing the information at the bequest of the owner?

* **BUSINESS CONTINUITY/DISASTER RECOVERY PLANNING**
  + Critical Success Factors
    - Understanding your responsibilities versus the cloud provider’s responsibilities.
    - Customer responsibilities.
    - Cloud provider responsibilities.
    - Understand any interdependencies/third parties (supply chain risks)
    - Order of restoration (priority)—who/what gets priority?
    - Appropriate frameworks/certifications held by the facility, services, and processes.
    - Right to audit/make regular assessments of continuity capabilities.
    - Communications of any issues/limited services.
    - Is there a need for backups to be held on-site/off-site or with another cloud provider?
    - Clearly state and ensure the SLA addresses which components of business continuity/disaster recovery are covered and to what degree they are covered.
    - Penalties/compensation for loss of service.
    - Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO)
    - Loss of integrity or confidentiality (are these both covered?)
    - Points of contact and escalation processes.
    - Where failover to ensure continuity is utilized, does this maintain compliance and ensure the same or greater level of security controls?
    - When changes are made that could impact the availability of services, that these are communicated in a timely manner.
    - Data ownership, data custodians, and data processing responsibilities are clearly defined within the SLA.
    - Where third parties and key supply chain are required to ensure that availability of services is maintained, that the equivalent or greater levels of security are met, as per the agreed-upon SLA between the customer and provider.

* **Important SLA Components**
  + Undocumented single points of failure should not exist
  + Migration to alternate provider(s) should be possible within agreed-upon timeframes
  + Whether all components will be supported by alternate cloud providers in the event of a failover or on-site/on-premise services would be required
  + Automated controls should be enabled to allow customers to verify data integrity
  + Where data backups are included, incremental backups should allow the user to select the desired settings, including desired coverage, frequency, and ease of use for recovery point restoration options
  + Regular assessment of the SLA and any changes that may impact the customer’s ability to utilize cloud computing components for disaster recovery should be captured at regular and set intervals.

**Cost–benefit analysis**

* Resource pooling: Resource sharing is essential to the attainment of significant cost savings when adopting a cloud computing strategy.
* Shift from CapEx to OpEx: The shift from capital expenditure (CapEx) to operational expenditure (OpEx) is seen as a key factor for many organizations
* Factor in time and efficiencies: Given that organizations rarely acquire used technology or servers, almost all purchases are of new and recently developed technology.
* Include depreciation: Lease cloud services, as opposed to constantly investing in technologies that become outdated in relatively short time periods.
* Reduction in maintenance and configuration time: Most of maintaining, operating, patching, updating, supporting, engineering, rebuilding, duties (if not all—depending on cloud service) are handled by the cloud provider
* Shift in focus: Technology and business personnel being able to focus on the key elements of their role, instead of the daily “firefighting” and responding to issues and technology components
* Utilities costs: Outside of the technology and operational elements, from a utilities cost perspective, massive savings can be achieved with the reduced requirement for power, cooling, support agreements, datacenter space, racks, cabinets, and so on.
* Software and licensing costs: Software and relevant licensing costs present a major cost saving as well, as you only pay for the licensing used versus the bulk or enterprise licensing levels of traditional non-cloud-based infrastructure models.
* Pay per usage: As outlined by the CapEx versus OpEx elements, cloud computing gives businesses a new and clear benefit—pay per usage.

**Certification Against Criteria**

* **INTERNATIONAL**
  + ISO/IEC 27001: consists of 35 control objectives and 114 controls spread over 14 domains.
    - Information Security Policies
    - Organization of Information Security
    - Human Resources Security
    - Asset Management
    - Access Control
    - Cryptographic
    - Physical and Environmental Security
    - Operations Security
    - Communications Security
    - System Acquisition, Development, and Maintenance
    - Supplier Relationship
    - Information Security Incident Management
    - Information Security Business Continuity Management
    - Compliance
  + SOC I/SOC II/SOC III: Statement on Auditing Standards 70 (SAS 70) was replaced by Service Organization Control (SOC) Type I and Type II reports in 2011. SOC reports are performed in accordance with Statement on Standards for Attestation Engagements (SSAE) 16
    - Levels
      * SOC I reports focus solely on controls at a service provider that are likely to be relevant to an audit of a subscriber’s financial statements. (Financial)
      * SOC II reporting was specifically designed for IT-managed service providers and cloud computing. (Security Controls)
      * SOC III Reporting also uses the Trust Services Principles but provides only the auditor’s report on whether the system achieved the specified principle, without disclosing relevant details and sensitive information. (Only statement which Security controls were passed)
    - Types:
      * Type 1: Point in time
      * Type 2: Certain timeframe

* **US**
  + NIST SP 800-53
    - Amendments 4th Rev.
    - Key components

* **AUSTRALIA**
  + Privacy Act 1988

* **INDUSTRY**
  + PCI-DSS
    - Merchant Levels Based on Transactions
    - Merchant Requirements

* **SYSTEM AND SUBSYSTEM**
  + Common Criteria
    - Common Criteria Components
    - FIPS 140-2
      * Specifications
      * Goal: accredit and distinguish secure and well-architected cryptographic modules produced by private sector vendors who seek to or are in the process of having their solutions and services certified for use in U.S. Government departments
      * Levels
        + Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.
        + Security Level 2 improves upon the physical security mechanisms of a Security Level 1 cryptographic module by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and [critical security parameters](https://en.wikipedia.org/wiki/Critical_Security_Parameter) (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.
        + Security Level 3 In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper-detection/response circuitry that zeroes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.
        + Security Level 4 provides the highest level of security. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the imediate deletion of all plaintext CSPs.

**2. Cloud Data Security**

**The Cloud Data Lifecycle Phases**

1. **Create:** The generation or acquisition of new digital content, or the alteration/updating of existing content.
   * The creation phase is the preferred time to classify content according to its sensitivity.
2. **Store:** The act of committing the digital data to some sort of storage repository. Typically occurs nearly simultaneously with creation.
   * Controls such as encryption, access policy, monitoring, logging, and backups should be implemented to avoid data threats.
3. **Use:** Data is viewed, processed, or otherwise used in some sort of activity, not including modification.
   * Data in use is most vulnerable because it might be transported into unsecure locations such as workstations, and in order to be processed, it is must be unencrypted.
   * Controls such as Data Loss Prevention (DLP), Information Rights Management (IRM), and database and file access monitors should be implemented in order to audit data access and prevent unauthorized access.
4. **Share:** Information is made accessible to others, such as between users, to customers, and to partners.
   * Technologies such as DLP can be used to detect unauthorized sharing, and IRM technologies can be used to maintain control over the information.
5. **Archive:** Data leaving active use and entering long-term storage. Archiving data for a long period of time can be challenging.
   * Storage compatibility might be an issue over time
   * Regulatory requirements must be addressed and different tools and providers might be part of this phase.
6. **Destroy:** The data is removed from the cloud provider.
   * Consideration should be made according to regulation, type of cloud being used (IaaS vs. SaaS), and the classification of the data.

**Location and Access of Data**

* **Location**
  + Who are the actors that potentially have access to data I need to protect?
  + What is/are the potential location(s) for data I have to protect?
  + What are the controls in each of those locations?
  + At what phases in each lifecycle can data move between locations?
  + How does data move between locations (via what channels)?
  + Where are these actors coming from (what locations, and are they trusted or untrusted)?
* **Access**
  + who can access relevant data
  + how they are able to access it (device and channels)

**Functions, Actors, and Controls of the Data**

* **DATA FUNCTIONS:** Each function is performed in a location by an actor
  + Access: View/access the data, including copying, file transfers, and other exchanges of information. Lifecycle mapping: all phases
  + Process: Perform a transaction on the data. Update it, use it in a business processing transaction, and so on. Lifecycle mapping: Create, Use phases
  + Store: Store the data (in a file, database, etc.). Lifecycle mapping: Store, Archive phases
* **CONTROLS:** act as a mechanism to restrict a list of possible actions down to allowed or permitted actions. They can be of a preventative, detective (monitoring), or corrective nature.
* **ACTORS:** Documenting what functions at what location are actors allowed helps to design appropriate controls.

**Cloud Services, Products, and Solutions**

* Processing data and running applications (compute servers)
* Moving data (networking)
* Preserving or storing data (storage)
  + Data Storage Types
    - IAAS
    - PAAS
    - SAAS
  + Data Storage Threats
    - Unauthorized usage: In the cloud, data storage can be manipulated into unauthorized usage, such as by account hijacking or uploading illegal content.
    - Unauthorized access: Unauthorized access can happen due to hacking, improper permissions in a multi-tenant’s environments, or an internal cloud provider employee.
    - Liability due to regulatory non-compliance: Certain controls (i.e., encryption) might be required in order to certain regulations. Not all cloud services enable all relevant data controls.
    - Denial of service (DoS) and distributed denial of service (DDoS) attacks on storage: Availability is a strong concern for cloud storage. Without data no instances can launch.
    - Corruption/modification and destruction of data: This can be caused by a wide variety of sources: human error, hardware or software failure, events such as fire or flood, or intentional hacks.
    - Data leakage/breaches: Consumers should always be aware that cloud data are exposed to data breaches. It can be external or coming from a cloud provider employee with storage access. Data tends to be replicated and moved in the cloud, which increase the likelihood of a leak.
    - Theft or accidental loss of media: This threat applies to portable storage, but as cloud datacenters grow and storage devices are getting smaller, there are increasingly more vectors for them to experience theft or similar threats as well.
    - Malware attack or introduction: The goal of almost every malware is eventually reaching the data storage.
    - Improper treatment or sanitization after end of use: End of use is challenging in cloud computing since usually we cannot enforce physical destruction of media. But the dynamic nature of data, where data is kept in different storages with multiple tenants, mitigates the risk that digital remnants can be located.
* Relevant Data Security Technologies
  + Data Leakage Prevention (DLP): For auditing and preventing unauthorized data exfiltration
    - Components
    - Architecture
    - Cloud-Based DLP Considerations
    - Cloud DLP policy should address
  + Encryption: For preventing unauthorized data viewing
    - Challenges
    - Architecture
  + Obfuscation, anonymization, tokenization, and masking: Different alternatives for protecting data without encryption
    - Data Masking/Data Obfuscation: process of hiding, replacing, or omitting sensitive information from a specific dataset.
    - Data Anonymization: Direct identifiers and indirect identifiers form two primary components for identification of individuals, users, or indeed personal information. Anonymization is the process of removing the indirect identifiers in order to prevent data analysis tools or other intelligent mechanisms from collating or pulling data from multiple sources to identify individual or sensitive information.
    - Tokenization: is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token. Tokenization is used to safeguard the sensitive data in a secure, protected, or regulated environment.
  + Data Dispersion Technique: Data dispersion is similar to a RAID solution, but it is implemented differently. Storage blocks are replicated to multiple physical locations across the cloud
  + Emerging Technologies
    - Bit splitting: involves splitting up and storing encrypted information across different cloud storage services.
    - 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.

**Data Discovery**

* Trends
  + Big data: On big data projects, data discovery is more important and more challenging. Not only is the volume of data that must be efficiently processed for discovery larger, but the diversity of sources and formats presents challenges that make many traditional methods of data discovery fail. Cases where big data initiatives also involve rapid profiling of high-velocity big data make data profiling harder and less feasible using existing toolsets.
  + Real-time analytics: The ongoing shift toward (nearly) real-time analytics has created a new class of use cases for data discovery. These use cases are valuable but require data discovery tools that are faster, more automated, and more adaptive.
  + Agile analytics and agile business intelligence: Data scientists and business intelligence teams are adopting more agile, iterative methods of turning data into business value. They perform data discovery processes more often and in more diverse ways, for example, when profiling new datasets for integration, seeking answers to new questions emerging this week based on last week’s new analysis, or finding alerts about emerging trends that may warrant new analysis work streams.
* Analysis Methods
  + Metadata: This is data that describes data, and all relational databases store metadata that describes tables and column attributes.
  + Labels: When data elements are grouped with a tag that describes the data. This can be done at the time the data is created, or tags can be added over time to provide additional information and references to describe the data. In many ways, it is just like metadata but slightly less formal.
  + Content analysis: In this form of analysis, we investigate the data itself by employing pattern matching, hashing, statistical, lexical, or other forms of probability analysis.
* Issues
  + Poor data quality: Data visualization tools are only as good as the information that is inputted.
  + Dashboards: Users modify data and change fields with no audit trail. This can lead to inconsistent insight and flawed decisions, drive up administration costs, and inevitably create multiple versions of the truth. Security poses a problem with data discovery tools. IT staff typically have little or no control over these types of solutions, which means they cannot protect sensitive information. This can result in unencrypted data being cached locally and viewed by or shared with unauthorized users.
  + Hidden costs: A common data discovery technique is to put all of the data into server RAM to take advantage of the inherent input/output rate improvements over disk.
* Challenges in the Cloud
  + Identify data location: hard to find ways to secure the data that users are accessing in real time, from multiple locations, across multiple platforms.
  + Accessing the data: Not all data stored in the cloud can be accessed easily. Sometimes customers do not have the necessary administrative rights to access their data on demand, or long-term data can be visible to the customer but not accessible to download in acceptable formats for use offline.
    - Limits on the volume of data that will be accessible
    - The ability to collect/examine large amounts of data
    - Whether any/all related metadata will be preserved
  + Preservation and maintenance: Preservation requirements should be clearly documented for, and supported by, the cloud provider as part of the SLA.

**Data Classification**

* Categories: should match the data controls to be used
  + Data type (format, structure)
  + Jurisdiction (of origin, domiciled) and other legal constraints
  + Context
  + Ownership
  + Contractual or business constraints
  + Trust levels and source of origin
  + Value, sensitivity, and criticality (to the organization or to third party)
  + Obligation for retention and preservation
* Challenges with Cloud Data
  + Data creation: The CSP needs to ensure that proper security controls are in place so that whenever data is created or modified by anyone, they are forced to classify or update the data as part of the creation/modification process.
  + Classification controls: Controls could be administrative (as guidelines for users who are creating the data), preventive, or compensating.
  + Metadata: Classifications can sometimes be made based on the metadata that is attached to the file, such as owner or location. This metadata should be accessible to the classification process in order to make the proper decisions.
  + Classification data transformation: Controls should be placed to make sure that the relevant property or metadata can survive data object format changes and cloud imports and exports.
  + Reclassification consideration: Cloud applications must support a reclassification process based on the data lifecycle.

**Data Privacy Acts**

* KEY QUESTIONS
  + What information in the cloud is regulated under data-protection laws?
  + Who is responsible for personal data in the cloud?
  + Whose laws apply in a dispute?
  + Where is personal data processed?
* GLOBAL P&DP LAWS
  + US:“Consumer Privacy Bill of Rights” 2012
  + EU 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.” replaced in 2014
  + EU enacted a privacy directive (e-privacy directive) 2002/58/EC “concerning the processing of personal data and the protection of privacy in the electronic communications sector.” This directive contains provisions concerning data breaches and the use of cookies.
  + EU General Data Protection Regulation 2014
  + EU directive for privacy in the Police and Criminal Justice sector
  + APEC (Asian-Pacific Economic Cooperation council) Privacy Framework
* DIFFERENCES BETWEEN JURISDICTION AND APPLICABLE LAW
  + Applicable law: This determines the legal regime applicable to a certain matter.
  + Jurisdiction: This usually determines the ability of a national court to decide a case or enforce a judgment or order.
* ESSENTIAL REQUIREMENTS IN P&DP LAWS
  + Typical Meanings for Common Privacy Terms
    - Data subject: An identifiable subject who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity (such as telephone number, or IP address).
    - Personal data: Any information relating to an identified or identifiable natural person. There are many types of personal data, such as sensitive/health data, and biometric data. According to the type of personal data, the P&DP laws usually set out specific privacy and data-protection obligations (e.g., security measures, data subject’s consent for the processing).
    - Processing: Operations that are performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.
    - Controller: The natural or legal person, public authority, agency, or any other body that alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law.
    - Processor: A natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the controller.
  + Privacy Roles for Customers and Service Providers
    - The customer determines the ultimate purpose of the processing and decides on the outsourcing or the delegation of all or part of the concerned activities to external organizations. Therefore, the customer acts as a controller.
    - When the service provider supplies the means and the platform, acting on behalf of the customer, it is considered to be a data processor. May be situations in which a service provider is considered either a joint controller or a controller in his own right, depending on concrete circumstances.
    - In a cloud services environment, it is not always easy to properly identify and assign the roles of controller and processor between the customer and the service provider
  + Responsibility Depending on the Type of Cloud Services
    - SaaS: The customer determines/collects the data to be processed with a cloud service (CS), while the service provider essentially makes the decisions of how to carry out the processing and implement specific security controls.
    - PaaS: The customer has higher possibility to determine the instruments of processing, although the terms of the services are not usually negotiable.
    - IaaS: The customer has a high level of control on data, processing functionalities, tools, and related operational management, thus achieving a very high level of responsibility in determining purposes and means of processing.
    - The main rule for identifying a controller is to search who determines purpose and scope of processing, in the SaaS and PaaS types, the service provider could also be considered a controller/joint controller with the customer. The proper identification of the controller and processor roles is essential for clarifying the P&DP liabilities of customer and service provider, as well as the applicable law.
  + Implementation of data discovery together with data-classification techniques represent the foundation of Data Leakage/Loss Prevention (DLP) and of Data Protection (DP), which is applied to personal data processing in order to operate in compliance with the P&DP laws.
    - Implementation of Data Discovery
    - Classification of Discovered Sensitive Data for the purpose of compliance with the applicable Privacy and Data Protection (P&DP) laws plays an essential role in the operative control of those elements that are the feeds of the P&DP fulfillments.
    - Data discovery solutions together with data classification techniques will provide an effective enabler factor for their ability to comply with the controller P&DP instructions.
  + Mapping and Definition of Controls
    - Key privacy cloud service factors:
    - Privacy Level Agreement (PLA)
    - Essential P&DP Requirements and PLA
    - Application of Defined Controls for Personally Identifiable Information (PII)

**Data Rights Management Objectives**

* Features
  + Information Rights Management (IRM) adds an extra layer of access controls on top of the data object or document. The Access Control List (ACL) determines who can open the document and what they can do with it and provides granularity that flows down to printing, copying, saving, and similar options.
  + Because IRM contains ACLs and is embedded into the original file, IRM is agnostic to the location of the data, unlike other preventative controls that depended on file location. IRM protection will travel with the file and provide continuous protection.
  + IRM is useful for protecting sensitive organization content such as financial documents. However, it is not limited to only documents; IRM can be implemented to protect emails, web pages, database columns, and other data objects.
  + IRM is useful for setting up a baseline for the default Information Protection Policy, that is, all documents created by a certain user, at a certain location, will receive a specific policy.
* IRM cloud challenges
  + Strong identity infrastructure is a must when implementing IRM, and the identity infrastructure should expand to customers, partners, and any other organizations with which data is shared.
  + IRM requires that each resource will be provisioned with an access policy. Each user accessing the resource will be provisioned with account and keys. Provisions should be made securely and efficiently in order for the implementation to be successful. Automation of provisioning of IRM resource access policy can help in implementing that goal. Automated policy provision can be based on file location, keywords, or origin of the document.
  + Access to resources can be granted per user bases or according to user role using an RBAC model. Provisioning of users and roles should be integrated into IRM policies. Since in IRM most of the classification is in the user responsibility, or based on automated policy, implementing the right RBAC policy is crucial.
  + Identity infrastructure can be implemented by creating a single location where users are created and authenticated or by creating federation and trust between different repositories of user identities in different systems. Carefully consider the most appropriate method based on the security requirements of the data.
  + Most IRM implementations will force end users to install a local IRM agent either for key storage or for authenticating and retrieving the IRM content. This feature may limit certain implementations that involve external users and should be considered part of the architecture planning prior to deployment.
  + When reading IRM-protected files, the reader software should be IRM-aware. Adobe and Microsoft products in their latest versions have good IRM support, but other readers could encounter compatibility issues and should be tested prior to deployment.
  + The challenges of IRM compatibility with different operating systems and different document readers increase when the data needs to be read on mobile devices. The usage of mobile platforms and IRM should also be tested carefully.
  + IRM can integrate into other security controls such as DLP and documents discovery tools, adding extra benefits.
* Key capabilities common to IRM solutions
  + Persistent protection: Ensures that documents, messages, and attachments are protected at rest, in transit, and even after they’re distributed to recipients
  + Dynamic policy control: Allows content owners to define and change user permissions (view, forward, copy, or print) and recall or expire content even after distribution
  + Automatic expiration: Provides the ability to automatically revoke access to documents, emails, and attachments at any point, thus allowing information security policies to be enforced wherever content is distributed or stored
  + Continuous audit trail: Provides confirmation that content was delivered and viewed and offers proof of compliance with your organization’s information security policies
  + Support for existing authentication security infrastructure: Reduces administrator involvement and speeds deployment by leveraging user and group information that exists in directories and authentication systems
  + Mapping for repository access control lists (ACLs): Automatically maps the ACL-based permissions into policies that control the content outside the repository
  + Integration with all third-party email filtering engines: Allows organizations to automatically secure outgoing email messages in compliance with corporate information security policies and federal regulatory requirements
  + Additional security and protection capabilities
    - Determining who can access a document
    - Prohibiting printing of an entire document or selected portions
    - Disabling copy/paste and screen capture capabilities
    - Watermarking pages if printing privileges are granted
    - Expiring or revoking document access at any time
    - Tracking all document activity through a complete audit trail
  + Support for email applications: Provides interface and support for email programs such as Microsoft Outlook and IBM Lotus Notes
  + Support for other document types: Other document types, besides Microsoft Office and PDF, can be supported as well

**Data-Protection Policies**

* Data retention: an organization’s established protocol for keeping information for operational or regulatory compliance needs
  + Defines
    - Retention periods
    - Data formats
    - Data security
    - Data-retrieval procedures for the enterprise
  + Components
    - Legislation, regulation, and standards requirements: Data-retention considerations are heavily dependent on the data type and the required compliance regimes associated with it.
    - Data mapping: The process of mapping all relevant data in order to understand data types (structured and unstructured), data formats, file types, and data locations (network drives, databases, object, or volume storage).
    - Data classification: Classifying the data based on locations, compliance requirements, ownership, or business usage, in other words, its “value.” Classification is also used in order to decide on the proper retention procedures for the enterprise.
    - Data-retention procedure: For each data category, the data-retention procedures should be followed based on the appropriate data-retention policy that governs the data type. How long the data is to be kept, where (physical location, and jurisdiction), and how (which technology and format) should all be spelled out in the policy and implemented via the procedure. The procedure should also include backup options, retrieval requirements, and restore procedures, as required and necessary for the data types being managed.
    - Monitoring and maintenance: Procedures for making sure that the entire process is working, including review of the policy and requirements to make sure that there are no changes.
* Data deletion: safe disposal of data once it is no longer needed. Failure to do so may result in data breaches and/or compliance failures.
  + Reasons
    - Regulation or legislation: Certain laws and regulations require specific degrees of safe disposal for certain records.
    - Business and technical requirements: Business policy may require safe disposal of data. Also, processes such as encryption might require safe disposal of the clear text data after creating the encrypted copy.
  + Disposal Options
    - Physical destruction: Physically destroying the media by incineration, shredding, or other means.
    - Degaussing: Using strong magnets for scrambling data on magnetic media such as hard drive and tapes.
    - Overwriting: Writing random data over the actual data. The more times the overwriting process occurs, the more thorough the destruction of the data is considered to be.
    - Encryption: Using an encryption method to rewrite the data in an encrypted format to make it unreadable without the encryption key.
* Data archiving: process of identifying and moving inactive data out of current production systems and into specialized long-term archival storage systems.
  + Data-encryption procedures: Long-term data archiving with an encryption could present a challenge for the organization with regard to key management.
  + Data monitoring procedures: Data stored in the cloud tends to be replicated and moved. In order to maintain data governance, it is required that all data access and movements be tracked and logged to make sure that all security controls are being applied properly throughout the data lifecycle.
  + Ability to perform eDiscovery and granular retrieval: Archive data may be subject to retrieval according to certain parameters such as dates, subject, authors, and so on. The archiving platform should provide the ability to do eDiscovery on the data in order to decide which data should be retrieved.
  + Backup and disaster recovery options: All requirements for data backup and restore should be specified and clearly documented.
  + Data format and media type: The format of the data is an important consideration because it may be kept for an extended period of time. Proprietary formats can change, thereby leaving data in a useless state, so choosing the right format is very important. The same consideration must be made for media storage types as well.
  + Data restoration procedures: Data restoral testing should be initiated periodically to make sure that the process is working. The trial data restore should be made into an isolated environment to mitigate risks, such as restoring an old virus or accidently overwriting existing data.

**Events**

* SOURCES
  + SaaS: minimal control of, and access to, event and diagnostic data, it is recommended to specify required data access requirements in the cloud SLA or contract with the cloud service provider.
    - Webserver logs
    - Application server logs
    - Database logs
    - Guest operating system logs
    - Host access logs
    - Virtualization platform logs and SaaS portal logs
    - Network captures
    - Billing records
  + PaaS: control of, and access to, event and diagnostic data. Because the applications that will be monitored are being built and designed by the organization directly, the level of application data that can be extracted and monitored is up to the developers.
    - Input validation failures, for example, protocol violations, unacceptable encodings, and invalid parameter names and values
    - Output validation failures, for example, database record set mismatch and invalid data encoding
    - Authentication successes and failures
    - Authorization (access control) failures
    - Session management failures, for example, cookie session identification value modification
  + Application errors and system events
    - Application and related systems start-ups and shut-downs, and logging initialization (starting, stopping, or pausing)
    - Use of higher-risk functionality
    - Legal and other opt-ins
  + IaaS: control of, and access to, event and diagnostic data
    - Cloud or network provider perimeter network logs
    - Logs from DNS servers
    - Virtual machine monitor (VMM) logs
    - Host operating system and hypervisor logs
    - API access logs
    - Management portal logs
    - Packet captures
    - Billing records
* EVENT ATTRIBUTE REQUIREMENTS
  + When
    - Log date and time (international format).
    - Event date and time. The event time stamp may be different to the time of logging
    - Interaction identifier.
  + Where
    - Application identifier, for example, name and version
    - Application address, for example, cluster/host name or server IPv4 or IPv6 address and port number, workstation identity, and local device identifier
    - Service name and protocol
    - Geolocation
    - Window/form/page, for example, entry point URL and HTTP method for a web application and dialog box name
    - Code location, including the script and module name
  + Who (human or machine user)
    - Source address, including the user’s device/machine identifier, user’s IP address, cell/RF tower ID, and mobile telephone number
    - User identity (if authenticated or otherwise known), including the user database table primary key value, username, and license number
  + What
    - Type of event
    - Severity of event (0=emergency, 1=alert, …, 7=debug), (fatal, error, warning, info, debug, and trace)
    - Security-relevant event flag (if the logs contain non-security event data too)
    - Description
  + Additional considerations
    - Secondary time source (GPS) event date and time.
    - Action, which is the original intended purpose of the request. Examples are log in, refresh session ID, log out, and update profile.
    - Object, for example, the affected component or other object (user account, data resource, or file), URL, session ID, user account, or file.
    - Result status. Whether the action aimed at the object was successful (can be Success, Fail, or Defer).
    - Reason. Why the status occurred, for example, the user was not authenticated in the database check, incorrect credentials.
    - HTTP status code (for web applications only). The status code returned to the user (often 200 or 301).
    - Request HTTP headers or HTTP user agent (web applications only).
    - User type classification, for example, public, authenticated user, CMS user, search engine, authorized penetration tester, and uptime monitor.
    - Analytical confidence in the event detection, for example, low, medium, high, or a numeric value.
    - Responses seen by the user and/or taken by the application, for example, status code, custom text messages, session termination, and administrator alerts.
    - Extended details, for example, stack trace, system error messages, debug information, HTTP request body, and HTTP response headers and body.
    - Internal classifications, for example, responsibility and compliance references.
    - External classifications
* STORAGE AND ANALYSIS
  + Preservation is defined by ISO 27037:2012 as the “process to maintain and safeguard the integrity and/or original condition of the potential digital evidence.”
  + Evidence preservation helps assure admissibility in a court of law.
  + Storage requires strict access controls to protect the items from accidental or deliberate modification, as well as appropriate environment controls.
  + Event logging mechanism should be tamper-proof in order to avoid the risks of faked event logs.
* SECURITY AND INFORMATION EVENT MANAGEMENT (SIEM)=SEM+SIM
  + security management that deals with real-time monitoring, correlation of events, notifications, and console views is commonly known as security event management (SEM)
  + provides long-term storage, analysis, and reporting of log data is known as security information management (SIM)
  + Capabilities
    - Data aggregation: Log management aggregates data from many sources, including network, security, servers, databases, and applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
    - Correlation: Looks for common attributes and links events together into meaningful bundles.
    - Alerting: The automated analysis of correlated events and production of alerts, to notify recipients of immediate issues.
    - Dashboards: Tools can take event data and turn it into informational charts to assist in seeing patterns or identifying activity that is not forming a standard pattern.
    - Compliance: Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance, and auditing processes.
    - Retention: Employing long-term storage of historical data to facilitate correlation of data over time and to provide the retention necessary for compliance requirements.
    - Forensic analysis: The ability to search across logs on different nodes and time periods based on specific criteria.
  + Challenges
    - targeted attack detection requires in-depth knowledge of internal systems, the kind found in corporate security teams.
    - trouble with recognizing the low-and-slow attacks
    - need to have access to the data gathered by the cloud provider’s monitoring infrastructure.
    - access to monitoring data would need to be specified as part of the SLA

**Supporting Continuous Operations**

* Audit logging: Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs. They must adhere to the applicable legal, statutory, or regulatory compliance obligations and provide unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies through to forensic investigative capabilities in the event of a security breach.
  + New event detection: The goal of auditing is to detect information security events. Policies should be created that define what a security event is and how to address it.
  + Adding new rules: Rules are built in order to allow detection of new events. Rules allow for the mapping of expected values to log files in order to detect events. In continuous operation mode, rules have to be updated to address new risks.
  + Reduction of false positives: The quality of the continuous operations audit logging is dependent on the ability to reduce over time the amount of false positives in order to maintain operational efficiency. This requires constant improvement of the rule set in use.
* Contract/authority maintenance: Points of contact for applicable regulatory authorities, national and local law enforcement, and other legal jurisdictional authorities should be maintained and regularly updated as per the business need
* Secure disposal: Policies and procedures must be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media.
* Incident response legal preparation: In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures, including chain of custody, should be required for preservation and presentation of evidence to support potential legal action subject to the relevant jurisdictions.

**Chain of Custody and Non-Repudiation**

* Chain of custody is the preservation and protection of evidence from the time it is collected until the time it is presented in court.
  + collection
  + possession
  + condition
  + location
  + transfer
  + access to
  + any analysis performed

**3. Cloud Platform and Infrastructure Security**

**Cloud environment**

* First Level Terms
  + Cloud Service Consumer: Person or organization that maintains a business relationship with, and uses service from, the Cloud Service Providers
  + Cloud Service Provider: Person, organization, or entity responsible for making a service available to service consumers
  + Cloud Carrier: The intermediary that provides connectivity and transport of cloud services between the Cloud Service Providers and Cloud Consumers
    - physical cabling (copper or fiber), which is a bandwidth-limiting factor
    - switches for local interconnects and routers for more complex network connectivity and flexibility.
    - VLANs (virtual LANs) separate local traffic into distinct “broadcast domains.”

* Physical infrastructure components
  + Design: four-tier classification scheme for datacenters. Tier 1 is a basic center, and tier 4 has the most redundancy.
  + Characteristics
    - High volume of expensive hardware, up to hundreds of thousands of servers in a single facility
    - High power densities, up to 10kW (kilowatts) per square meter
    - Enormous and immediate impact of downtime on all dependent business.
    - Data center owners can provide multiple levels of service. The basic level is often summarized as “power, pipe, and ping.”
    - Electrical power and cooling pipe, that is, air conditioning. “Power” and “pipe” limit the density with which servers can be stacked in the datacenter.
    - Power density is expressed in kW per rack
    - Network connectivity.
    - Data center providers (co-location) could provide floor space, rack space, and cages (lockable floor space) on any level of aggregation.

* Virtual infrastructure components
  + Network
    - Software Defined Networks: provides a clearly defined and separate network control plane to manage network traffic that is separated from the forwarding plane.
    - Functionality
  + Compute
    - Ability to manage and allocate CPU and RAM resources effectively, either on a per-guest OS basis or on a per-host basis within a resource cluster.
    - Virtualization: provides a shared resource pool that can be managed to maximize the number of guest operating systems running on each host.
    - Scalability: with virtualization, there is the ability to run multiple operating systems (guests) and their associated applications on a single host.
    - Hypervisor: a piece of software, firmware, or hardware that gives the impression to the guest operating systems that they are operating directly on the physical hardware of the host.
  + Storage
    - 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.
* Management plane: create, start, and stop virtual machine instances and provision them with the proper virtual resources such as CPU, memory, permanent storage, and network connectivity.
  + runs on its own set of servers and will have dedicated connectivity to the physical machines under management.
  + the most powerful tool in the entire cloud infrastructure, it will also integrate authentication, access control, and logging and monitoring of resources used.
  + used by the most privileged users: those who install and remove hardware, system software, firmware, and so on.
  + the pathway for individual tenants who will have limited and controlled access to the cloud’s resources.
  + APIs allow automation of control tasks. A graphical user interface (i.e., web page) is typically built on top of those APIs.

**Management of Cloud Computing Risks**

* Corporate governance: risks around cloud computing should be judged in relation to the corporate goals.
* Enterprise risk management is the set of processes and structure to systematically manage all risks to the enterprise. This explicitly covers supply chain risks and third-party risks, the biggest of which is typically the failure of an external provider to deliver the services that are contracted.
* Risk Assessments/Analysis
  + Risk Categories
    - Policy and Organization Risks
    - General Risks
    - Virtualization Risks
    - Cloud-Specific Risks
    - Legal Risks
    - Non-Cloud-Specific Risks
  + Cloud Attack Vectors
    - Cloud computing uses new technology such as virtualization, federated identity management, and automation through a management interface.
    - Cloud computing introduces external service providers.
    - Guest breakout
    - Identity compromise, either technical or social (e.g., through employees of the provider)
    - API compromise, for example by leaking API credentials
    - Attacks on the provider’s infrastructure and facilities (e.g., from a third-party administrator that may be hosting with the provider)
    - Attacks on the connecting infrastructure (cloud carrier)
* Countermeasure Strategies Across the Cloud
  + multiple layers of defense against any risk
    - for a control that directly addresses a risk, there should be an additional control to catch the failure of the first control. These controls are referred to as compensating controls.
  + CONTINUOUS UPTIME. This implies that every component is redundant.
    - It makes the infrastructure resilient against component failure.
    - It allows individual components to be updated without affecting the cloud infrastructure uptime.
  + AUTOMATION OF CONTROLS. Controls should be automated as much as possible, thus ensuring their immediate and comprehensive implementation.
    - integrate software into the build process of virtual machine images that
    - automated system for configuration and resilience makes it possible to replace the running instance with a fresh, updated one. This is often referred to as the baseline image.
  + ACCESS CONTROLS. Depending on the service and deployment models, the responsibility and actual execution of the control can lie with the cloud consumer, with the cloud provider, or both.
    - Cloud services should deploy a user-centric approach for effective access control, in which every user request is bundled with the user identity. Particular attention is required for enabling adequate access to external auditors, without jeopardizing the infrastructure.
    - Building access
    - Computer floor access
    - Cage or rack access
    - Access to physical servers (hosts)
    - Hypervisor access (API or management plane)
    - Guest operating system access (VMs)
    - Developer access
    - Customer access
    - Database access rights
    - Vendor access
    - Remote access
    - Application/software access to data (SaaS)
* Security controls management
  + Physical and Environmental Protections
    - KEY REGULATIONS
    - CONTROLS
    - PROTECTING DATACENTER FACILITIES
  + System and Communication Protections
    - AUTOMATION OF CONFIGURATION
    - RESPONSIBILITIES OF PROTECTING THE CLOUD SYSTEM
    - FOLLOWING THE DATA LIFECYCLE
  + Virtualization Systems Controls
    - The virtualization components include compute, storage, and network, all governed by the management plane. These components merit specific attention. As they implement cloud multi-tenancy, they are a prime source of both cloud-specific risks and compensating controls.
    - Management plane GUI and API
    - Isolation of the management network with respect to other networks. Separate physical network to meet regulatory and compliance requirements
    - The virtualization system components implement controls that isolate tenants. This includes not only confidentiality and integrity but also availability. Fair, policy-based resource allocation over tenants is also a function of the virtualization system components. For this, capacity monitoring of all relevant physical and virtual resources should be considered. This includes network, disk, memory, and CPU.
    - Trust zones can be used to segregate the physical infrastructure
    - The virtualization layer is also a potential residence for other controls (traffic analysis, DLP, virus scanning)
    - Procedures for snapshotting live images should be incorporated into incident response procedures to facilitate cloud forensics.
    - The virtualization infrastructure should also enable the tenants to implement the appropriate security controls
  + Managing Identification, Authentication, and Authorization in the Cloud Infrastructure
    - Identity in cloud computing can be federated across multiple collaborating parties. This implies a split between “identity providers” and “relying parties,” who rely on identities to be issued (provided) by the providers.
    - MANAGING IDENTIFICATION
    - MANAGING AUTHORIZATION
    - ACCOUNTING FOR RESOURCES
    - MANAGING IDENTITY AND ACCESS MANAGEMENT
    - MAKING ACCESS DECISIONS
    - THE ENTITLEMENT PROCESS
    - THE ACCESS CONTROL DECISION-MAKING PROCESS
  + Risk Audit Mechanisms
    - The purpose of a risk audit is to provide reasonable assurance that adequate risk controls exist and are operationally effective.
    - Evidence is essential component of audits
    - CLOUD COMPUTING AUDIT

**Disaster recovery and business continuity management**

* BCDR Relevant Cloud Infrastructure
  + SCENARIOS
    - ON-PREMISE, CLOUD AS BCDR
    - CLOUD CONSUMER, PRIMARY PROVIDER BCDR
    - CLOUD CONSUMER, ALTERNATIVE PROVIDER BCDR
  + PLANNING FACTORS
    - The important assets: data and processing
    - The current locations of these assets
    - The networks between the assets and the sites of their processing
    - Actual and potential location of workforce and business partners in relation to the disaster event
  + CHARACTERISTICS
    - Rapid elasticity and on-demand self-service lead to flexible infrastructure that can be quickly deployed to execute an actual disaster recovery without hitting any unexpected ceilings.
    - Broad network connectivity, which reduces operational risk.
    - Cloud infrastructure providers have resilient infrastructure, and an external BCDR provider has the potential for being very experienced and capable as their technical and people resources are being shared across a number of tenants.
    - Pay-per-use can mean that the total BCDR strategy can be a lot cheaper than alternative solutions. During normal operation, the BCDR solution is likely to have a low cost. Even a trial of an actual DR will have a low run cost.
* Business Requirements
  + Glossary
    - Recovery Point Objective (RPO) helps determine how much information must be recovered and restored
    - Recovery Time Objective (RTO) is a time measure of how fast you need each system to be up and running in the event of a disaster or critical failure.
    - Recovery Service Level (RSL). RSL is a percentage measurement (0–100%) of how much computing power is necessary based on the percentage of the production system needed during a disaster.
  + Questions that need to be answered before an optimal cloud BCDR strategy can be developed
    - Is the data sufficiently valuable for additional BCDR strategies?
    - What is the required recovery point objective (RPO); that is, what data loss would be tolerable?
    - What is the required recovery time objective (RTO); that is, what unavailability of business functionality is tolerable?
    - What kinds of “disasters” are included in the analysis?
    - Does that include provider failure?
    - What is the necessary Recovery Service Level (RSL) for the systems covered by the plan?
* Risk management
  + Risks threatening the assets
    - Damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster
    - Wear and tear of equipment
    - Availability of qualified staff
    - Utility service outages (e.g., power failures and network disruptions)
    - Failure of a provider to deliver services
  + Risks threatening the BCDR execution
    - A BCDR strategy typically involves a redundant architecture, or failover tactic. Such architectures intrinsically add complication to the existing solution. Because of that, it will have new failure modes and will require additional skills.
    - Most BCDR strategies will still have common failure modes. For example, the mitigation of VM failure by introducing a failover cluster will still have a residual risk of failure of the zone in which the cluster is located. Likewise, multi-zone architectures will still be vulnerable to region failures.
    - The DR site is likely to be geographically remote from any primary sites. This may impact performance because of network bandwidth and latency considerations. In addition, there could be regulatory compliance concerns if the DR site is in a different jurisdiction.
  + Concerns About The BCDR Scenarios
    - ON-PREMISE, CLOUD AS BCDR: workloads on physical machines may need to be converted to workloads in a virtual environment
    - CLOUD CONSUMER, PRIMARY PROVIDER BCDR: consider load-balancing functionality and available bandwidth between the redundant facilities of the cloud provider.
    - CLOUD CONSUMER, ALTERNATIVE PROVIDER BCDR
* BCDR Strategies
  + LOCATION
    - The relevant locations to be considered depend on the geographic scale of the calamity anticipated.
    - Power or network failure may be mitigated in a different zone in the same datacenter
    - Flooding, fire, and earthquakes will likely require locations that are more remote.
  + DATA REPLICATION
    - block level
    - file level
    - database level
    - in bulk
    - on the byte level
  + FUNCTIONALITY REPLICATION
    - re-creating the processing capacity on a different location.
    - active passive
    - active mode
    - many applications have extensive connections to other providers
  + PLANNING, PREPARING, AND PROVISIONING
    - about tooling, functionality, and processes that lead up to the actual DR failover response
  + FAILOVER CAPABILITY
    - requires some form of load balancer to redirect user service requests to the appropriate services.
  + RETURNING TO NORMAL
    - return to normal would be back to the original provider (or in-house infrastructure, as the case may be). Alternatively, the original provider may no longer be a viable option, in which case the DR provider becomes the “new normal.”
* Developing And Implementing The Plan
  + THE SCOPE
    - The BCDR plan and its implementation are embedded in an information security strategy
    - clearly defined roles
    - risk assessment
    - classification
    - policy
    - awareness
    - training
  + GATHERING REQUIREMENTS AND CONTEXT
    - identification of critical business processes and their dependence on specific data and services
    - Services characteristics
    - Services descriptions
    - SLA
    - risks
    - threats
    - internal policies and procedures
    - applicable legal, statutory, or regulatory compliance obligations
  + ANALYSIS OF THE PLAN
    - purpose is to translate BCDR requirements into INPUTS that will be used in the design phase
  + RISK ASSESSMENT
    - Elasticity of the cloud provider—can they provide all the resources if BCDR is invoked?
    - Will any new cloud provider address all contractual issues and SLA requirements?
    - Available network bandwidth for timely replication of data.
    - Available bandwidth between the impacted user base and the BCDR locations.
    - Legal/licensing risks—there may be legal or licensing constraints that prohibit the data or functionality to be present in the backup location.
  + PLAN DESIGN
    - objective is to establish and evaluate candidate architecture solutions and flesh out procedures and workflow
    - How will the BCDR solution be invoked?
    - What is the manual or automated procedure for invoking the failover services?
    - How will the business use of the service be impacted during the failover, if at all?
    - How will the DR be tested?
    - Finally, what resources will be required to set it up, to turn it on, and to return to normal?
  + OTHER PLAN CONSIDERATIONS
    - On the primary platform, BCDR activities are likely to include the implementation of functionality for enabling data replication on a regular or continuous schedule and functionality to automatically monitor for any contingency that might arise and raise a failover event.
    - On the DR platform, the required infrastructure and services will need to be built up and brought into trial production mode.
  + PLANNING, EXERCISING, ASSESSING, AND MAINTAINING THE PLAN
    - Testing strategy
    - The testing scope and objectives should
    - Test plans
  + TEST PLAN REVIEW
    - Review process
    - The type or combination of testing methods employed by an organization should be determined by
    - Testing methods include
    - Tabletop Exercise/Structured Walk-Through Test
    - Walk-Through Drill/Simulation Test
    - Functional Drill/Parallel Test
    - Full-Interruption/Full-Scale Test
  + TESTING AND ACCEPTANCE TO PRODUCTION
    - business continuity plan, as any other security incident response plan, is subject to testing at planned intervals or upon significant organizational or environmental changes

**4. Cloud Application Security**

**Determining Data Sensitivity and Importance**

* Independence and the ability to present a true and accurate account of information types along with the requirements for confidentiality, integrity, and availability may be the difference between a successful project and a failure.
* “CLOUD-FRIENDLINESS” QUESTIONS: What would the impact be if
  + The information/data became widely public and widely distributed (including crossing geographic boundaries)?
  + An employee of the cloud provider accessed the application?
  + The process or function was manipulated by an outsider?
  + The process or function failed to provide expected results?
  + The information/data were unexpectedly changed?
  + The application was unavailable for a period of time?

**Application Programming Interfaces (APIs)**

* Representational State Transfer (REST): A software architecture style consisting of guidelines and best practices for creating scalable web service
  + Uses simple HTTP protocol
  + Supports many different data formats like JSON, XML, YAML, etc.
  + Performance and scalability are good and uses caching
  + Widely used
* Simple Object Access Protocol (SOAP): A protocol specification for exchanging structured information in the implementation of web services in computer networks
  + Uses SOAP envelope and then HTTP (or FTP/SMTP, etc.) to transfer the data
  + Only supports XML format
  + Slower performance, scalability can be complex, and caching is not possible
  + Used where REST is not possible, provides WS-\* features

**Common Pitfalls of Cloud Security Application Deployment**

* ON-PREMISE DOES NOT ALWAYS TRANSFER (AND VICE VERSA)
  + Present performance and functionality may not be transferable. Current configurations and applications may be hard to replicate on or through cloud services.
    - First, they were not developed with cloud-based services in mind. The continued evolution and expansion of cloud-based service offerings looks to enhance previous technologies and development, not always maintaining support for more historical development and systems.
    - Second, not all applications can be “forklifted” to the cloud. Forklifting an application is the process of migrating an entire application the way it runs in a traditional infrastructure with minimal code changes.
* NOT ALL APPS ARE “CLOUD-READY”
  + Business critical systems were developed, tested, and assessed in on-premise or traditional environments to a level where confidentiality and integrity have been verified and assured. Many high-end applications come with distinct security and regulatory restrictions or rely on legacy coding projects.
* LACK OF TRAINING AND AWARENESS
  + New development techniques and approaches require training and a willingness to utilize new services.
* DOCUMENTATION AND GUIDELINES (OR LACK THEREOF)
  + Developers have to follow relevant documentation, guidelines, methodologies, processes, and lifecycles in order to reduce opportunities for unnecessary or heightened risk to be introduced. Disconnect between some providers and developers on how to utilize, integrate, or meet vendor requirements for development might exist
* COMPLEXITIES OF INTEGRATION
  + When developers and operational resources do not have open or unrestricted access to supporting components and services, integration can be complicated, particularly where the cloud provider manages infrastructure, applications, and integration platforms.
  + From a troubleshooting perspective, it can prove difficult to track or collect events and transactions across interdependent or underlying components. In an effort to reduce these complexities, where possible (and available), the cloud provider’s API should be used.
* OVERARCHING CHALLENGES
  + developers must keep in mind two key risks associated with applications that run in the cloud
    - Multi-tenancy
    - Third-party administrators
  + developers must understand the security requirements based on the
    - Deployment model (public, private, community, hybrid) that the application will run in
    - Service model (IaaS, PaaS, or SaaS)
  + developers must be aware that metrics will always be required
    - cloud-based applications may have a higher reliance on metrics than internal applications to supply visibility into who is accessing the application and the actions they are performing.
  + developers must be aware of encryption dependencies for
    - Encryption of data at rest
    - Encryption of data in transit
    - Data masking (or data obfuscation)

**Software Development Lifecycle (SDLC) Process for a Cloud Environment**

* SDLC PROCESS MODELS PHASES
  + 1. Planning and requirements analysis: Business (functional and non-functional), quality-assurance and security requirements and standards are being determined and risks associated with the project are being identified. This phase is the main focus of the project managers and stakeholders.
  + 2.Defining: The defining phase is meant to clearly define and document the product requirements in order to place them in front of the customers and get them approved. This is done through a requirement specification document, which consists of all the product requirements to be designed and developed during the project lifecycle.
  + 3.Designing: System design helps in specifying hardware and system requirements and also helps in defining overall system architecture. The system design specifications serve as input for the next phase of the model. Threat modeling and secure design elements should be undertaken and discussed here.
  + 4.Developing: Upon receiving the system design documents, work is divided into modules/units and actual coding starts. This is typically the longest phase of the software development lifecycle. Activities include code review, unit testing, and static analysis.
  + 5.Testing: After the code is developed, it is tested against the requirements to make sure that the product is actually solving the needs gathered during the requirements phase. During this phase, unit testing, integration testing, system testing, and acceptance testing are all conducted.
* SECURE OPERATIONS PHASE
  + Proper software configuration management and versioning is essential to application security. There are some tools
    - Puppet: Puppet is a configuration management system that allows you to define the state of your IT infrastructure and then automatically enforces the correct state.
    - Chef: With Chef, you can automate how you build, deploy, and manage your infrastructure. The Chef server stores your recipes as well as other configuration data. The Chef client is installed on each server, virtual machine, container, or networking device you manage (called nodes). The client periodically polls the Chef server for the latest policy and the state of your network. If anything on the node is out of date, the client brings it up to date.
  + Activities
    - Dynamic analysis
    - Vulnerability assessments and penetration testing (as part of a continuous monitoring plan)
    - Activity monitoring
    - Layer-7 firewalls (e.g., web application firewalls)
* DISPOSAL PHASE
  + Challenge: ensure that data is properly disposed
    - Crypto-shredding is effectively summed up as the deletion of the key used to encrypt data that’s stored in the cloud.

**Assessing Common Vulnerabilities**

* (OWASP) Top 10
  + “Injection: Includes injection flaws such as SQL, OS, LDAP, and other injections. These occur when untrusted data is sent to an interpreter as part of a command or query. If the interpreter is successfully tricked, it will execute the unintended commands or access data without proper authorization.
  + “Broken authentication and session management: Application functions related to authentication and session in management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens or to exploit other implementation flaws to assume other users’ identities.
  + “Cross-site scripting (XSS): XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim’s browser, which can hijack user sessions, deface websites, or redirect the user to malicious sites.
  + “Insecure direct object references: A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
  + “Security misconfiguration: Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
  + “Sensitive data exposure: Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection, such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
  + “Missing function-level access control: Most web applications verify function-level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
  + “Cross-site request forgery (CSRF): A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests that the vulnerable application thinks are legitimate requests from the victim.
  + “Using components with known vulnerabilities: Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
  + “Invalidated redirects and forwards: Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites or use forwards to access unauthorized pages.”
* NIST Framework for Improving Critical Infrastructure Cybersecurity
  + Parts
    - Framework Core: Cybersecurity activities and outcomes divided into five functions: Identify, Protect, Detect, Respond, and Recover
    - Framework Profile: To help the company align activities with business requirements, risk tolerance, and resources
    - Framework Implementation Tiers: To help organizations categorize where they are with their approach
  + Framework provides a common taxonomy and mechanism for organizations to
    - Describe their current cybersecurity posture
    - Describe their target state for cybersecurity
    - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
    - Assess progress toward the target state
    - Communicate among internal and external stakeholders about cybersecurity risk

**Cloud-Specific Risks**

* Applications that run in a PaaS environment may need security controls baked into them
  + encryption may be needed to be programmed into applications
  + logging may be difficult depending on what the cloud service provider can offer your organization
  + ensure that one application cannot access other applications on the platform unless it’s allowed access through a control
* CSA: The Notorious Nine: Cloud Computing Top Threats in 2013
  + Data breaches: If a multi-tenant cloud service database is not properly designed, a flaw in one client’s application could allow an attacker access not only to that client’s data but to every other client’s data as well.
  + Data loss: Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers’ data unless the provider takes adequate measures to back up data. Furthermore, the burden of avoiding data loss does not fall solely on the provider’s shoulders. If a customer encrypts his or her data before uploading it to the cloud but loses the encryption key, the data will be lost as well.
  + Account hijacking: If attackers gain access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker.
  + Insecure APIs: Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent on the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.
  + Denial of service: By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space, or network bandwidth, the attacker causes an intolerable system slowdown
  + Malicious insiders: CERN defines an insider threat as “A current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.”
  + Abuse of cloud services: It might take an attacker years to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes. Alternately, he might use that array of cloud servers to stage a DDoS attack, serve malware, or distribute pirated software.
  + Insufficient due diligence: Too many enterprises jump into the cloud without understanding the full scope of the undertaking. Without a complete understanding of the CSP environment, applications, or services being pushed to the cloud, and operational responsibilities such as incident response, encryption, and security monitoring, organizations are taking on unknown levels of risk in ways they may not even comprehend but that are a far departure from their current risks.
  + Shared technology issues: Whether it’s the underlying components that make up this infrastructure (CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models. A defensive in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider’s cloud.

**Threat Modeling**

* Threat modeling is performed once an application design is created. The goal of threat modeling is to determine any weaknesses in the application and the potential ingress, egress, and actors involved before it is introduced to production.
* STRIDE THREAT MODEL
  + Spoofing: Attacker assumes identity of subject
  + Tampering: Data or messages are altered by an attacker
  + Repudiation: Illegitimate denial of an event
  + Information disclosure: Information is obtained without authorization
  + Denial of service: Attacker overloads system to deny legitimate access
  + Elevation of privilege: Attacker gains a privilege level above what is permitted
* APPROVED APPLICATION PROGRAMMING INTERFACES (APIS)
  + Benefits of API
    - Programmatic control and access
    - Automation
    - Integration with third-party tools
  + CSP must ensure that there is a formal approval process in place for all APIs (internal and external)
* SOFTWARE SUPPLY CHAIN (API) MANAGEMENT
  + Consuming software that is being developed by a third party or accessed with or through third-party libraries to create or enable functionality, without having a clear understanding of the origins of the software and code in question leads to a situation where there is complex and highly dynamic software interaction taking place between and among one or more services and systems within the organization and between organizations via the cloud.
  + It is important to assess all code and services for proper and secure functioning no matter where they are sourced
* SECURING OPEN SOURCE SOFTWARE
  + Software that has been openly tested and reviewed by the community at large is considered by many security professionals to be more secure than software that has not undergone such a process.

**Identity and Access Management (IAM)**

* Identity and Access Management (IAM) includes people, processes, and systems that are used to manage access to enterprise resources by ensuring that the identity of an entity is verified and then granting the correct level of access based on the protected resource, this assured identity, and other contextual information
* IDENTITY MANAGEMENT
  + Identity management is a broad administrative area that deals with identifying individuals in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity.
* ACCESS MANAGEMENT
  + Authentication identifies the individual and ensures that he is who he claims to be. It establishes identity by asking, “Who are you?” and “How do I know I can trust you?”
  + Authorization evaluates “What do you have access to?” after authentication occurs.
  + Policy management establishes the security and access policies based on business needs and degree of acceptable risk.
  + Federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions
    - Federated Identity Management
  + Identity repository includes the directory services for the administration of user account attributes.

**Multi-Factor Authentication**

* adds an extra level of protection to verify the legitimacy of a transaction.
* What they know (e.g., password)
* What they have (e.g., display token with random numbers displayed)
* What they are (e.g., biometrics)
* Step-up authentication is an additional factor or procedure that validates a user’s identity, normally prompted by high-risk transactions or violations according to policy rules. Methods:
  + Challenge questions
  + Out-of-band authentication (a call or SMS text message to the end user)
  + Dynamic knowledge-based authentication (questions unique to the end user)

**Supplemental Security Devices**

* used to add additional elements and layers to a defense-in-depth architecture.
* WAF
  + A Web Application Firewall (WAF) is a layer-7 firewall that can understand HTTP traffic.
  + A cloud WAF can be extremely effective in the case of a denial-of-service (DoS) attack; several cases exist where a cloud WAF was used to successfully thwart DoS attacks of 350Gbs and 450Gbs.
* DAM
  + Database Activity Monitoring (DAM) is a layer-7 monitoring device that understands SQL commands.
  + DAM can be agent-based (ADAM) or network-based (NDAM).
  + A DAM can be used to detect and stop malicious commands from executing on an SQL server.
* XML
  + XML gateways transform how services and sensitive data are exposed as APIs to developers, mobile users, and cloud users.
  + XML gateways can be either hardware or software.
  + XML gateways can implement security controls such as DLP, antivirus, and anti-malware services.
* Firewalls
  + Firewalls can be distributed or configured across the SaaS, PaaS, and IaaS landscapes; these can be owned and operated by the provider or can be outsourced to a third party for the ongoing management and maintenance.
  + Implementation of firewalls in the cloud will need to be installed as software components (e.g., host-based firewall).
* API Gateway
  + An API gateway is a device that filters API traffic; it can be installed as a proxy or as a specific part of your applications stack before data is processed.
  + API gateway can implement access control, rate limiting, logging, metrics, and security filtering.

**Cryptography**

* In Transit
  + Transport Layer Security (TLS): A protocol that ensures privacy between communicating applications and their users on the Internet.
  + Secure Sockets Layer: The standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
  + VPN (e.g., IPSEC gateway): A network that is constructed by using public wires—usually the Internet—to connect to a private network, such as a company’s internal network.
* At rest
  + Whole instance encryption: A method for encrypting all of the data associated with the operation and use of a virtual machine, such as the data stored at rest on the volume, disk I/O, and all snapshots created from the volume, as well as all data in transit moving between the virtual machine and the storage volume.
  + Volume encryption: A method for encrypting a single volume on a drive. Parts of the hard drive will be left unencrypted when using this method. (Full disk encryption should be used to encrypt the entire contents of the drive, if that is what is desired).
  + File/directory encryption: A method for encrypting a single file/directory on a drive.
* There are times when the use of encryption may not be the most appropriate or functional choice for a system protection element, due to design, usage, and performance concerns. As a result, additional technologies and approaches become necessary
  + Tokenization generates a token (often a string of characters) that is used to substitute sensitive data, which is itself stored in a secured location such as a database.
  + Data masking is a technology that keeps the format of a data string but alters the content.
  + Sandbox isolates and utilizes only the intended components, while having appropriate separation from the remaining components (i.e., the ability to store personal information in one sandbox, with corporate information in another sandbox). Within cloud environments, sandboxing is typically used to run untested or untrusted code in a tightly controlled environment.

**Application Virtualization**

* creates an encapsulation from the underlying operating system.
* Examples
  + “Wine” allows for some Microsoft applications to run on a Linux platform.
  + Windows XP mode in Windows 7
* Assurance and validation techniques
  + Software assurance: Software assurance encompasses the development and implementation of methods and processes for ensuring that software functions as intended while mitigating the risks of vulnerabilities, malicious code, or defects that could bring harm to the end user.
  + Verification and validation: In order for project and development teams to have confidence and to follow best practice guidelines, verification and validation of coding at each stage of the development process are required. Coupled with relevant segregation of duties and appropriate independent review, verification and validation look to ensure that the initial concept and delivered product is complete.
  + verify that requirements are specified and measurable
  + test plans and documentation are comprehensive and consistently applied to all modules and subsystems and integrated with the final product.
  + Verification and validation should be performed at each stage of the SDLC and in line with change management components.

**Cloud-Based Functional Data**

* the data collected, processed, and transferred by the separate functions of the application can have separate legal implications depending on how that data is used, presented, and stored.
* Breaking down systems to the functions and services that have legal implications from those that don’t is essential to the overall security posture of your cloud-based systems and overall enterprise need to meet contractual, legal, and regulatory requirements.

**Cloud-Secure Development Lifecycle**

* the purpose of a cloud-secure development lifecycle: Understanding that security must be “baked in” from the very onset of an application being created/consumed by an organization leads to a higher reasonable assurance that applications are properly secured prior to being used by an organization
* ISO/IEC 27034-1
  + “Information Technology – Security Techniques – Application Security.”: defines concepts, frameworks, and processes to help organizations integrate security within their software development lifecycle.
  + ORGANIZATIONAL NORMATIVE FRAMEWORK (ONF)
    - Business context: Includes all application security policies, standards, and best practices adopted by the organization
    - Regulatory context: Includes all standards, laws, and regulations that affect application security
    - Technical context: Includes required and available technologies that are applicable to application security
    - Specifications: Documents the organization’s IT functional requirements and the solutions that are appropriate to address these requirements
    - Roles, responsibilities, and qualifications: Documents the actors within an organization who are related to IT applications
    - Processes: Related to application security
    - Application security control library: Contains the approved controls that are required to protect an application based on the identified threats, the context, and the targeted level of trust
  + APPLICATION NORMATIVE FRAMEWORK (ANF)
    - The ANF maintains the applicable portions of the ONF that are needed to enable a specific application to achieve a required level of security or the targeted level of trust. The ONF to ANF is a one-to-many relationship, where one ONF will be used as the basis to create multiple ANFs.
  + APPLICATION SECURITY MANAGEMENT PROCESS (ASMP)
    - ASMP manages and maintains each ANF
    - 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 Security Testing**

* STATIC APPLICATION SECURITY TESTING (SAST)
  + a white-box test, where an analysis of the application source code, byte code, and binaries is performed by the application test without executing the application code.
  + Goal: determine coding errors and omissions that are indicative of security vulnerabilities
  + SAST can be used to find cross-site scripting errors, SQL injection, buffer overflows, unhandled error conditions, as well as potential back doors.
  + SAST typically delivers more comprehensive results than those found using Dynamic Application Security Testing (DAST)
* DYNAMIC APPLICATION SECURITY TESTING (DAST)
  + a black-box test, where the tool must discover individual execution paths in the application being analyzed.
  + DAST is mainly considered effective when testing exposed HTTP and HTML interfaces of web applications.
* RUNTIME APPLICATION SELF PROTECTION (RASP)
  + is generally considered to focus on applications that possess self-protection capabilities built into their runtime environments, which have full insight into application logic, configuration, and data and event flows.
* VULNERABILITY ASSESSMENTS AND PENETRATION TESTING
  + both play a significant role and support security of applications and systems prior to an application going into and while in a production environment.
  + Vulnerability assessments are often performed as white-box tests, where the assessor knows that application and they have complete knowledge of the environment the application runs in.
  + Penetration testing is a process used to collect information related to system vulnerabilities and exposures, with the view to actively exploit the vulnerabilities in the system. Penetration testing is often a black-box test
  + SaaS providers are most likely not to grant permission for penetration tests to occur by clients. Generally, only a SaaS provider’s resources will be permitted to perform penetration tests on the SaaS application.
* SECURE CODE REVIEWS
  + informal
    - one or more individuals examining sections of the code, looking for vulnerabilities.
  + formal
    - trained teams of reviewers that are assigned specific roles as part of the review process, as well as the use of a tracking system to report on vulnerabilities found.
* OPEN WEB APPLICATION SECURITY PROJECT (OWASP) RECOMMENDATIONS
  + Identity management testing
  + Authentication testing
  + Authorization testing
  + Session management testing
  + Input validation testing
  + Testing for error handling
  + Testing for weak cryptography
  + Business logic testing
  + Client-side testing

**5. Operations**

**Modern Datacenters and Cloud Service Offerings**

* providers are to take into account the challenges and complexities associated with differing outlooks, drivers, requirements, and services.

**Factors That Impact Datacenter Design**

* legal and regulatory requirements because the geographic location of the datacenter impacts its jurisdiction
* contingency, failover, and redundancy involving other datacenters in different locations are important to understand
* the type of services (PaaS, IaaS, and SaaS) the cloud
* automating service enablement
* consolidation of monitoring capabilities
* reducing mean time to repair (MTTR)
* reducing mean time between failure (MTBF)
* LOGICAL DESIGN
  + All logical design decisions should be mapped to specific compliance requirements, such as logging, retention periods, and reporting capabilities for auditing. There also needs to be ongoing monitoring systems designed to enhance effectiveness.
  + Multi-Tenancy
  + The multi-tenant nature of a cloud deployment requires a logical design that partitions and segregates client/customer data.
  + Multi-tenant networks, in a nutshell, are datacenter networks that are 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.
  + Cloud Management Plane
    - The cloud management plane needs to be logically isolated although physical isolation may offer a more secure solution. It provides:
  + Virtualization Technology
    - Communications access (permitted and not permitted), user access profiles, and permissions, including API access
    - Secure communication within and across the management plane
    - Secure storage (encryption, partitioning, and key management)
    - Backup and disaster recovery along with failover and replication
  + Other Logical Design Considerations
    - Design for segregation of duties so datacenter staff can access only the data needed to do their job.
    - Design for monitoring of network traffic. The management plane should also be monitored for compromise and abuse. Hypervisor and virtualization technology need to be considered when designing the monitoring capability. Some hypervisors may not allow enough visibility for adequate monitoring. The level of monitoring will depend on the type of cloud deployment.
    - Automation and the use of APIs are essential for a successful cloud deployment. The logical design should include the secure use of APIs and a method to log API use.
    - Logical design decisions should be enforceable and monitored. For example, access control should be implemented with an identity and access management system that can be audited.
    - Consider the use of software-defined networking tools to support logical isolation.
  + Logical Design Levels
    - Logical design for data separation needs to be incorporated at the following levels
  + Service Model
    - IaaS, many of the hypervisor features can be used to design and implement security
    - PaaS, logical design features of the underling platform and database can be leveraged to implement security
    - SaaS, same as above plus additional measures in the application can be used to enhance security
* PHYSICAL DESIGN
  + Considerations
    - Does the physical design protect against environmental threats such as flooding, earthquakes, and storms?
    - Does the physical design include provisions for access to resources during disasters to ensure the datacenter and its personnel can continue to operate safely? Examples include
    - Are there physical security design features that limit access to authorized personnel? Some examples include
  + Building or Buying
    - If you build the datacenter, the organization will have the most control over the design and security of it. However, there is a significant investment required to build a robust datacenter.
    - Buying a datacenter or leasing space in a datacenter may be a cheaper alternative. With this option, there may be limitations on design inputs. The leasing organization will need to include all security requirements in the RFP and contract.
    - When using a shared datacenter, physical separation of servers and equipment will need to be included in the design.
  + Datacenter Design Standards
    - BICSI (Building Industry Consulting Service International Inc.):The ANSI/BICSI 002-2014 standard covers cabling design and installation
    - IDCA The (International Datacenter Authority): The Infinity Paradigm covers datacenter location, facility structure, and infrastructure and applications
    - NFPA (The National Fire Protection Association): NFPA 75 and 76 standards specify how hot/cold aisle containment is to be carried out, and NFPA standard 70 requires the implementation of an emergency power off button to protect first responders in the datacenter in case of emergency
    - Uptime Institute’s Datacenter Site Infrastructure Tier Standard Topology
* ENVIRONMENTAL DESIGN CONSIDERATIONS
  + Temperature and Humidity Guidelines
    - The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)
    - Temperature control locations
  + HVAC Considerations
    - the lower the temperature in the data center is, the greater the cooling costs per month will be
  + Air Management for Datacenters
    - all the design and configuration details minimize or eliminate mixing between the cooling air supplied to the equipment and the hot air rejected from the equipment
    - key design issues: configuration of
  + Cable Management
    - Under-floor and over-head obstructions, which often interfere with the distribution of cooling air. Such interferences can significantly reduce the air handlers’ airflow and negatively affect the air distribution.
    - Cable congestion in raised-floor plenums, which can sharply reduce the total airflow as well as degrade the airflow distribution through the perforated floor tiles.
    - Instituting a cable mining program (i.e., a program to remove abandoned or inoperable cables) as part of an ongoing cable management plan will help optimize the air delivery performance of datacenter cooling systems.
  + Aisle Separation and Containment
    - Strict hot aisle/cold aisle configurations can significantly increase the air-side cooling capacity of a datacenter’s cooling system
    - The rows of racks are placed back-to-back, and holes through the rack (vacant equipment slots) are blocked off on the intake side to create barriers that reduce recirculation. Additionally, cable openings in raised floors and ceilings should be sealed as tightly as possible.
    - One recommended design configuration supplies cool air via an under-floor plenum to the racks; the air then passes through the equipment in the rack and enters a separated, semi-sealed area for return to an overhead plenum
  + HVAC Design Considerations
    - The local climate will impact the HVAC design requirements.
    - Redundant HVAC systems should be part of the overall design.
    - The HVAC system should provide air management that separates the cool air from the heat exhaust of the servers.
    - Consideration should be given to energy efficient systems
    - Backup power supplies should be provided to run the HVAC system for the amount of time required for the system to stay up.
    - The HVAC system should filter contaminants and dust.
* MULTI-VENDOR PATHWAY CONNECTIVITY (MVPC)
  + There should be redundant connectivity from multiple providers into the datacenter. This will help prevent a single point of failure for network connectivity.
  + The redundant path should provide the minimum expected connection speed for datacenter operations.
* IMPLEMENTING PHYSICAL INFRASTRUCTURE FOR CLOUD ENVIRONMENTS
  + Cloud computing removes the traditional silos within the datacenter and introduces a new level of flexibility and scalability to the IT organization.

**Enterprise Operations**

* Large enterprises need to isolate HR records, finance, customer credit card details, and so on.
* Resources externally exposed for out-sourced projects require separation from internal corporate environments
* Healthcare organizations must ensure patient record confidentiality.
* Universities need to partition student user services from business operations, student administrative systems, and commercial or sensitive research projects.
* Service providers must separate billing, CRM, payment systems, reseller portals, and hosted environments.
* Financial organizations need to securely isolate client records and investment, wholesale, and retail banking services.
* Government agencies must partition revenue records, judicial data, social services, operational systems, and so on.

**Secure Configuration of Hardware**

* Private and public cloud providers must enable all customer data, communication, and application environments to be securely separated, protected, and isolated from other tenants. To accomplish these goals, all hardware inside the datacenter will need to be securely configured. This includes:
  + BEST PRACTICES FOR SERVERS
    - Secure build: To implement fully, follow the specific recommendations of the operating system vendor to securely deploy their operating system.
    - Secure initial configuration: This may mean many different things depending on a number of variables, such as OS vendor, operating environment, business requirements, regulatory requirements, risk assessment, and risk appetite, as well as workload(s) to be hosted on the system
    - Secure ongoing configuration maintenance: Achieved through a variety of mechanisms, some vendor-specific, some not.
  + BEST PRACTICES FOR STORAGE CONTROLLERS
    - Initiator: The consumer of storage, typically a server with an adapter card in it called a Host Bus Adapter (HBA). The initiator “initiates” a connection over the fabric to one or more ports on your storage system, which are called target ports.
    - Target: The ports on your storage system that deliver storage volumes (called target devices or LUNs) to the initiators.
    - iSCSI traffic should be segregated from general traffic. Layer-2 VLANs are a particularly good way to implement this segregation.
    - Oversubscription is permissible on general-purpose LANs, but you should not use an oversubscribed configuration for iSCSI.
    - iSCSI Implementation Considerations
  + NETWORK CONTROLLERS BEST PRACTICES
    - Major differences between physical and virtual switches
    - With a physical switch, when a dedicated network cable or switch port goes bad, only one server goes down
    - with virtualization, one cable could offer connectivity to 10 or more virtual machines (VMs), causing a loss in connectivity to multiple VMs.
    - connecting multiple VMs requires more bandwidth, which must be handled by the virtual switch.
  + VIRTUAL SWITCHES BEST PRACTICES
    - Redundancy is achieved by assigning at least two physical NICs to a virtual switch with each NIC connecting to a different physical switch.
    - Network Isolation
    - The network that is used to move live virtual machines from one host to another does so in clear text. That means it may be possible to “sniff” the data or perform a man-in-the-middle attack when a live migration occurs.
    - When dealing with internal and external networks, always create a separate isolated virtual switch with its own physical network interface cards and never mix internal and external traffic on a virtual switch.
    - Lock down access to your virtual switches so that an attacker cannot move VMs from one network to another and so that VMs do not straddle an internal and external network.
    - For a better virtual network security strategy, use security applications that are designed specifically for virtual infrastructure and integrate them directly into the virtual networking layer. This includes network intrusion detection and prevention systems, monitoring and reporting systems, and virtual firewalls that are designed to secure virtual switches and isolate VMs. You can integrate physical and virtual network security to provide complete datacenter protection.
    - If you use network-based storage such as iSCSI or Network File System, use proper authentication. For iSCSI, bidirectional Challenge-Handshake Authentication Protocol (or CHAP) authentication is best. Be sure to physically isolate storage network traffic because the traffic is often sent as clear text. Anyone with access to the same network could listen and reconstruct files, alter traffic, and possibly corrupt the network.

**Installation and Configuration of Virtualization Management Tools for the Host**

* The virtualization platform will determine what management tools need to be installed on the host. The latest tools should be installed on each host, and the configuration management plan should include rules on updating these tools.
* LEADING PRACTICES
  + Defense in depth: Implement the tool(s) used to manage the host as part of a larger architectural design that mutually reinforces security at every level of the enterprise. The tool(s) should be seen as a tactical element of host management, one that is linked to operational elements such as procedures and strategic elements such as policies.
  + Access control: Secure the tool(s) and tightly control and monitor access to them.
  + Auditing/monitoring: Monitor and track the use of the tool(s) throughout the enterprise to ensure proper usage is taking place.
  + Maintenance: Update and patch the tool(s) as required to ensure compliance with all vendor recommendations and security bulletins.
* RUNNING A PHYSICAL INFRASTRUCTURE FOR CLOUD ENVIRONMENTS
  + Considerations when sharing resources include
    - Legal: Simply by sharing the environment in the cloud, you may put your data at risk of seizure. Exposing your data in an environment shared with other companies could give the government “reasonable cause” to seize your assets because another company has violated the law.
    - Compatibility: Storage services provided by one cloud vendor may be incompatible with another vendor’s services should you decide to move from one to the other.
    - Control: If information is encrypted while passing through the cloud, does the customer or cloud vendor control the encryption/decryption keys? Make sure you control the encryption/decryption keys, just as if the data were still resident in the enterprise’s own servers.
    - Log data: As more and more mission-critical processes are moved to the cloud, SaaS suppliers will have to provide log data in a real-time, straightforward manner, probably for their administrators as well as their customers’ personnel. Since the SaaS provider’s logs are internal and not necessarily accessible externally or by clients or investigators, monitoring is difficult.
    - PCI-DSS access: Since access to logs is required for Payment Card Industry Data Security Standard (PCI-DSS) compliance and may be requested by auditors and regulators, security managers need to make sure to negotiate access to the provider’s logs as part of any service agreement.
    - Upgrades and changes: Cloud applications undergo constant feature additions. The speed at which applications change in the cloud will affect both the SDLC and security. A secure SDLC may not be able to provide a security cycle that keeps up with changes that occur so quickly.
    - Failover technology: Having proper failover technology is a component of securing the cloud that is often overlooked. The company can survive if a non-mission-critical application goes offline, but this may not be true for mission-critical applications.
    - Compliance: SaaS makes the process of compliance more complicated, since it may be difficult for a customer to discern where his data resides on a network controlled by the SaaS provider, or a partner of that provider, which raises all sorts of compliance issues of data privacy, segregation, and security.
    - Regulations: Compliance with government regulations are much more challenging in the SaaS environment. The data owner is still fully responsible for compliance.
    - Outsourcing: Outsourcing means losing significant control over data, and while this is not a good idea from a security perspective, the business ease and financial savings will continue to increase the usage of these services. You need to work with your company’s legal staff to ensure that appropriate contract terms are in place to protect corporate data and provide for acceptable service level agreements.
    - Placement of security: Cloud-based services will result in many mobile IT users accessing business data and services without traversing the corporate network. This will increase the need for enterprises to place security controls between mobile users and cloud-based services. Placing large amounts of sensitive data in a globally accessible cloud leaves organizations open to large, distributed threats. Attackers no longer have to come onto the premises to steal data, and they can find it all in the one “virtual” location.
    - Virtualization: Virtualization efficiencies in the cloud require virtual machines from multiple organizations to be co-located on the same physical resources. Although traditional datacenter security still applies in the cloud environment, physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server. Administrative access is through the Internet rather than the controlled and restricted direct or on-premises connection that is adhered to in the traditional datacenter model. This increases risk and exposure and will require stringent monitoring for changes in system control and access control restriction.
    - Virtual machine: The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure that records can be audited. The ease of cloning and distribution between physical servers could result in the propagation of configuration errors and other vulnerabilities. Proving the security state of a system and identifying the location of an insecure virtual machine will be challenging. The co-location of multiple virtual machines increases the attack surface and risk of virtual machine-to-virtual machine compromise.
    - Operating system and application files: Operating system and application files are on a shared physical infrastructure in a virtualized cloud environment and require system, file, and activity monitoring to provide confidence and auditable proof to enterprise customers that their resources have not been compromised or tampered with. In the cloud computing environment, the enterprise subscribes to cloud computing resources, and the responsibility for patching is the subscriber’s rather than the cloud computing vendor’s. The need for patch maintenance vigilance is imperative. Lack of due diligence in this regard could rapidly make the task unmanageable or impossible.
    - Data fluidity: Enterprises are often required to prove that their security compliance is in accord with regulations, standards, and auditing practices, regardless of the location of the systems at which the data resides. Data is fluid in cloud computing and may reside in on-premises physical servers, on-premises virtual machines, or off-premises virtual machines running on cloud computing resources, and this will require some rethinking on the part of auditors and practitioners alike.
* CONFIGURING ACCESS CONTROL AND SECURE KVM
  + Isolated data channels: Located in each KVM port and make it impossible for data to be transferred between connected computers through the KVM.
  + Tamper-warning labels on each side of the KVM: These provide clear visual evidence if the enclosure has been compromised
  + Housing intrusion detection: Causes the KVM to become inoperable and the LEDs to flash repeatedly if the housing has been opened.
  + Fixed firmware: Cannot be reprogrammed, preventing attempts to alter the logic of the KVM.
  + Tamper-proof circuit board: It’s soldered to prevent component removal or alteration.
  + Safe buffer design: Does not incorporate a memory buffer, and the keyboard buffer is automatically cleared after data transmission, preventing transfer of keystrokes or other data when switching between computers.
  + Selective USB access: Only recognizes human interface device USB devices (such as keyboards and mice) to prevent inadvertent and insecure data transfer.
  + Push-button control: Requires physical access to KVM when switching between connected computers.

**Securing the Network Configuration**

* NETWORK ISOLATION
  + All networks should be monitored and audited to validate separation.
  + All management of the datacenter systems should be done on isolated networks. Strong authentication methods should be used on the management network to validate identity and authorize usage
  + Access to the storage controllers should also be granted over isolated network components that are non-routable to prevent the direct download of stored data and to restrict the likelihood of unauthorized access or accidental discovery.
  + Customer access should be provisioned on isolated networks. This isolation can be implemented through the use of physically separate networks or via VLANs.
  + TLS and IPSec can be used for securing communications in order to prevent eavesdropping.
  + Secure DNS (DNSSEC) should be used to prevent DNS poisoning.
* PROTECTING VLANS
  + VLAN Communication
    - Broadcast packets sent by one of the workstations will reach all the others in the VLAN.
    - Broadcasts sent by one of the workstations in the VLAN will not reach any workstations that are not in the VLAN.
    - Broadcasts sent by workstations that are not in the VLAN will never reach workstations that are in the VLAN.
    - The workstations can all communicate with each other without needing to go through a gateway.
  + VLAN Advantages
    - The ability to isolate network traffic to certain machines or groups of machines via association with the VLAN allows for the opportunity to create secured pathing of data between endpoints
    - It is a building block that when combined with other protection mechanisms allows for data confidentiality to be achieved.
* USING TRANSPORT LAYER SECURITY (TLS)
  + TLS is made up of two layers:
    - TLS record protocol: Provides connection security and ensures that the connection is private and reliable. Used to encapsulate higher-level protocols, among them TLS handshake protocol.
    - TLS handshake protocol: Allows the client and the server to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is sent or received.
* USING DOMAIN NAME SYSTEM (DNS)
  + Domain Name System Security Extensions (DNSSEC)
    - DNSSEC provides origin authority, data integrity, and authenticated denial-of-existence.
    - Validation of DNS responses occurs through the use of digital signatures that are included with DNS responses
  + Threats to the DNS Infrastructure
    - Footprinting: The process by which DNS zone data, including DNS domain names, computer names, and Internet Protocol (IP) addresses for sensitive network resources, is obtained by an attacker.
    - Denial-of-service attack: When an attacker attempts to deny the availability of network services by flooding one or more DNS servers in the network with queries.
    - Data modification: An attempt by an attacker to spoof valid IP addresses in IP packets that the attacker has created. This gives these packets the appearance of coming from a valid IP address in the network. With a valid IP address the attacker can gain access to the network and destroy data or conduct other attacks.
    - Redirection: When an attacker can redirect queries for DNS names to servers that are under the control of the attacker.
    - Spoofing: When a DNS server accepts and uses incorrect information from a host that has no authority giving that information. DNS spoofing is in fact malicious cache poisoning where forged data is placed in the cache of the name servers.
    - Cache poisoning: Attackers sometimes exploit vulnerabilities or poor configuration choices in DNS servers, bug, vulnerabilities in the DNS protocol itself – to inject fraudulent addressing information into caches. Users accessing the cache to visit the targeted site would find themselves instead at a server controlled by the attacker.
    - Typosquatting: The practice of registering a domain name that is confusingly similar to an existing popular brand – typosquatting
* USING INTERNET PROTOCOL SECURITY (IPSEC)
  + Supports
    - network-level peer authentication
    - data origin authentication
    - data integrity
    - encryption
    - replay protection
  + Challenges
    - Configuration management
    - Performance

**Identifying and Understanding Server Threats**

* OS bugs, missconfiguration
* Threat actors
* General guidelines should be addressed when identifying and understanding threats
  + Use an asset management system that has configuration management capabilities to enable documentation of all system configuration items (CIs) authoritatively.
  + Use system baselines to enforce configuration management throughout the enterprise. In configuration management
    - A “baseline” is an agreed-upon description of the attributes of a product, at a point in time that serves as a basis for defining change.
    - A “change” is a movement from this baseline state to a next state.
    - Consider automation technologies that will help with the creation, application, management, updating, tracking, and compliance checking for system baselines.
    - Develop and use a robust change management system to authorize the required changes that need to be made to systems over time.
    - The use of an exception reporting system to force the capture and documentation of any activities undertaken that are contrary to the “expected norm” with regard to the lifecycle of a system under management.
    - The use of vendor-specified configuration guidance and best practices as appropriate based on the specific platform(s) under management.

**Using Stand-Alone Hosts**

* The business seeks to
  + Create isolated, secured, dedicated hosting of individual cloud resources; the use of a stand-alone host would be an appropriate choice.
  + Make the cloud resources available to end users so they appear as if they are independent of any other resources and are “isolated”; either a stand-alone host or a shared host configuration that offers multi-tenant secured hosting capabilities would be appropriate
* Stand-alone host availability considerations
  + Regulatory issues
  + Current security policies in force
  + Any contractual requirements that may be in force for one or more systems, or areas of the business
  + The needs of a certain application or business process that may be using the system in question
  + The classification of the data contained in the system

**Using Clustered Hosts**

* RESOURCE SHARING
  + Reservations
  + Limits
  + Shares
* DISTRIBUTED RESOURCE SCHEDULING (DRS)/COMPUTE RESOURCE SCHEDULING
  + Provide highly available resources to your workloads
  + Balance workloads for optimal performance
  + The initial workload placement across the cluster as a VM is powered on is the beginning point for all load-balancing operations.
  + Load balancing is achieved through a movement of the VM between hosts in the cluster in order to achieve/maintain the desired compute resource allocation thresholds specified for the DRS service.
  + Scale and manage computing resources without service disruption

**Accounting for Dynamic Operation**

* In outsourced and public deployment models, cloud computing also can provide elasticity. This refers to the ability for customers to quickly request, receive, and later release as many resources as needed.
* If an organization is large enough and supports a sufficient diversity of workloads, an on-site private cloud may be able to provide elasticity to clients within the consumer organization.
* Smaller on-site private clouds will, exhibit maximum capacity limits similar to those of traditional datacenters.

**Using Storage Clusters**

* CLUSTERED STORAGE ARCHITECTURES
  + A tightly coupled cluster has a physical backplane into which controller nodes connect. While this backplane fixes the maximum size of the cluster, it delivers a high-performance interconnect between servers for load-balanced performance and maximum scalability as the cluster grows.
  + A loosely coupled cluster offers cost-effective building blocks that can start small and grow as applications demand. A loose cluster offers performance, I/O, and storage capacity within the same node. As a result, performance scales with capacity and vice versa.
* STORAGE CLUSTER GOALS
  + Meet the required service levels as specified in the SLA
  + Provide for the ability to separate customer data in multi-tenant hosting environments
  + Securely store and protect data through the use of confidentiality, integrity, and availability mechanisms such as encryption, hashing, masking, and multi-pathing

**Using Maintenance Mode**

* Maintenance mode can apply to both data stores as well as hosts
* Maintenance mode is tied to is the SLA.
* Enter maintenance mode, operate within it, and exit it successfully using the vendor-specific guidance and best practices.

**Providing High Availability on the Cloud**

* MEASURING SYSTEM AVAILABILITY
* HIGH AVAILABILITY APPROACHES
  + the use of redundant architectural elements to safeguard data in case of failure, such as a drive mirroring solution.
  + the use of multiple vendors within the cloud architecture to provide the same services. This allows you to build certain systems that need a specified level of availability to be able to switch, or failover, to an alternate provider’s system within the specified time period defined in the SLA that is used to define and manage the availability window for the system.

**The Physical Infrastructure for Cloud Environments**

* An infrastructure built for cloud computing provides numerous benefits
  + Flexible and efficient utilization of infrastructure investments
  + Faster deployment of physical and virtual resources
  + Higher application service levels
  + Less administrative overhead
  + Lower infrastructure, energy, and facility costs
  + Increased security
* Servers
* Virtualization
* Storage
* Network
* Management
* Security
* Backup and recovery
* Infrastructure systems

**Configuring Access Control for Remote Access**

* Some of the threats with regard to remote access are as follows
  + Lack of physical security controls
  + Unsecured networks
  + Infected endpoints accessing the internal network
  + External access to internal resources
* Controlling remote access
  + Tunneling via a VPN—IPSec or SSL
  + Remote Desktop Protocol (RDP) allows for desktop access to remote systems
  + Access via a secure terminal
  + Deployment of a DMZ
* Cloud environment access requirements
  + Encrypted transmission of all communications between the remote user and the host
  + Secure login with complex passwords and/or certificate-based login
  + Two-factor authentication providing enhanced security
  + A log and audit of all connection
  + A secure baseline should be established, and all deployments and updates should be made from a change- and version-controlled master image.
  + Sufficient supporting infrastructure and tools should be in place to allow for the patching and maintenance of relevant infrastructure without any impact on the end user/customer.

**Performing Patch Management**

* THE PATCH MANAGEMENT PROCESS
  + Vulnerability detection and evaluation by the vendor
  + Subscription mechanism to vendor patch notifications
  + Severity assessment of the patch by the receiving enterprise using that software
  + Applicability assessment of the patch on target systems
  + Opening of tracking records in case of patch applicability
  + Customer notification of applicable patches, if required
  + Change management
  + Successful patch application verification
  + Issue and risk management in case of unexpected troubles or conflicting actions
  + Closure of tracking records with all auditable artifacts
* EXAMPLES OF AUTOMATION
  + Notification Automation
    - Vulnerability severity is assessed
    - A security patch or an interim solution is provided
    - This information is entered into a system
    - Automated e-mail notifications are sent to predefined accounts in a straightforward process
  + Security patch applicability
  + The creation of tracking records and their assignment to predefined resolver groups, in case of matching.
  + Change record creation, change approval, and change implementation (if agreed-upon maintenance windows have been established and are being managed via SLAs).
  + Verification of the successful implementation of security patches.
  + Creation of documentation to support that patching has been successfully accomplished.
* CHALLENGES OF PATCH MANAGEMENT
  + The lack of service standardization. For enterprises transitioning to the cloud, lack of standardization is the main issue. For example, a patch management solution tailored to one customer often cannot be used or easily adopted by another customer.
  + Patch management is not simply using a patch tool to apply patches to endpoint systems, but rather, a collaboration of multiple management tools and teams, for example, change management and patch advisory tools.
  + In a large enterprise environment, patch tools need to be able to interact with a large number of managed entities in a scalable way and handle the heterogeneity that is unavoidable in such environments.
  + To avoid problems associated with automatically applying patches to endpoints, thorough testing of patches beforehand is absolutely mandatory.
  + Multiple Time Zones
    - In a cloud environment, virtual machines that are physically located in the same time zone can be configured to operate in different time zones. When a customer’s VMs span multiple time zones, patches need to be scheduled carefully so the correct behavior is implemented.
    - For some patches, the correct behavior is to apply the patches at the same local time of each virtual machine
    - For other patches, the correct behavior is to apply at the same absolute time to avoid mixed-mode problem where multiple versions of a software are concurrently running, resulting in data corruption.
  + VM Suspension and Snapshot
    - There are additional modes of operations available to system administrators and users, such as VM suspension and resume, snapshot, and revert back. The management console that allows use of these operations needs to be tightly integrated with the patch management and compliance processes.

**Performance Monitoring**

* OUTSOURCING MONITORING
  + Having HR check references
  + Examining the terms of any SLA or contract being used to govern service terms
  + Executing some form of trial of the managed service in question before implementing into production
* HARDWARE MONITORING
  + Extend monitoring of the four key subsystems
    - Network: Excessive dropped packets
    - Disk: Full disk or slow reads and writes to the disks (IOPS)
    - Memory: Excessive memory usage or full utilization of available memory allocation
    - CPU: Excessive CPU utilization
  + Additional items that exist in the physical plane of these systems, such as CPU temperature, fan speed, and ambient temperature within the datacenter hosting the physical hosts.
* REDUNDANT SYSTEM ARCHITECTURE
  + Allow for additional hardware items to be incorporated directly into the system as either an online real-time component
  + Share the load of the running system, or in a hot standby mode
  + Allow for a controlled failover, to minimize downtime
* MONITORING FUNCTIONS
  + The use of any vendor-supplied monitoring capabilities to their fullest extent is necessary in order to maximize system reliability and performance.
  + Monitoring hardware may provide early indications of hardware failure and should be treated as a requirement to ensure stability and availability of all systems being managed.
  + Some virtualization platforms offer the capability to disable hardware and migrate live data from the failing hardware if certain thresholds are met.

**Backing Up and Restoring the Host Configuration challenges**

* Control: The ability to decide, with high confidence, who and what is allowed to access consumer data and programs and the ability to perform actions (such as erasing data or disconnecting a network) with high confidence both that the actions have been taken and that no additional actions were taken that would subvert the consumer’s intent
* Visibility: The ability to monitor, with high confidence, the status of a consumer’s data and programs and how consumer data and programs are being accessed by others.

**Implementing Network Security Controls: Defense in Depth**

* FIREWALLS
  + Host-Based Software Firewalls
  + Configuration of Ports Through the Firewall
* LAYERED SECURITY
  + Intrusion Detection System
    - Network Intrusion Detection Systems (NIDSs)
    - Host Intrusion Detection Systems (HIDSs)
  + Intrusion Prevention System
    - It can reconfigure other security controls, such as a firewall or router, to block an attack; some IPS devices can even apply patches if the host has particular vulnerabilities.
    - Some IPS can remove the malicious contents of an attack to mitigate the packets, perhaps deleting an infected attachment from an e-mail before forwarding the e-mail to the user.
  + Combined IDS and IPS (IDPS)
* UTILIZING HONEYPOTS
* CONDUCTING VULNERABILITY ASSESSMENTS
  + conduct external vulnerability assessments to validate any internal assessments.
* LOG CAPTURE AND LOG MANAGEMENT
  + Log data should be
    - Protected and consideration given to the external storage of log data
    - Part of the backup and disaster recovery plans of the organization
  + NIST SP 800-92 recommendations
    - Develop standard processes for performing log management.
    - Define its logging requirements and goals as part of the planning process.
    - Develop policies that clearly define mandatory requirements and suggested recommendations for log management activities, including log generation, transmission, storage, analysis, and disposal.
    - Ensure that related policies and procedures incorporate and support the log management requirements and recommendations.
  + Organizations should prioritize log management appropriately throughout the organization. After an organization defines its requirements and goals for the log management process, it should prioritize the requirements and goals based on the perceived reduction of risk and the expected time and resources needed to perform log management functions.
  + Organizations should create and maintain a log management infrastructure. A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data. They typically perform several functions that support the analysis and security of log data.
    - Major factors to consider in the design
  + Organizations should establish standard log management operational processes. The major log management operational processes typically include configuring log sources, performing log analysis, initiating responses to identified events, and managing long-term storage. Administrators have other responsibilities as well, such as the following:
    - Monitoring the logging status of all log sources
    - Monitoring log rotation and archival processes
    - Checking for upgrades and patches to logging software and acquiring, testing, and deploying them
    - Ensuring that each logging host’s clock is synched to a common time source
    - Reconfiguring logging as needed based on policy changes, technology changes, and other factors
    - Documenting and reporting anomalies in log settings, configurations, and processes
* USING SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)
  + A locally hosted SIEM system offers easy access and lower risk of external disclosure
  + An external SIEM system may prevent tampering of data by an attacker
  + Sample Controls and Effective Mapping to an SIEM Solution <https://www.cisecurity.org/critical-controls/download.cfm>
    - Critical Control 1: Inventory of Authorized and Unauthorized Devices
    - Critical Control 2: Inventory of Authorized and Unauthorized Software
    - Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
    - Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
    - Critical Control 12: Controlled Use of Administrative Privileges
    - Critical Control 13: Boundary Defense

**Developing a Management Plan**

* MAINTENANCE
  + schedule system repair and maintenance
  + schedule customer notifications
  + ensure adequate resources are available to meet expected demand and service level agreement requirements
  + ensure that appropriate change-management procedures are implemented and followed
  + ensure all appropriate security protections and safeguards continue to apply to all hosts while in maintenance mode and to all virtual machines while they are being moved and managed on alternate hosts as a result of maintenance mode activities being performed on their primary host.
* ORCHESTRATION

**Building a Logical Infrastructure for Cloud Environments**

* LOGICAL DESIGN
  + Lacks specific details such as technologies and standards while focusing on the needs at a general level
  + Communicates with abstract concepts, such as a network, router, or workstation, without specifying concrete details
* PHYSICAL DESIGN
  + Is created from a logical network design
  + Will often expand elements found in a logical design
* SECURE CONFIGURATION OF HARDWARE-SPECIFIC REQUIREMENTS
  + Storage Controllers Configuration
    - Turn off all unnecessary services, such as web interfaces and management services that will not be needed or used.
    - Validate that the controllers can meet the estimated traffic load based on vendor specifications and testing (1 GB | 10 GB | 16 GB | 40 GB).
    - Deploy a redundant failover configuration such as a NIC team.
    - Deploy a multipath solution.
    - Change default administrative passwords for configuration and management access to the controller.
  + Networking Models
    - Traditional Networking Model
    - Converged Networking Model

**Running a Logical Infrastructure for Cloud Environments**

* BUILDING A SECURE NETWORK CONFIGURATION
  + VLANs: Allow for the logical isolation of hosts on a network. In a cloud environment, VLANs can be utilized to isolate the management network, storage network, and the customer networks. VLANs can also be used to separate customer data.
  + Transport Layer Security (TLS): Allows for the encryption of data in transit between hosts. Implementation of TLS for internal networks will prevent the “sniffing” of traffic by a malicious user. A TLS VPN is one method to allow for remote access to the cloud environment.
  + DNS: DNS servers should be locked down and only offer required services and utilize Domain Name System Security Extensions (DNSSEC) when feasible. DNSSEC is a set of DNS extensions that provide authentication, integrity, and “authenticated denial-of-existence” for DNS data. Zone transfers should be disabled. If an attacker comprises DNS, they may be able to hijack or reroute data.
  + IPSec: IPSec VPN is one method to remotely access the cloud environment. If an IPSec VPN is utilized, IP whitelisting, only allowing approved IP addresses, is considered a best practice for access. Two-factor authentication can also be used to enhance security.
* OS HARDENING VIA APPLICATION BASELINE
  + Capturing a Baseline
    - A clean installation of the target OS must be performed (physical or virtual).
    - All non-essential services should be stopped and set to disabled in order to ensure that they do not run.
    - All non-essential software should be removed from the system.
    - All required security patches should be downloaded and installed from the appropriate vendor repository.
    - All required configuration of the host OS should be accomplished per the requirements of the baseline being created.
    - The OS baseline should be audited to ensure that all required items have been configured properly.
    - Full documentation should be created, captured, and stored for the baseline being created.
    - An image of the OS baseline should be captured and stored for future deployment. This image should be placed under change management control and have appropriate access controls applied.
    - The baseline OS image should also be placed under the Configuration Management system and cataloged as a Configuration Item (CI).
    - The baseline OS image should be updated on a documented schedule for security patches and any additional required configuration updates as needed.
  + Baseline Configuration by Platform
    - Windows
    - Linux
    - VMware
* AVAILABILITY OF A GUEST OS
  + High availability should be used where the goal is to minimize the impact of system downtime
  + Fault tolerance should be used where the goal is to eliminate system downtime as a threat to system availability altogether

**Managing the Logical Infrastructure for Cloud Environments**

* ACCESS CONTROL FOR REMOTE ACCESS
  + Key benefits of a remote access solution for the cloud can include
    - Secure access without exposing the privileged credential to the end user, eliminating the risk of credential exploitation or key logging.
    - Accountability of who is accessing the datacenter remotely with a tamper-proof audit trail.
    - Session control over who can access, enforcement of workflows such as managerial approval, ticketing integration, session duration limitation, and automatic termination when idle.
    - Real-time monitoring to view privileged activities as they are happening or as a recorded playback for forensic analysis. Sessions can be remotely terminated or intervened with when necessary for more efficient and secure IT compliance and cyber security operations.
    - Secure isolation between the remote user’s desktop and the target system they are connecting to so that any potential malware does not spread to the target systems.
* OS BASELINE COMPLIANCE MONITORING AND REMEDIATION
* BACKING UP AND RESTORING THE GUEST OS CONFIGURATION

**Implementation of Network Security Controls**

* LOG CAPTURE AND ANALYSIS
  + Log data needs to be collected and analyzed both for the hosts as well as for the guest
  + Centralization and offsite storage of log data can prevent tampering provided the appropriate access controls and monitoring systems are put in place.
* MANAGEMENT PLAN IMPLEMENTATION THROUGH THE MANAGEMENT PLANE
* ENSURING COMPLIANCE WITH REGULATIONS AND CONTROLS
  + Establishing explicit, comprehensive SLAs for security, continuity of operations, and service quality is key for any organization.
  + Compliance responsibilities of the provider and the customer should be clearly delineated in contracts and SLAs.
  + Consider the provider and customers’ geographic locations.
  + certain agreements focusing on premise service provisioning may be in place but not structured appropriately to encompass a full cloud services solution

**Using an IT Service Management (ITSM) Solution**

* Ensure portfolio management, demand management, and financial management are all working together for efficient service delivery to customers and effective charging for services if appropriate
* Involve all the people and systems necessary to create alignment and ultimately success

**Considerations for Shadow IT**

* Shadow IT expenditures backup 44%
* Shadow IT expenditures file sharing SW 36%
* Shadow IT expenditures archiving 33%

**Operations Management**

* INFORMATION SECURITY MANAGEMENT
  + Security management
  + Security policy
  + Information security organization
  + Asset management
  + Human resources security
  + Physical and environmental security
  + Communications and operations management
  + Access control
  + Information systems acquisition, development, and maintenance
  + Provider and customer responsibilities
* CONFIGURATION MANAGEMENT
  + The development and implementation of new configurations; they should apply to the hardware and software configurations of the cloud environment
  + Quality evaluation of configuration changes and compliance with established security baselines
  + Changing systems, including testing and deployment procedures; they should include adequate oversight of all configuration changes
  + The prevention of any unauthorized changes in system configurations
* CHANGE MANAGEMENT
  + Change-Management Objectives
    - Respond to a customer’s changing business requirements while maximizing value and reducing incidents, disruption, and re-work.
    - Respond to business and IT requests for change that will align services with business needs.
    - Ensure that changes are recorded and evaluated.
    - Ensure that authorized changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner.
    - Ensure that all changes to configuration items are recorded in the configuration management system.
    - Optimize overall business risk. It is often correct to minimize business risk, but sometimes it is appropriate to knowingly accept a risk because of the potential benefit.
  + Change-Management Process
    - The development and acquisition of new infrastructure and software
    - Quality evaluation of new software and compliance with established security baselines
    - Changing systems, including testing and deployment procedures; they should include adequate oversight of all changes
    - Preventing the unauthorized installation of software and hardware
* INCIDENT MANAGEMENT
  + Event vs. Incidents
    - An event is defined as a change of state that has significance for the management of an IT service or other configuration item. The term can also be used to mean an alert or notification created by an IT service, configuration item, or monitoring tool. Events often require IT operations staff to take actions and lead to incidents being logged.
    - An incident is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service.
  + Purpose of Incident Response
    - Restore normal service operation as quickly as possible
    - Minimize the adverse impact on business operations
    - Ensure service quality and availability are maintained
  + Objectives of Incident Response
    - Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation ongoing management, and reporting of incidents
    - Increase visibility and communication of incidents to business and IT support staff
    - Enhance business perception of IT by using professional approach in quickly resolving and communicating incidents when they occur
    - Align incident management activities with those of the business
    - Maintain user satisfaction
  + Incident Management Plan
    - Definitions of an incident by service type or offering
    - Customer and provider roles and responsibilities for an incident
    - Incident management process from detection to resolution
    - Response requirements
    - Media coordination
    - Legal and regulatory requirements such as data breach notification
  + Incident Classification
    - Impact = Effect upon the business
    - Urgency = Extent to which the resolution can bear delay
    - Priority = Urgency x Impact
* PROBLEM MANAGEMENT
  + A problem is the unknown cause of one or more incidents, often identified as a result of multiple similar incidents.
  + A known error is an identified root cause of a problem.
  + A workaround is a temporary way of overcoming technical difficulties (i.e., incidents or problems).
* RELEASE AND DEPLOYMENT MANAGEMENT
  + Define and agree upon deployment plans
  + Create and test release packages
  + Ensure integrity of release packages
  + Record and track all release packages in the Definitive Media Library (DML)
  + Manage stakeholders
  + Check delivery of utility and warranty (utility + warranty = value in the mind of the customer)
  + Utility is the functionality offered by a product or service to meet a specific need; it’s what the service does.
  + Warranty is the assurance that a product or service will meet agreed-upon requirements (SLA); it’s how the service is delivered.
  + Manage risks
  + Ensure knowledge transfer
* SERVICE LEVEL MANAGEMENT
  + Service level agreements (SLAs) are negotiated with the customers.
  + Operational level agreements (OLAs) are SLAs negotiated between internal business units within the enterprise.
  + Underpinning Contracts (UCs) are external contracts negotiated between the organization and vendors or suppliers.
* AVAILABILITY MANAGEMENT
* CAPACITY MANAGEMENT
* BUSINESS CONTINUITY MANAGEMENT
  + The difference between BC and BCM <https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en>
    - Business continuity (BC) is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. (Source: ISO 22301:2012)
    - Business continuity management (BCM) is defined as a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and that provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities. (Source: ISO 22301:2012)
  + Continuity Management Plan
    - Required capability and capacity of backup systems
    - Trigger events to implement the plan
    - Clearly defined roles and responsibilities by name and title
    - Clearly defined continuity and recovery procedures
    - Notification requirements
* CONTINUAL SERVICE IMPROVEMENT (CSI) MANAGEMENT
* HOW MANAGEMENT PROCESSES RELATE TO EACH OTHER
  + Release and Deployment Management and Change Management
  + Release and Deployment Management Role and Incident and Problem Management
  + Release and Deployment Management and Configuration Management
  + Release and Deployment Management Is Related to Availability Management
  + Release and Deployment Management and the Help/Service Desk
  + Configuration Management and Availability Management
  + Configuration Management and Change Management
  + Service Level Management and Change Management
* INCORPORATING MANAGEMENT PROCESSES

**Managing Risk in Logical and Physical Infrastructures**[**http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf**](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf)

* FRAMING RISK
* RISK ASSESSMENT
  + Risk
    - Threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations
    - Vulnerabilities internal and external to organizations
    - The harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities
    - The likelihood that harm will occur
  + Conducting a Risk Assessment
    - Qualitative Risk Assessment
    - Quantitative assessments
    - Identifying Vulnerabilities
    - Identifying Threats
    - Selecting Tools and Techniques for Risk Assessment
    - Likelihood Determination
    - Determination of Impact
    - Determination of Risk
    - Critical Aspects of Risk Assessment: at least cover following
* RISK RESPONSE
  + Developing alternative courses of action for responding to risk
  + Evaluating the alternative courses of action
  + Determining appropriate courses of action consistent with organizational risk tolerance
  + Implementing risk responses based on selected courses of action
    - Risk can be accepted
    - Risk can be avoided
    - Risk can be transferred
    - Risk can be mitigated
* RISK MONITORING
  + Determine the ongoing effectiveness of risk responses (consistent with the organizational risk frame)
  + Identify risk-impacting changes to organizational information systems and the environments in which the systems operate
  + Verify that planned risk responses are implemented and information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied

**Collection and Preservation of Digital Evidence**

* CLOUD FORENSICS CHALLENGES
  + Control over data
  + Multi-tenancy
  + Data volatility
    - Chain of custody
  + Evidence acquisition
* DATA ACCESS WITHIN SERVICE MODELS
  + SaaS
    - Access Control
  + PaaS
    - Data
    - Application
    - Access Control
  + IaaS
    - OS
    - Middleware
    - Runtime
    - Data
    - Application
    - Access Control
  + Local
    - Networking
    - Storage
    - Servers
    - Virtualization
    - OS
    - Middleware
    - Runtime
    - Data
    - Application
    - Access Control
* FORENSICS READINESS
  + Performing regular backups of systems and maintaining previous backups for a specific period of time
  + Enabling auditing on workstations, servers, and network devices
  + Forwarding audit records to secure centralized log servers
  + Configuring mission-critical applications to perform auditing, including recording all authentication attempts
  + Maintaining a database of file hashes for the files of common OS and application deployments, and using file integrity checking software on particularly important assets
  + Maintaining records (e.g., baselines) of network and system configurations
  + Establishing data-retention policies that support performing historical reviews of system and network activity, complying with requests or requirements to preserve data relating to ongoing litigation and investigations, and destroying data that is no longer needed
* PROPER METHODOLOGIES FOR FORENSIC COLLECTION OF DATA
  + Collection
    - Data Acquisition
    - Challenges
    - Additional Steps
    - Collecting Data from a Host OS
    - Collecting Data from a Guest OS
    - Collecting Metadata
    - Examination
      * Bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms
      * Using text and pattern searches to identify pertinent data, such as finding documents that mention a particular subject or person or identifying e-mail log entries for a particular e-mail address
      * Using a tool that can determine the type of contents of each data file, such as text, graphics, music, or a compressed file archive
      * Using knowledge of data file types to identify files that merit further study, as well as to exclude files that are of no interest to the examination
      * Using any databases containing information about known files to include or exclude files from further consideration
  + Analysis
    - Should include identifying people, places, items, and events and determining how these elements are related so that a conclusion can be reached. Often, this effort will include correlating data among multiple sources.
  + Reporting
    - Alternative explanations
    - Audience consideration
    - Actionable information
* THE CHAIN OF CUSTODY
  + When an item is gathered as evidence, that item should be recorded in an evidence log with a description, the signature of the individual gathering the item, a signature of a second individual witnessing the item being gathered, and an accurate time and date.
  + Whenever that item is stored, the location in which the item is stored should be recorded, along with the item’s condition. The signatures of the individual placing the item in storage and of the individual responsible for that storage location should also be included, along with an accurate time and date.
  + Whenever an item is removed from storage, it should be recorded, along with the item’s condition and the signatures of the person removing the item and the person responsible for that storage location, along with an accurate time and date.
  + Whenever an item is transported, that item’s point of origin, method of transport, and the item’s destination should be recorded, as well as the item’s condition at origination and destination. Also record the signatures of the people performing the transportation and a responsible party at the origin and destination witnessing its departure and arrival, along with accurate times and dates for each.
  + Whenever any action, process, test, or other handling of an item is to be performed, a description of all such actions to be taken, and the person(s) who will perform such actions, should be recorded. The signatures of the person taking the item to be tested and of the person responsible for the items storage should be recorded, along with an accurate time and date.
  + Whenever any action, process, test, or other handling of an item is performed, record a description of all such actions, along with accurate times and dates for each. Also record the person performing such actions, any results or findings of such actions, and the signatures of at least one person of responsibility as witness that the actions were performed as described, along with the resulting findings as described.
* EVIDENCE MANAGEMENT

**Managing Communications with Relevant Parties**

* THE FIVE WS AND ONE H
  + Who: Who is the target of the communication?
  + What: What is the communication designed to achieve?
  + When: When is the communication best delivered/most likely to reach its intended target(s)?
  + Where: Where is the communication pathway best managed from?
  + Why: Why is the communication being initiated in the first place?
  + How: How is the communication being transmitted and how is it being received?
* COMMUNICATING WITH VENDORS/PARTNERS
  + Communication paths
  + Emergency communication paths should be established and tested with all vendors.
  + Categorizing, or ranking, a vendor/supplier on some sort of scale is critical
* COMMUNICATING WITH CUSTOMERS
  + SLAs are a form of communication that clarify responsibilities
    - What percentage of the time services will be available
    - The number of users that can be served simultaneously
    - Specific performance benchmarks to which actual performance will be periodically compared
    - The schedule for notification in advance of network changes that may affect users
    - Help/service desk response time for various classes of problems
    - Remote access availability
    - Usage statistics that will be provided
* COMMUNICATING WITH REGULATORS
* COMMUNICATING WITH OTHER STAKEHOLDERS

**6. Legal and Compliance**

**International Legislation Conflicts**

* copyright law
* intellectual property
* violation of patents
* breaches of data protection
* legislative requirements
* privacy-related components

**Legislative Concepts**

* International Law
  + International conventions, whether general or particular, establishing rules expressly recognized by contesting states
  + International custom, as evidence of a general practice accepted as law
  + The general principles of law recognized by civilized nations
  + Judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law
* State Law
* Copyright/Piracy Laws
* Enforceable Governmental Request(s)
* Intellectual Property Rights
* Privacy Laws
* The Doctrine of the Proper Law
* Criminal Law
* Tort Law
  + It seeks to compensate victims for injuries suffered by the culpable action or inaction of others.
  + It seeks to shift the cost of such injuries to the person or persons who are legally responsible for inflicting them.
  + It seeks to discourage injurious, careless, and risky behavior in the future.
  + It seeks to vindicate legal rights and interests that have been compromised, diminished, or emasculated.
* Restatement (Second) Conflict of Laws

**Frameworks and Guidelines Relevant to Cloud Computing**

* ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD)—PRIVACY & SECURITY GUIDELINES
  + National privacy strategies
  + Privacy management programs
  + Data security breach notification
* ASIA PACIFIC ECONOMIC COOPERATION (APEC) PRIVACY FRAMEWORK
  + Framework that is made up of four parts,
    - Part I: Preamble
    - Part II: Scope
    - Part III: Information Privacy Principles
    - Part IV: Implementation
  + The nine principles
    - Preventing Harm
    - Notice
    - Collection Limitation
    - Use of Personal Information
    - Choice
    - Integrity of Personal Information
    - Security Safeguards
    - Access and Correction
    - Accountability
* EU DATA PROTECTION DIRECTIVE
  + It does not apply to the processing of data:
    - By a natural person in the course of purely personal or household activities
    - In the course of an activity that falls outside the scope of community law, such as operations concerning public safety, defense or state security
  + The quality of the data
  + The legitimacy of data processing
    - For the performance of a contract to which the data subject is party
    - For compliance with a legal obligation to which the controller is subject
    - In order to protect the vital interests of the data subject
    - For the performance of a task carried out in the public interest
    - For the purposes of the legitimate interests pursued by the controller
  + Special categories of processing
  + Information to be given to the data subject
  + The data subject’s right of access to data
    - Confirmation as to whether or not data relating to him/her is being processed and communication of the data undergoing processing
    - The rectification, erasure, or blocking of data the processing of which does not comply with the provisions of this directive either because of the incomplete or inaccurate nature of the data, and the notification of these changes to third parties to whom the data has been disclosed
  + Exemptions and restrictions
  + The right to object to the processing of data
  + The confidentiality and security of processing
  + The notification of processing to a supervisory authority
  + Scope
* GENERAL DATA PROTECTION REGULATION
* EPRIVACY DIRECTIVE

**Common Legal Requirements**

* United States Federal Laws
* United States State Laws
* Standards
* International Regulations and Regional Regulations
* Contractual Obligations
* Restrictions of Cross-border Transfers

**Legal Controls and Cloud Providers**

**eDiscovery**

* EDISCOVERY CHALLENGES
  + Is the cloud under your control?
  + Who is controlling or hosting the relevant data?
  + Does this mean that it is under “the provider’s” control?
* CONSIDERATIONS AND RESPONSIBILITIES OF EDISCOVERY
* REDUCING RISK
* CONDUCTING EDISCOVERY INVESTIGATIONS
  + SaaS-based eDiscovery
  + Hosted eDiscovery (provider)
  + Third-party eDiscovery

**Cloud Forensics and ISO/IEC 27050-1**

**Protecting Personal Information in the Cloud**

* PII is “any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security Number, date and place of birth, mother’s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”
* DIFFERENTIATING BETWEEN CONTRACTUAL AND REGULATED PERSONALLY IDENTIFIABLE INFORMATION (PII)
  + Contractual PII
  + Regulated PII
    - Reasons for regulation
    - Mandatory Breach Reporting
  + Contractual Components
    - Scope of processing
    - Use of subcontractors
    - Removal/deletion of data
    - Appropriate/required data security controls
    - Location(s) of data
    - Return of data/restitution of data
    - Audits/right to audit subcontractors
* COUNTRY-SPECIFIC LEGISLATION AND REGULATIONS RELATED TO PII/DATA PRIVACY/DATA PROTECTION
  + European Union
    - Directive 95/46 EC
    - EU General Data Protection Regulation 2012
    - United Kingdom and Ireland
  + Argentina
    - Argentina’s legislative basis, over and above the constitutional right of privacy, is the Personal Data Protection Act 2000. This act openly tracks the EU directive, resulting in the EU commission’s approval of Argentina as a country offering an adequate level of data protection. This means personal data can be transferred between Europe and Argentina as freely as if Argentina were part of the EEA.
  + United States
    - The Federal Trade Commission (FTC) and other associated U.S. regulators do hold that the applicable U.S. laws and regulations apply to the data after it leaves its jurisdiction, and the U.S. regulated entities remain liable for the following:
  + Safe Harbor
  + EU View on U.S. Privacy
  + The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  + The Gramm-Leach-Bliley Act (GLBA)
  + The Stored Communication Act
  + The Sarbanes-Oxley Act (SOX)
  + Australia and New Zealand
    - Regulations in Australia and New Zealand make it extremely difficult for enterprises to move sensitive information to cloud providers that store data outside of Australian/New Zealand borders. The Office of the Australian Information Commissioner (OAIC) provides oversight and governance on data privacy regulations of sensitive personal information.
    - The Australian National Privacy Act of 1988 provides guidance and regulates how organizations collect, store, secure, process, and disclose personal information. It lists the National Privacy Principles (NPP) to ensure that organizations holding personal information handle and process it responsibly.
    - Within the privacy principles, the following components are addressed for personal information:
    - Since March 2014, the revised Privacy Amendment Act introduces a set of new principles, focusing on the handling of personal information, now called the Australian Privacy Principles (APPs).
  + Russia
    - Data Localization Law valid from September 1, 2015
  + Switzerland
    - Data Processing by Third Parties
    - Transferring Personal Data Abroad
    - Data Security

**Auditing in the Cloud**

* INTERNAL AND EXTERNAL AUDITS
  + Internal audit acts as a third line of defense after the business/IT functions and risk management functions through
    - Independent verification of the cloud program’s effectiveness
    - Providing assurance to the board and risk management function(s) of the organization with regard to the cloud risk exposure
    - performs a number of cloud audits such as
  + Another potential source of independent verification on internal controls will be audits performed by external auditors. An external auditor’s scope varies greatly from an internal audit, whereas the external audit usually focuses on the internal controls over financial reporting.
* TYPES OF AUDIT REPORTS
  + Service Organization Controls 1 (SOC 1)
    - Users
    - Concern
    - Detail Required
  + Service Organization Controls 2 (SOC 2)
    - Users
    - Concern
    - Detail Required
    - Type 1
    - Type 2
  + Service Organization Controls 3 (SOC 3)
    - Users
    - Concern
    - Detail Required
  + Agreed Upon Procedures (AUP)
  + Cloud Security Alliance’s Security, Trust and Assurance Registry (STAR) program
  + EuroCloud Star Audit (ESCA) program
* IMPACT OF REQUIREMENT PROGRAMS BY THE USE OF CLOUD SERVICES
  + Due to the nature of the cloud, auditors need to re-think how they audit and obtain evidence to support their audit.
    - What is the universal population to sample from?
    - What would be the sampling methods in a highly dynamic environment?
    - How do you know that the virtualized server you are auditing was the same server over time?
* ASSURING CHALLENGES OF THE CLOUD AND VIRTUALIZATION
  + In order to obtain assurance and conduct appropriate auditing on the virtual machines/hypervisor, the CSP must:
    - Understand the virtualization management architecture
  + Verify systems are up to date and hardened according to best-practice standards
  + Verify configuration of hypervisor according to organizational policy
* INFORMATION GATHERING
  + Initial scoping of requirements
  + Market analysis
  + Review of services
  + Solutions assessment
  + Feasibility study
  + Supplementary evidence
  + Competitor analysis
  + Risk review/risk assessment
  + Auditing
  + Contract/service level agreement review
* AUDIT SCOPE
  + Audit Scope Statements
    - General statement of focus and objectives
    - Scope of audit (including exclusions)
    - Type of audit (certification, attestation, and so on)
    - Security assessment requirements
    - Assessment criteria (including ratings)
    - Acceptance criteria
    - Deliverables
    - Classification (confidential, highly confidential, secret, top secret, public, and so on)
    - circulation list,
    - key individuals associated with the audit
  + Audit Scope Restrictions
    - typically specify operational components, along with asset restrictions, which include acceptable times and time periods (e.g., time of day) and acceptable and non-accepted testing methods (e.g., no destructive testing).
    - indemnification of any liability for systems performance degradation, along with any other adverse effects, will be required where technical testing is being performed.
  + Gap Analysis
    - Stages that are carried out prior to commencing a gap analysis review:
    - The value of such an assessment is:
* CLOUD AUDITING GOALS
  + Ability to understand, measure, and communicate the effectiveness of cloud service provider controls and security to organizational stakeholders/executives
  + Proactively identify any control weaknesses or deficiencies, while communicating these both internally and to the cloud service provider
  + Obtain levels of assurance and verification as to the cloud service provider’s ability to meet the SLA and contractual requirements, while not relying on reporting or cloud service provider reports
* AUDIT PLANNING
  + Defining Audit Objectives
    - Document and define audit objectives
    - Define audit outputs and format
    - Define frequency and audit focus
    - Define the number of auditors and subject matter experts required
    - Ensure alignment with audit/risk management processes (internal)
  + Defining Audit Scope
    - Ensure the core focus and boundaries to which the audit will operate
    - Document list of current services/resources utilized from cloud provider(s)
    - Define key components of services (storage, utilization, processing, etc.)
    - Define cloud services to be audited (IaaS, PaaS, and SaaS)
    - Define geographic locations permitted/required
    - Define locations for audits to be undertaken
    - Define key stages to audit (information gathering, workshops, gap analysis, verification evidence, etc.)
    - Document key points of contact within the cloud service provider as well as internally
    - Define escalation and communication points
    - Define criteria and metrics to which the cloud service provider will be assessed
    - Ensure criteria is consistent with the SLA and contract
    - Factor in “busy periods” or organizational periods (financial yearend, launches, new services, etc.)
    - Ensure findings captured in previous reports or stated by the cloud service provider are actioned/verified
    - Ensure previous non-conformities/high-risk items are re-assessed/verified as part of the audit process
    - Ensure any operational or business changes internally have been captured as part of the audit plan (reporting changes, governance, etc.)
    - Agree on final reporting dates (conscious of business operations and operational availability)
    - Ensure findings are captured and communicated back to relevant business stakeholders/executives
    - Confirm report circulation/target audience
    - Document risk management/risk treatment processes to be utilized as part of any remediation plans
    - Agree on a ticketing/auditable process for remediation actions (ensuring traceability and accountability)
  + Conducting the Audit
    - Adequate staff
    - Adequate tools
    - Schedule
    - Supervision of audit
    - Reassessment
  + Refining the Audit Process/Lessons Learned
    - Ensure that approach and scope are still relevant
    - When any provider changes have occurred, these should be factored in
    - Ensure reporting details are sufficient to enable clear, concise, and appropriate business decisions to be made
    - Determine opportunities for reporting improvement/enhancement
    - Ensure that duplication of efforts is minimal (crossover or duplication with other audit/risk efforts)
    - Ensure audit criteria and scope are still accurate (factoring in business changes)
    - Have a clear understanding of what levels of information/details could be collected using automated methods/mechanisms
    - Ensure the right skillsets are available and utilized to provide accurate results and reporting
    - Ensure the Plan, Do, Check, and Act (PDCA) is also applied to the cloud service provider auditing planning/processes

**Standard Privacy Requirements (ISO/IEC 27018)**

* Consent
* Control
* Transparency
* Communication
* Independent and yearly audit

**Generally Accepted Privacy Principles (GAPP)**

* The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
* The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
* The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
* The entity collects personal information only for the purposes identified in the notice.
* The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
* The entity provides individuals with access to their personal information for review and update.
* The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
* The entity protects personal information against unauthorized access (both physical and logical).
* The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
* The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints, and disputes.

**Internal Information Security Management System (ISMS)**

* THE VALUE OF AN ISMS
  + ISMS ensures that a structured, measured, and ongoing view of security is taken across an organization, allowing security impacts and risk-based decisions to be taken. Of crucial importance is the “top-down” sponsorship and endorsement of information security across the business, highlighting its overall value and necessity.
* INTERNAL INFORMATION SECURITY CONTROLS SYSTEM: ISO 27001:2013 DOMAINS
  + A.5—Security Policy Management
  + A.6—Corporate Security Management
  + A.7—Personnel Security Management
  + A.8—Organizational Asset Management
  + A.9—Information Access Management
  + A.10—Cryptography Policy Management
  + A.11—Physical Security Management
  + A.12—Operational Security Management
  + A.13—Network Security Management
  + A.14—System Security Management
  + A.15—Supplier Relationship Management
  + A.16—Security Incident Management
  + A.17—Security Continuity Management
  + A.18—Security Compliance Management
* REPEATABILITY AND STANDARDIZATION
  + the existence and continued use of an internal ISMS will assist in standardizing and measuring security across the organization and beyond its perimeters. Given that cloud computing may well be both an internal and external solution for the organization, it is a strong recommendation that the ISMS has sight of and factors in reliance and dependencies on third parties for the delivery of business services.

**Implementing Policies**

* ORGANIZATIONAL POLICIES
  + form the basis of functional policies that can reduce the likelihood of:
    - Financial loss
    - Irretrievable loss of data
    - Reputational damage
    - Regulatory and legal consequences
    - Misuse/abuse of systems and resources
* FUNCTIONAL POLICIES
  + Information security policy
  + Information technology policy
  + Data classification policy
  + Acceptable usage policy
  + Network security policy
  + Internet use policy
  + E-mail use policy
  + Password policy
  + Virus and spam policy
  + Software security policy
  + Data backup policy
  + Disaster recovery policy
  + Remote access policy
  + Segregation of duties policy
  + Third-party access policy
  + Incident response/incident management policy
  + Human resources security policy
  + Employee background checks/screening policy
  + Legal compliance policy/guidelines
* BRIDGING THE POLICY GAPS
  + When the policy requirements cannot be fulfilled by cloud-based services, there needs to be an agreed-upon list or set of mitigation controls or techniques. You should not revise the policies to reduce or lower the requirements if at all possible. All changes and variations to policy should be explicitly listed and accepted by all relevant risk and business stakeholders.

**Identifying and Involving the Relevant Stakeholders**

* STAKEHOLDER IDENTIFICATION CHALLENGES
  + Defining the enterprise architecture (which can be a sizeable task, if not currently in place)
  + Independently/objectively viewing potential options and solutions (where individuals may be conflicted due to roles/functions)
  + Objectively selecting the appropriate service(s) and provider
  + Engaging with the users and IT personnel who will be impacted, particularly if their job is being altered or removed
  + Identifying direct and indirect costs (training, up skilling, reallocating, new tasks, responsibilities, etc.)
  + Extending of risk management and enterprise risk management
* GOVERNANCE CHALLENGES
  + Audit requirements and extension or additional audit activities
  + Verify all regulatory and legal obligations will be satisfied as part of the NDA/contract
  + Establish reporting and communication lines both internal to the organization and for cloud service provider(s)
  + Ensure that where operational procedures and processes are changed (due to use of cloud services), all documentation and evidence is updated accordingly
  + Ensure all business continuity, incident management/response, and disaster recovery plans are updated to reflect changes and interdependencies
* COMMUNICATION COORDINATION with business units should include
  + Information technology
  + Information security
  + Vendor management
  + Compliance
  + Audit
  + Risk
  + Legal
  + Finance
  + Operations
  + Data protection/privacy
  + Executive committee/directors

**Impact of Distributed IT Models**

* COMMUNICATIONS/CLEAR UNDERSTANDING
  + Traditional IT deployment and operations typically allow clear line of sight or understanding of the personnel, their roles, functions, and core areas of focus, allowing for far more access to individuals, either on a name basis or based on their roles. Communications allow for collaboration, information sharing, and the availability of relevant details and information when necessary. This can be from an operations, engineering, controls, or development.
  + Distributed IT models challenge and essentially redefine the roles, functions, and ability for “face-to-face communications” or direct interactions, such as emails, phone calls, or messengers. Distributed IT models brings structured, regimented, and standardized requests. From a security perspective, this can be seen as an enhancement in many cases, thus alleviating and removing the opportunity for untracked changes or for bypassing change management controls, along with the risks associated with implementing changes or amendments without proper testing and risk management being taken into account.
* COORDINATION/MANAGEMENT OF ACTIVITIES
  + Bringing in an independent and focused group of subject matter experts whose focus is on the delivery of such projects and functionality can make for a swift rollout or deployment.
* GOVERNANCE OF PROCESSES/ACTIVITIES
  + Effective governance allows for “peace of mind” and a level of confidence to be established in an organization. This is even more true with distributed IT and the use of IT services or solutions across dispersed organizational boundaries from a variety of users.
  + IT department may now need to pull information from a number of sources and providers, leading to
  + Increased number of sources for information
  + Varying levels of cooperation
  + Varying levels of information/completeness
  + Varying response times and willingness to assist
  + Multiple reporting formats/structures
  + Lack of cohesion in terms of activities and focus
  + Requirement for additional resources/interactions with providers
  + Minimal evidence available to support claims/verify information
  + Disruption or discontent from internal resources (where job function or role may have undergone change)
* COORDINATION IS KEY
  + Interacting with and collecting information from multiple sources places requires coordination of efforts, including defining how these processes will be managed from the outset.
* SECURITY REPORTING
  + An independent report of the security posture of the virtualized machines in a format that illustrates any high, medium, or low risks (typical of audit reports), or alternatively be based on industry ratings such as Common Vulnerabilities and Exploits (CVE) or Common Vulnerability Scoring System (CVSS) scoring.
  + Common approaches also include reporting against the OWASP Top 10 and SANS Top 20 listings.

**Implications of the Cloud to Enterprise Risk Management**

* RISK PROFILE
  + The risk profile is determined by an organization’s willingness to take risks, as well as the threats to which it is itself exposed. It should identify the level of risk to be accepted, how risks are taken, and how risk-based decision making is performed. Additionally, the risk profile should take into account potential costs and disruptions should one or more risks be exploited.
* RISK APPETITE
  + when assessing and measuring the relevant risks in cloud service offerings, it’s best to have a systematic, measurable, and pragmatic approach.
  + Many “emerging” or rapid-growth companies will be more likely to take significant risks when utilizing cloud computing services to be “first to market.”
* DIFFERENCE BETWEEN DATA OWNER/CONTROLLER AND DATA CUSTODIAN/PROCESSOR
  + The data subject is an individual who is the subject of personal data.
  + The data controller is a person who (either alone or jointly with other persons) determines the purposes for which and the manner in which any personal data are processed.
  + The data processor in relation to personal data is any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
  + Data stewards are commonly responsible for data content, context, and associated business rules.
  + Data custodians are responsible for the safe custody, transport, and storage of the data, and implementation of business rules.
  + Data owners hold the legal rights and complete control over a single piece or set of data elements. Data owners also possess the ability to define distribution and associated policies.
* SERVICE LEVEL AGREEMENT (SLA)
  + Should cover at minimum:
    - Availability (e.g., 99.99% of services and data)
    - Performance (e.g., expected response times vs. maximum response times)
    - Security/privacy of the data (e.g., encrypting all stored and transmitted data)
    - Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators)
    - Disaster recovery expectations (e.g., worse-case recovery commitment, recovery time objectives [RTO], maximum period of tolerable disruption [MPTD])
    - Location of the data (e.g., ability to meet requirements/consistent with local legislation)
    - Data format/structure (e.g., data retrievable from provider in readable and intelligent format)
    - Portability of the data (e.g., ability to move data to a different provider or to multiple providers)
    - Identification and problem resolution (e.g., helpline, call center, or ticketing system)
    - Change-management process (e.g., changes such as updates or new services)
    - Dispute-mediation process (e.g., escalation process and consequences)
    - Exit strategy with expectations on the provider to ensure a smooth transition
  + SLA Components
    - Uptime Guarantees
    - SLA Penalties
    - SLA Penalty Exclusions
  + Security Recommendations
    - Immediate notification of any security or privacy breach as soon as the provider is aware is highly recommended.
    - Since the CSP is ultimately responsible for the organization’s data and alerting its customers, partners, or employees of any breach, it is particularly critical for companies to determine what mechanisms are in place to alert customers if any security breaches do occur and establishing SLAs determining the time frame the cloud provider has to alert you of any breach.
    - The time frames you have to respond within will vary by jurisdiction but may be as little as 48 hours. Be aware that if law enforcement becomes involved in a provider security incident, it may supersede any contractual requirement to notify you or to keep you informed.
  + Key SLA Elements to be assessed before agreeing to SLA
    - Assessment of risk environment (e.g., service, vendor, and ecosystem)
    - Risk profile (of the SLA and the company providing services)
    - Risk appetite (what level of risk is acceptable?)
    - Responsibilities (clear definition and understanding of who will do what)
    - Regulatory requirements (will these be met under the SLA?)
    - Risk mitigation (which mitigation techniques/controls can reduce risks?)
    - Different risk frameworks (what frameworks are to be used to assess the ongoing effectiveness, along with how the provider will manage risks?)
  + Ensuring Quality of Service (QoS)
    - Availability: This looks to measure the uptime (availability) of the relevant service(s) over a specified period as an overall percentage, that is, 99.99%.
    - Outage Duration: This looks to capture and measure the loss of service time for each instance of an outage; for example, 1/1/201X—09:20 start—10:50 restored—1 hour 30 minutes loss of service/outage.
    - Mean Time Between Failures: This looks to capture the indicative or expected time between consecutive or recurring service failures, that is, 1.25 hours/day of 365 days.
    - Capacity Metric: This looks to measure and report on capacity capabilities and the ability to meet requirements.
    - Performance Metrics: Utilizing and actively identifying areas, factors, and reasons for “bottlenecks” or degradation of performance. Typically, performance is measured and expressed as requests/connections per minute.
    - Reliability Percentage Metric: Listing the success rate for responses and based on agreed criteria, that is, 99% success rate in transactions completed to the database.
    - Storage Device Capacity Metric: Listing metrics and characteristics related to storage device capacity; typically provided in gigabytes.
    - Server Capacity Metric: These look to list the characteristics of server capacity, based and influenced by CPUs, CPU frequency in GHz, RAM, virtual storage, and other storage volumes.
    - Instance Startup Time Metric: Indicates or reports on the length of time required to initialize a new instance, calculated from the time of request (by user or resource), and typically measured in seconds and minutes.
    - Response Time Metric: Reports on the time required to perform the requested operation or tasks; typically measured based on the number of requests and response times in milliseconds.
    - Completion Time Metric: Provides the time required to complete the initiated/requested task, typically measured by the total number of requests as averaged in seconds.
    - Mean-Time to Switchover Metric: Provides the expected time to switch over from a service failure to a replicated failover instance. This is typically measured in minutes and captured from commencement to completion.
    - Mean-Time System Recovery Metric: Highlights the expected time for a complete recovery to a resilient system in the event of or following a service failure/outage. This is typically measured in minutes, hours, and days.
    - Scalability Component Metrics: Typically used to analyze customer use, behavior, and patterns that can allow for the auto-scaling and auto-shrinking of servers.
    - Storage Scalability Metric: Indicates the storage device capacity available in the event/where increased workloads and storage requirements are necessary.
    - Server Scalability Metric: Indicates the available server capacity that can be utilized/called upon where changes in increased workloads are required.

**Risk Mitigation**

* RISK-MANAGEMENT METRICS
* DIFFERENT RISK FRAMEWORKS
  + ISO 31000:2009
    - 11 key principles as a guiding set of rules to enable senior decision makers and organizations to manage risks
    - core component of ISO 31000:2009 is management endorsement, support, and commitment to ensure overall accountability and support.
    - focuses on risk identification, analysis, and evaluation through to risk treatment.
  + European Network and Information Security Agency (ENISA)
  + National Institute of Standards and Technology (NIST)—Cloud Computing Synopsis and Recommendations

**Understanding Outsourcing and Contract Design**

**Business Requirements**

**Vendor Management**

* RISK EXPOSURE
  + Is the provider an established technology provider?
  + Is this cloud service a core business of the provider?
  + Where is the provider located?
  + Is the company financially stable?
  + Is the company subject to any takeover bids or significant sales of business units?
  + Is the company outsourcing any aspect of the service to a third party?
  + Are there contingencies where key third-party dependencies are concerned?
  + Does the company conform/is it certified against relevant security and professional standards/frameworks?
  + How will the provider satisfy relevant regulatory, legal, and other compliance requirements?
  + How will the provider ensure the ongoing confidentiality, integrity, and availability of your information assets if placed in the cloud environment (where relevant)?
  + Are adequate business continuity/disaster recovery processes in place?
  + Are reports or statistics available from any recent events or incidents affecting cloud services availability?
  + Is interoperability a key component to facilitate ease of transition or movement between cloud providers?
  + Are there any unforeseeable regulatory-driven compliance requirements?
* ACCOUNTABILITY OF COMPLIANCE
* COMMON CRITERIA ASSURANCE FRAMEWORK
* CSA SECURITY, TRUST, AND ASSURANCE REGISTRY (STAR)
  + Level 1, Self-Assessment
  + Level 2, Attestation
  + Level 3, Ongoing Monitoring Certification

**Cloud Computing Certification: Cloud Certification Schemes List (CCSL) and Cloud Certification Schemes Metaframework (CCSM)**

* CCSL
  + Certified Cloud Service—TUV Rhineland
  + Cloud Security Alliance (CSA) Attestation—OCF level 2  (Open Certification Framework)
  + Cloud Security Alliance (CSA) Certification—OCF level 2
  + Cloud Security Alliance (CSA) Self Assessment—OCF level 1
  + EuroCloud Self Assessment
  + EuroCloud Start Audit Certification
  + ISO/IEC 27001 Certification
  + Payment Card Industry Data Security Standard (PCI-DSS) v3
  + LEET Security Rating Guide
  + AICPA Service Organization Control (SOC) 1
  + AICPA Service Organization Control (SOC) 2
  + AICPA Service Organization Control (SOC) 3
* CCSM security objectives
  + 1. Information security policy
  + 2. Risk management
  + 3. Security roles
  + 4. Security in Supplier relationships
  + 5. Background checks
  + 6. Security knowledge and training
  + 7. Personnel changes
  + 8. Physical and environmental security
  + 9. Security of supporting utilities
  + 10. Access control to network and information systems
  + 11. Integrity of network and information systems
  + 12. Operating procedures
  + 13. Change management
  + 14. Asset management
  + 15. Security incident detection and response
  + 16. Security incident reporting
  + 17. Business continuity
  + 18. Disaster recovery capabilities
  + 19. Monitoring and logging policies
  + 20. System tests
  + 21. Security assessments
  + 22. Checking compliance
  + 23. Cloud data security
  + 24. Cloud interface security
  + 25. Cloud software security
  + 26. Cloud interoperability and portability
  + 27. Cloud monitoring and log access

**Contract Management**

* IMPORTANCE OF IDENTIFYING CHALLENGES EARLY
  + Understanding the contractual requirements will form the organization’s baseline and checklist for the right to audit.
  + Understanding the gaps will allow the organization to challenge and request changes to the contract before signing acceptance.
  + The CSP will have an idea of what he/she is working with and the kind of leverage he/she will have during the audit.
* KEY CONTRACT COMPONENTS
  + Performance measurement—how will this be performed and who is responsible for the reporting?
  + Service Level Agreements (SLAs)
  + Availability and associated downtime
  + Expected performance and minimum levels of performance
  + Incident response
  + Resolution timeframes
  + Maximum and minimum period for tolerable disruption
  + Issue resolution
  + Communication of incidents
  + Investigations
  + Capturing of evidence
  + Forensic/eDiscovery processes
  + Civil/state investigations
  + Tort law/copyright
  + Control and compliance frameworks
  + ISO 27001/2
  + COBIT
  + PCI DSS
  + HIPAA
  + GLBA
  + PII
  + Data protection
  + Safe Harbor
  + U.S. Patriot Act
  + Business Continuity and disaster recovery
  + Priority of restoration
  + Minimum levels of security and availability
  + Communications during outages
  + Personnel checks
  + Background checks
  + Employee/third-party policies
  + Data retention and disposal
  + Retention periods
  + Data destruction
  + Secure deletion
  + Regulatory requirements
  + Data access requests
  + Data protection/freedom of information
  + Key metrics and performance related to quality of service (QoS)
  + Independent assessments/certification of compliance
  + Right to audit (including period or frequencies permitted)
  + Ability to delegate/authorize third parties to carry out audits on your behalf
  + Penalties for nonperformance
  + Delayed or degraded performance penalties
  + Payment of penalties (supplemented by service or financial payment)
  + Backup of media, and relevant assurances related to the format and structure of the data
  + Restrictions and prohibiting the use of your data by the CSP without prior consent, or for stated purposes
  + Authentication controls and levels of security
  + Two-factor authentication
  + Password and account management
  + Joiner, mover, leaver (JML) processes
  + Ability to meet and satisfy existing internal access control policies
  + Restrictions and associated non-disclosure agreements (NDAs) from the cloud service provider related to data and services utilized
  + Any other component and requirements deemed necessary and essential

**Supply Chain Management**

* SUPPLY CHAIN RISK
  + You should obtain regular updates of a clear and concise listing of all dependencies and reliance on third parties, coupled with the key suppliers.
  + Where single points of failure exist, these should be challenged and acted upon in order to reduce outages and disruptions to business processes.
  + Organizations need a way to quickly prioritize hundreds or thousands of contracts to determine which of them, and which of their suppliers’ suppliers, pose a potential risk.
* CLOUD SECURITY ALLIANCE (CSA) CLOUD CONTROLS MATRIX (CCM)
* THE ISO 28000:2007 SUPPLY CHAIN STANDARD
  + certification against ISO 28000:2007
    - Security management policy
    - Organizational objectives
    - Risk-management program(s)/practices
    - Documented practices and records
    - Supplier relationships
    - Roles, responsibilities, and relevant authorities
    - Use of Plan, Do, Check, Act (PDCA)
    - Organizational procedures and related processes