- ***Key Terms***
  - Type 1 Hypervisor
    - Installed directly on physical server
  - Type 2 Hypervisor
    - Installed on top of OS already running on a server
  - Conceptual model
    - Visualizations and descriptions that explain concepts and principles
  - Controls Models
    - Specific security controls and/or categories of controls; CCM, ISO 27017
  - Reference Architecture
    - Anything abstract and high level concepts to very detailed concept down to controls and functions
    - NIST 500-299, CSA Enterprise Architecture
  - Design Patterns
    - Reusable solution to a problem
    - Abstract or specific to a particular platform
  - Governance
    - Policies, processes, internal controls that direct how an organization runs
    - Relies on compliance function to ensure directives are fulfilled
  - Enterprise Risk Management
    - Manage overall risk to organization considering governance and risk tolerance
  - Information Risk Management
    - Risk to information and IT falls under this umbrella
  - Information Security
    - Tools and practices to manage risk to information
  - IT Governance
    - Processes to ensure effective and efficient use of IT in enabling organization to achieve its goals
  - Contract
    - Legally binding agreement between customer and cloud provider
  - Terms and Conditions
    - Main document that describes aspects of the service, how data is used, termination clause, warranties, and applicable laws
  - Acceptable Usage Policy
    - What you can and cannot do with service
  - Service Terms
    - Service-specific contractual agreements by provider

  COBIT
    - Control Objectives and Information for Related Technology
    - Governance and risk management framework by ISACA
    - Focuses on enterprise governance and management of all IT
  - Provider / Processor
    - Cloud Provider
    - Must operate in accordance with the laws in the jurisdiction in which they operate
  - Custodian / Controller
    - Entity that holds end-user data and is legally accountable for securely storing data

        - Must operate in accordance with the laws in the jurisdiction in which they operate
    - Omnibus privacy laws
        - Covers all categories of data
    - Sectoral privacy laws
        - Covers specific categories of personal data
    - Treaty
        - Agreement between two political authorities
    - European Economic Area (EEA)
        - Consists of EU countries and Iceland, Lichtenstein, Norway
    - Federal Rules of Civil Procedure (FRCP) Rule 26: Duty to Disclose
        - eDiscovery
    - Audit
        - Prove or disprove compliance
    - Compliance
        - Conformance to regulation, laws, policies, standards, best practices and contracts
    - Compliance Framework
        - Set of policies, procedures, processes, and technologies
    - Continuous Monitoring
        - Security controls and organizational risks are assessed and analyzed at frequency sufficient to support risk-based security decisions to adequately protect organizational information
    - Compliance Testing
        - Determine whether controls properly designed and implemented
    - Substantive Testing
        - Accuracy and integrity of transactions that go through systems
    - ISO/IEC 27001
        - Requirements for information security management system
        - Has appendix of controls
    - ISO/IEC 27002
        - Control catalog for ISMS
        - Lists controls and implementation guidance
    - ISO/IEC 27005
        - Information security risk management guidelines
    - ISO/IEC 27017
        - Set of security controls from ISO/IEC 27002 modified for cloud
    - ISO/IEC 27018
        - Implementation guidance for controls applicable to protecting personal information
    - Data Classification
        - Process of grouping data into categories through evaluation and labeling for purpose of identifying appropriate security controls
    - Data Security Lifecycle
        - Focuses on security aspects and locations through stages
    - Business Continuity
        - Continue business operations while disaster recovery steps are undertake people and operations
    - Disaster Recovery

        - Recovery and resiliency function that focuses on recovery from an incident; IT focused
    - Software Defined Networking (RFC 7426)
        - Architectural concept that moves network control plan from networking device to a controller
    - Network Functions Virtualization (NFV)
        - Replace physical networking appliance with virtualized networking function
    - Microsegmentation
        - Uses network virtualization to implement fine-grained approach to creating separate zones
    - Data Dispersion
        - Multiple copies of data spread across multiple storage locations to improve resiliency
    - Container
        - Constrained to run segmented processes while still utilizing kernal and capabilities of base operating systems
    - Container Engine
        - Environment on top of where container runs (container runtime)
        - EXAMPLE: Docker
    - Orchestration and Scheduling Controller
        - Provisioning and deployment of containers, scaling, movement of containers, container health monitoring
        - EXAMPLE: Kubernetes, Docker Swarm
    - Image repository
        - Location where images and code that can be deployed as containers
    - Event
        - Change of state that has significance of an IT service or CI
    - Incident
        - Unplanned event; operational or security
    - Rugged DevOps
        - Integration of security testing throughout entire application development process to produce secure and resilient applications
    - Entity
        - Someone or something that has an identity
    - Identity
        - Unique expression of an entity within an environment
    - Identifier
        - Cryptographic token that identifies an identity in a digital environment (Windows SID)
    - Persona
        - Identity and attributes in a specific situation
    - eXtensible Access Control Markup Language (XACML)
        - Standard for defining attribute-based access controls and authorizations
        - Policy decision point (PDP) and policy enforcement point (PEP)
        - Controls what entity is allowed to do
    - Vulnerability
        - Any circumstance or even with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, or DoS

- Risk
  - Change that threat exploits a vulnerability
- Runtime Lock-In
  - Situation where code must be customized based on providers unique environment
- Know-how
  - How a customer does what they do; similar to trade secret

- ***Key Facts***
  - Responsibility can be outsourced by accountability cannot
  - Contract between a customer and provider will identify responsibilities and mechanisms for governance
  - Cloud must be continually assessed due to dynamic nature
  - China and Russia prohibit data from being exported
  - CSA draws from NIST 800-61r2 for incident response
  - SLAs around communication of security incidents, rules, and responsibilities
  - CSA recommends host-based vulnerability assessments using host-based agents
  - Governance -> Risk Management -> Compliance

  - Cloud Characteristics Standards
    - ISO/IEC 17788
    - NIST 800-145

  - Cloud Security Reference Architecture
    - ISO/IEC 17789
    - NIST 500-292

  - Key Roles
    - Governance
    - Enterprise Risk Management
    - Information Risk Management
    - Information Security

- ***Key Concepts***
  - CSA Cloud Logical Model
    - Infrastructure layer - infrastructure security (traditional services, networking, etc)
    - Metastructure layer - virtual environment security (management plane)
    - Infostructure layer - data security (file, storage, databases)
    - Applistructure layer - app and OS security

  - Cloud Characteristics
    - Resource pooling
    - Broad network access
    - Rapid elasticity
    - Measured service; utility computing
    - (ISO/IEC 17788) multitenancy

  - Cloud Service Models

- IaaS
- PaaS
- SaaS

- Cloud Deployment Model
  - Public Cloud
  - Private Cloud - all tenants trusted
  - Community Cloud - financial risk shared across multiple contractually trusted organizations
  - Hybrid Cloud - portability, cloud bursting

- Shared Responsibility Model
  - IaaS
    - Customer - Data governance, client access endpoints, IAM, application security, network security, operating system security
    - Provider - Physical security
  - PaaS
    - Customer - Data governance, client access endpoints, IAM
    - Shared - Application security, network security
    - Provider - operating system security, physical security
  - SaaS
    - Customer - Data governance, client access endpoints, IAM
    - Provider - application security, network security, operating system security, physical security

- CSA Cloud Controls Matrix (CCM)
  - Control Domain and Control
  - Control ID
  - Updated control specification -> control objective
  - Architectural relevance -> areas impacted by control
  - Corporate Governance Relevance -> governance or technical
  - Cloud Service Delivery Model applicabiity
  - Supplier relationship -> customer, provider, both
  - Scope applicability -> standards mapping

- Consensus Assessments Initiative Questionnaire (CAIQ)
  - Uses CCM specifications and asks specific yes or no questions

- STAR Registry
  - Filled out CAIQs
  - Level 1 - Self assessments
  - Level 2 - 3rd party certificates (SOC2 / ISO 27001)
  - Level 3 - Continuous auditing - still in development

- Cloud Security Process Model
  - Identify requirements
  - Select cloud service provider, service model, and deployment model
  - Define architecture

        - Assess security controls; shared responsibility
        - Identify control gaps
        - Design and implement controls to fill gaps
        - Manage changes over time

    - Corporate Governance
        - Board of directors and committees
        - Values and ethics
        - Policies and regulatory frameworks
        - Risk management
        - Accountability
        - Monitoring and internal controls

    - IT Governance Components
        - IT Strategic Alignment
        - IT resource management
        - Risk management
        - Performance measurement
        - IT value delivery

    - System and Organizational Control Report (SOC)
        - AICPA report
        - SOC1 - Financial statements
        - SOC2 - controls related to security, availability, integrity, configuration, and privacy
        - SOC3 - statement from independent CPA that SOC was performed and high level statement as to effectiveness

    - SOC 2 Types
        - Type 1 -> point in time look at design of a control
        - Type 2 -> Inspection of effectiveness of control

    - Supplier Assessment
        - Request and review docs
        - Review cloud provider's security program and documentation
        - Review legal, regulatory, contractual, and jurisdictional requirements for customer and provider
        - Evaluate contracted service in context of customer information asset
        - Evaluate overall provider such as finances, reputation, and outsources

    - Applicable Law Considerations
        - Location of cloud provider
        - Location of data custodian/controller
        - Location of end users/subjects
        - Location of hardware servers
        - Jurisdiction of contract
        - Treaties and legal frameworks between locations

- International Safe Harbor Privacy Principles (Safe Harbor Agreement)
    - Treaty between US and EU which allowed companies to commit voluntarily to protecting EU citizen's data stored in the US in same way it would be protected in EU
    - Replaced by EU-US Privacy Shield

- EU-US Privacy Shield
    - Operates in same way as Safe Harbor
    - Companies self-certify that appropriate privacy measures are in place
    - Data transfer mechanisms are same as GDPR

- CLOUD Act (Clarifying Lawful Overseas Use of Data Act)
    - US law which allows US government to issue subpoenas or warrants to access client data stored by American provider regardless of where it is stored

- Australia Privacy Act / Australian Consumer Law (ACL)
    - Includes 13 Austrialian Privacy Principles (APPs)
    - Applies to all private sector/non-profit w/ revenue >$3m AUD, private health, small businesses
    - Applies to CSP even if based outside a and other laws are in contract
    - Requires notification of security breach if disclosure will cause serious harm or if disclosure likely to happen and will cause harm

- Personal Information Protection and Electronics Documents Act (PIPEDA)
    - Canadian Law
    - Requires notification of breach if entity that lost data believes it will cause serious harm

- China Cyber Security Law
    - Requires operators to implement series of security requirements
    - Inform users of security defects and bugs and report to authorities
    - Data localization for citizen data
    - Ministry of Public Safety (MSP) can perform penetration testing (local or remote) check for prohibited content, copy user information, and share with other state agencies

- Act on the Protection of Personal Information (APPI)
    - Japanese Law
    - Requires private sector to protect personal information and data securely
    - Limits ability to transfer citizen personal data without consent of data subject unless country of destination has established framework meeting its standards

- Russian Data Protection Law
    - Citizen data must be localized

- EU/EEA Director 2002/58/EC on Privacy and Electronic Communications
    - AKA ePrivacy Directive (ePD)
    - Erase or anonymize traffic data when no longer needed

        - Prohibits use of email for marketing unless agreed upon
        - User must consent to cookies
        - ePrivacy regulation is planned to superseded this

    - General Data Protection Regulation (GDPR)
        - "Privacy by design" and "privacy by default"
        - Binding to all member states and EEA
        - Replaced Directive 95/46/EC
        - Applies to any legal entity engaged in economic activity that processes data associated with EU citizens
        - Adjudicated by member states with closet relationship with the individuals or entities on both sides of dispute
        - Process data only if subject has given specific consent or if authorized by statutory provisions
        - Data subjects have right to use data, correct data, and be forgotten
        - Data cannot be transferred out of EU/EEA unless similar protection
        - If no comparable country regulation then company can use SCC, EU-US Privacy Shield, BCR, some cases specific data subject consent
        - Notify of breaches within 72 hours and who is notified depends on risk
        - Member states can implement requirements above and beyond
        - Sanctions are 4% of global company income or up to $20m EUR

    - Network Information Security Directive (NIS Directive)
        - EU/EEA Directive
        - Addresses security requirements to compliment GDPR privacy law
        - Applies to operators of essential services and digital service providers
        - Companies operating outside of EU/EEA but sell to EU/EEA are subject and must assign an EU representative
        - Adjudicated by member states with closet relationship with the individuals or entities on both sides of dispute
        - Each member state must create CSIRT which works together across EU/EEA
        - Digital service providers must notify CSIRT of security incidents
        - Members have requirements around security programs and notification of incidents

    - GDPR Applicability
        - Processing of personal data for controller/processor in EU/EEA regardless of where processing takes place
        - Processing of EU/EEA if processing related to offerings goods or services or monitoring of behavior of data subject when behavior takes place within EU/EEA
    - FTC
        - Has ability to issue fines and consent orders
        - "unfair and deceptive practice"
        - Consumer privacy rights at federal level
    - South America
        - Argentina, Chile, Columbia, Mexico, Peru, Uruguay
        - Laws are similar to EU Directive 95/46/EC and reference APEC Privacy Framework

        - Security requirements remain in place for data controller wherever data are stored
    - Compliance Considerations
        - Jurisdiction
        - Shared responsibility model
        - Compliance inheritance
        - Supply chain complexity
        - Artifacts of compliance from provider
        - Scope relevance
        - Compliance management
        - Audit performance
        - Provider experience
    - Governance Risk and Compliance (GRC)
        - Plan -> determine regulations in scope and what controls need to be addressed
        - Do -> Implement required controls
        - Check -> Perform audits to ensure controls meet requirement
        - Act -> fix deficiencies and provide feedback
    - Cloud Contract Concerns
        - SLAs
        - Data ownership
        - Right to audit
        - Third-party audits
        - Conformance of security policies
        - Compliance of laws and regulations
        - Incident notification
        - Liabilities
        - Termination terms
        - Service levels
        - Quality levels

    - Audit Management
        - Ensure audit directives are implemented properly
        - Determine appropriate requirements, scope, scheduling, and responsibilities
        - Uses compliance requirements and risk data to scope, plan, and prioritize audit engagements

    - Audit Planning Considerations
        - Purpose
        - Scope
        - Risk analysis
        - Audit procedures
        - Resources
        - Schedule

    - AICPA Trust Services Criteria
        - Security
        - Availability
        - Confidentiality

- Processing integrity
- Privacy

- AICPA Common Criteria
  - Seven categories and control objectives within each category that must be checked
  - Organization and management
  - Communications
  - Risk management, design, implementation of controls
  - Monitoring of controls
  - Logical and physical access controls
  - Systems operations
  - Change management

- Complementary User Entity Controls (CUEC)
  - Included in SOC report and supplied to customers by provider to advise customers of controls they are accountable for

- Data and Information Governance Domains
  - Ownership and custodianship
  - Information classification
  - Information management policies
  - Location and jurisdiction
  - Authorizations
  - Contractual controls
  - Security controls

- Data Classification Approaches
  - User-based
  - Content-based
  - Context-based

- Information Management
  - How organization plans, identifies, creates, receives, governs, secures, uses, exchanges, maintains, dispose of information
  - Makes information available to right person, in right format, at right time

- Information Management Lifecycle
  - Create
  - Store
  - Use
  - Share
  - Archive
  - Destroy

- Information Management Functions
  - Accessing Data -> Create, Store, Use, Share, Archive, Destroy
  - Process Data -> Create, Use

- Store Data -> Store, Archive

- REST
  - Representational State Transfer
  - Not a standard but an architectural style
  - Stateless and depends on other standards
  - GET, POST, PUT, DELETE, PATCH

- SOAP
  - Simple Object Access Protocol
  - Standard and protocol
  - Security included within typically seen for internal API
- IaaS Networks
  - Management network -> management plane to pools
  - Storage Network -> storage volumes to instances
  - Service Network -> Internet to instance and instance to instance

- VLAN (802.1Q)
  - Provides network segmentation not isolation
  - Supports 4096 addresses due to 12-bits for addressing

- VXLAN (RFC 7348)
  - Virtual extensible LAN
  - Encapsulates layer 2 frames within UDP packets using a VXLAN Tunnel End Point (VTEP) creating tunneling scenarios
  - Inside UDP packets VXLAN Network Identifier (VNI) used for addressing
  - 24-bit for addressing supporting ~16m addresses
  - Enables a virtual network to span multiple physical networks across a WAN

- Network Planes
  - Management planes
  - Control plane -> controls how traffic is processed in data planes (brains)
  - Data Plane

- SDN Security Benefits
  - Isolation
  - SDN firewall
  - Deny by default
  - Identification tags
  - Resistance to low level networking attacks

- Software Defined Perimeter (SDP)
  - CSA model
  - Uses user and device authenticated to provision network access to resources dynamic

- CSAs Compute Distribution
  - VMs

        - Containers
        - Platform-based workloads
        - Serverless

    - Incident Response Lifecycle
        - Preparation
        - Detection and analysis
        - Containment, eradication, and recovery
        - Post-incident activity

    - CSA Preparation
        - Process to handle incidents
        - Handler communications and facilities
        - Incident analysis hardware and software
        - Internal documentation
        - Training identification
        - Evaluation of infrastructure by proactive scanning, network monitoring, vulnerability assessments, risk assessments
        - Subscription to third-party threat intelligence services

    - CSA Detection and Analysis
        - Form system of alerts, including endpoint protection, network security monitoring, host monitoring, account creation, privilege escalation, SIEM, security analytics
        - Validate alerts
        - Estimate scope of incident
        - Assign incident manager
        - Designate communicator
        - Build timelines
        - Determine extent of data loss
        - Notification and coordination activities

    - CSA Containment, Education, Recovery
        - Take machines offline and ensure data is not destroyed
        - Cleanups and restore normal operations
        - Validate steady state and deploy controls to prevent similar incidents
        - Document incidents and gather evidence

    - CSA Forensic Guidance
        - Snapshot the storage of a VM
        - Capture metadata at time of alert
        - Try to preserve memory from IaaS
        - Network flow logs, firewall configs
        - Data access Logs

    - CSA SSDLC Categories
        - Secure design and development -> training, developing organizational standards, requirements, threat modeling, write and test code

- Secure development -> security and testing activities performed when moving application code from dev to prod
- Secure operations -> ongoing security of applications, vulnerability assessments, penetration tests

- CSA SSDLC
  - Training
  - Define-> code standards, security functional requirements
  - Design -> threat modeling, secure design
  - Develop
  - Test

- Penetration Testing In The Cloud
  - Use firms that know the platform
  - Address developers and administrators
  - Try to break tenant isolation

- Deployment Pipeline
  - Source code, infrastructure templates, server configuration
  - Version control repository
  - Continuous integration server (functional tests, nonfunctional tests, security tests)
  - Test
  - Production

- CSA Application Security
  - Separate dev and prod
  - Monitor for changes and deviations from baselines
  - Testing and assessments must be ongoing
  - Monitor cloud management plane and infrastructure as well

- Tokenization
  - Tokenization and data masking can keep original length and format
  - Used when format of data is important
  - Stores both original data and randomized data in secure database for retrieval

- Proxy Encryption
  - Hybrid storage gateway
  - Proxy handles all cryptography operations and encryption keys held within appliance or external key management service

- CSA Key Management Options
  - HSM/appliance
  - Virtual appliance/software
  - Cloud provider services
  - Hybrid

- SecaaS Benefits

        - Cloud-computing benefits
        - Staffing and experience
        - Intelligence sharing
        - Deployment flexibility
        - Insulation of clients
        - Scaling and cost

    - SecaaS Issues
        - Lack of visibilities
        - Regulation differences
        - Handling of regulated data
        - Data leakage
        - Changing of providers
        - Migration of SecaaS

    - Security Assessment Systems
        - Traditional security and vulnerability assessments of cloud-based instances
        - SAST, DAST, RASP
        - Cloud platform assessments

    - Big Data
        - High velocity
        - High volume
        - High variety

    - Big Data Components
        - Distributed data collection
        - Distributed storage (HDFS)
        - Distributed processing (Mapreduce, Spark)

    - IoT CSA Recommendations
        - Secure data collection and sanitization
        - Device register; authN/authZ
        - API security for connections back to cloud infrastructure
        - Encrypted communications
        - Patch and update devices

    - Mobile CSA recommendations
        - Device register; authN/authZ
        - Application APIs that run in cloud services

    - Serverless CSA Challenges
        - Security of provider
        - Application logging
        - Provider compliance
        - Access to management plane
        - Reduce attack service by breaking up components
        - Vulnerability assessments must comply with vendor requirements

        - Challenges to incident response

- ***<u>ENISA Cloud Computing Security Assessment (Matt's Notes)</u>***
    - Security Benefits
        - Security and benefits of scale
        - Security as market differentiator
        - Standardized interfaces for managed security services
        - Rapid, smart, scaling of resources
        - Audit and evidence gathering
        - More timely, effective, efficient updates
        - Benefits of resource concentration

    - Top Risks
        - Loss of governance
        - Lock-in
        - Isolation failure
        - Compliance risks
        - Management interface compromise
        - Data protection (how cloud provider protects data)
        - Insecure or incomplete data deletion
        - Malicious insider

    - Policy and Organizational Risks
        - (H) Lock-In
        - (H) Loss of governance
        - (H) Compliance challenges
        - (M) Loss of business reputation due to co-tenant activities
        - (M) Cloud service termination or failure
        - (M) Cloud provider's acquisition
        - (M) Supply chain failure

    - Technical Risks
        - (M) Resource exhaustion
        - (H) Isolation failure
        - (H) Cloud provider malicious insider
        - (M) Management interface compromise
        - (M) Intercepting data in tenant
        - (M) Data leakage on upload/download, intra-cloud
        - (M) Insecure or ineffective deletion of data
        - (M) DDoS
        - (M) Economic DDoS
        - (M) Loss of encryption key
        - (M) Undertaking malicious probes or scans
        - (M) Compromise of service engine (cloud orchestration platform)
        - (M) Conflicts between customer hardening procedures and cloud environment

    - Legal Risks
        - (H) Subpoena and ediscovery

        - (H) risk from changes of jurisdiction
        - (H) Data protection risk
        - (M) licensing risk

    - Non-cloud Specific Risks
        - (M) Network breaks
        - (M) Network management
        - (M) modifying network traffic
        - (M) Privilege escalation
        - (M) social engineering attack
        - (M) loss or compromise of operational logs
        - (M) loss or compromise of security logs
        - (M) backups lost/stolen
        - (M) unauthorized access to premises
        - (M) theft of computer equipment
        - (M) natural disasters

- ***Extra Content (Not on exam)***
    - SAN Layers
        - Host Layer -> servers receive calls from LAN and enable access to SAN fabric
        - Fabric Layer -> networking components that make up for SAN
        - Storage Layer -> storage devices
    - SAN Facts
        - Protocols used include FCoE, iSCSI, InfiniBand
        - Host bus adapters (HBA) and converged network adapters (CNA) used to connect to SAN
        - Converged network allows SAN to use standard ethernet cables by encapsulating SCSI commands in Ethernet frame using FCoE or ISCI
    - Logical Unit Number (LUN)
        - Used to present logical disk drive to host server and abstract pool of storage
    - Zoning
        - Allows you to restrict a set of hosts to being able to access a set of ports or nodes in a storage array
        - Hard zoning -> restricts at the hardware level
        - Soft zoning -> prevents ports from being seen using software
    - LUN Masking
        - Fine-grained control on top of zoning to control what LUNs within a zone a host sees