- ## Chapter 1 – Architectural Concepts

  - CSA Trusted Cloud Initiative (TCI) Reference Model
    - Intent is to provide a reference architecture cloud providers can use to give cloud customers confidence in their solutions
    - Draws requirements from SOX, GLBC, ISO 27002, PCI-DSS, COBIT
    - Uses SABSA, ITIL, TOGAF, and Jericho frameworks to structure guidance

  - CSA Trusted Cloud Initiative (TCI) Reference Model Components
    - Business Operation Support Services (BOSS) -> SABSA
    - IT Operations and Support -> ITIL
    - Presentation, Application, Information, Infrastructure Services -> TOGAF
    - Security and Risk Management -> Jericho

  - Sherwood Business Security Architecture (SABSA)
    - Framework for enterprise security architecture and service management
    - Everything derived from analysis of business requirements for security
    - Layers -> contextual, conceptual, logical, physical, component, management
    - What, why, how, who, when where

  - The Open Group Architecture Framework (TOGAF)
    - Framework for enterprise architecture that helps with designing, planning, implementing, and governing
    - Four levels -> business, application, data, technology
    - High-level approach to design

  - NIST 800-53 – Recommended Security Controls for Federal Information Systems and Organizations
    - Guidance document w/ primary goal of ensuring appropriate security requirements and controls are applied to US Federal government information management systems

  - Managed Services Provider
    - IT Service where customer dictates tech and operational procedures and external party executes administration and operations support contract

  - FIPS 140-2
    - NIST standards document that lists accredited and outmoded cryptosystems

  - Eucalyptus
    - Open source cloud computing and IaaS platform for enabling private clouds

  - Cloud Service Broker (CSB)

    - Intermediary between cloud service customers and CSPs to help select best provider for each customers

- Cloud Computing Reseller
    - Company purchases hosting services from cloud server hosting or compute provider and resells its own customers

- Cloud Access Security Broker
    - 3rd party offering IAM to CSPs and cloud customers that comes with single sign-on, certificate management, and cryptographic key escrow

- Cloud Bursting
    - Augment internal private datacenter capabilities with managed services during time of increased demand

- Business Requirement
    - Operational driver for decision making and input for risk management

- Nonfunctional Requirements
    - Aspects of device or process that are not necessary for accomplishing business task but are desired or expected
    - EXAMPLE: salesperson's connection to corporate network is secure

- Functional Requirements
    - Performance aspects of the device or process that are necessary for business task to be accomplished
    - EXAMPLE: salesperson must be able to connect to corporate network remotely

- Cloud Characteristics
    - Elasticity
    - Simplicity
    - Scalability

- Cloud Computing Characteristics
    - Broad network access
    - On-demand services
    - Resource pooling
    - Measured/metered service

- **Chapter 2 – Design Requirements**

    - Homomorphic encryption
        - Process data in cloud while it is encrypted w/o having to encrypt

- Cloud Provider Security Devices
  - All guest accounts are removed
  - All unused ports are closed
  - No default passwords remain
  - Strong password policies
  - Admin accounts secured and logged
  - Unnecessary services are disabled
  - Physical access severly limited and controlled
  - Systems patched, maintained, updated according to vendor guidance

- How to deal with risks
  - Avoid
  - Accept
  - Mitigate
  - Transfer

- Risk
  - Potential for loss, damage, destruction of an asset as result of a threat exploiting a vulnerability
  - Intersection of asset, threat, and vulnerability

- Threat
  - Anything that can exploit a vulnerability intentionally or accidentally and obtain or destroy an asset
  - The thing we protect against

- Vulnerability
  - Weakness or gaps in security program that can be exploited by threats to gain unauthorized access to an asset
  - Weakness or gap in protection efforts

- Dealing with Single Point of Failure (SPOF)
  - Add redundancy
  - Create alternative paths
  - Crosstrain personnel
  - Backups and restore
  - Load sharing

- Business Impact Analysis (BIA)
  - Determine value of asset
  - Cost to org if asset lost
  - Cost to replace or repair
  - Method to deal with loss

    - Used to identify SPOF

- Business requirements Analysis
    - Inventory all assets
    - Valuation of all assets
    - Determination of critical paths, processes, and assets
    - Understanding of risk appetite

Chapter 3 – Data Classification

- Data Lifecycle
    - Create
    - Store
    - Use
    - Share
    - Archive
    - Destroy

- Data classification
    - Characteristics of data such as sensitivity, jurisdiction, or criticality
    - Classify by a trait

- Data categorization
    - Define how data is used
    - Categorize by its use

- Data Metadata
    - Listing of traits or characteristics about specific data elements or sets
    - Created as same time as data

- Data Owner (Data Controller)
    - Org that collected or created the data

- Data Custodian (Data Processor)
    - Manipulates, stored, moves data on behalf of data owner

- Data Labeling
    - Data owner
    - Date of creation
    - Data of scheduled destruction
    - Confidentiality level
    - Handling directions
    - Dissemination / distribution instructions

  - Access limitations
  - Source
  - Jurisdiction
  - Applicable regulation

- Data Discovery Methods
  - Label-based discovery
  - Metadata-based discovery
  - Content-based discovery
  - Data Analytics

- Datamining
  - Organization collects various data streams and can run queries across various feeds and organization can detect and analyze previously unknown trends and patterns
  - Real-time analytics
  - Agile business Intelligence

- DRM Traits
  - Persistent protection
  - Dynamic policy control
  - Automation expiration
  - Continuous auditing
  - Replication restrictions
  - Remote rights revocation

- Data Retention Policy Requirements – Archive Stage of Data Lifecycle
  - Retention period
  - Applicable regulation
  - Retention formats
  - Data classification
  - Archiving and retrieval procedures
  - Monitoring, maintenance, enforcement

- Data Audit Policy requirements – All Phases of Data Lifecycle
  - Audit periods
  - Audit scopes
  - Audit responsibilities
  - Audit processes and procedures
  - Applicable regulations
  - Monitoring, maintenance, enforcement

- Cryptoshredding (cryptographic erasure)

    - Encrypt data with strong encryption engine and then taking keys generated in process and encrypting with a different engine and then destroy keys
    - Effective destruction technique in cloud

- Data Disposal Policy requirements – Destroy phase of Data lifecycle
    - Process for data disposal
    - Applicable regulations
    - Clear direction of when data should be destroyed

- **Chapter 4 – Cloud Data Security**

    - Protect data created remotely – Create Stage
        - Encrypt before uploading to cloud
        - Cryptosystem should be on FIPS 140-2 list
        - Connection should be secure

    - Protect data when in use – Use stage
        - Connections should be secure
        - Secure user platform/device
        - Least privilege
        - Strong access control
        - Logging and audit

    - Protect data during archive stage
        - Cryptography and key management
        - Jurisdiction / location
        - Format
        - Staff (people)
        - Procedure (backup/recovery)

    - Key Management Tenants
        - Level of protection -> encryption keys secured at same level or higher
        - Key recovery
        - Key distribution
        - Key recovery
        - Key escrow
        - Don’t store key with data

    - Randomization
        - Replace data or part of data with random characters

    - Shuffling
        - Use different entries from within same data set to represent data

    - Drawback uses production data

- Static obscuring
    - New dataset is created as a coy and only obscured copy is used

- Dynamic obscuring
    - Data obscured as called

- SIEM Goals
    - Centralize collection of log data
    - Enhanced analysis capabilities
    - Dashboarding
    - Automated response

- Data Loss Protection (DLP)
    - Additional security
    - Policy enforcement
    - Enhanced monitoring
    - Regulatory compliance

- **Chapter 5 – Security in the Cloud**

    - Responsibilities in IaaS
        - Security Governance, Risk, and Compliance -> Enterprise
        - Data Security -> Enterprise
        - Application security -> Enterprise
        - Platform security -> Enterprise
        - Infrastructure security -> Shared
        - Physical security -> Cloud

    - Responsibilities in PaaS
        - Security Governance, Risk, and Compliance -> Enterprise
        - Data Security -> Enterprise
        - Application security -> Enterprise
        - Platform security -> Shared
        - Infrastructure security -> Cloud
        - Physical security -> Cloud

    - Responsibilities in SaaS
        - Security Governance, Risk, and Compliance -> Enterprise
        - Data Security -> Enterprise
        - Application security -> Shared
        - Platform security -> Cloud

    - Infrastructure security -> Cloud
    - Physical security -> Cloud

- Private Cloud Risks
    - Personnel threats
    - Natural disasters
    - External attackers
    - Regulatory compliance
    - Malware

- Community Cloud Risks
    - Risks of each node in the community being an entry point into the larger community
    - Shared access and control
    - No centralized administration for performance and monitoring

- Multitenant Environment Risks
    - Conflict of interest
    - Escalation of privilege
    - Information bleed
    - Legal activity

- Vendor Lock-In Mitigations
    - Ensure favorable contract terms for portability
    - Avoid proprietary formats
    - Ensure no physical limitations (bandwidth)
    - Regulatory constraints (needs to be more than on CSP)

- Vendor Lock-Out Mitigations
    - Provider longevity
    - Core competency
    - Jurisdictional suitability
    - Supply chain dependencies
    - Legislative environment

- Brewer Nash
    - Users given permission to access datasets based on which datasets user had previously seen but also considers free will to choose initial silo
    - Reduces risk of cloud administration conflict of interest by having access to multiple cloud customers that are competitors

- IaaS Threats
    - Personnel threats
    - External threats

    - Lack of specific skillsets

- PaaS Threats
    - Interoperability issues
    - Persistent backdoors
    - Virtualization threats
    - Resource sharing

- SaaS Threats
    - Proprietary formats
    - Virtualization threats
    - Web app security

- Virtualization Threats
    - Hypervisor threat
    - Guest escape
    - Information bleed
    - Data seizure

- Guest Escape vs Host Escape
    - Attacker leaves confines of virtualized instance
    - Attacker leaves confines of virtualized instance and host

- Private Cloud Threats
    - Malware
    - Internal threats
    - External attackers
    - Man-in-the-middle
    - Social engineering
    - Theft/loss of device
    - Regulatory violations
    - Natural disasters

- Community Cloud Threats
    - All private cloud threats
    - Loss of policy control
    - Loss of physical control
    - Lack of audit access

- Public Cloud Threats
    - All private cloud threats
    - All community cloud threats
    - Rogue admins
    - Escalation of privilege

    - Contractual failure

- Hybrid Cloud Threats
    - All private cloud threats
    - All community cloud threats
    - All public cloud threats
    - Loss of uniformity and centralized control

- Malware Countermeasures
    - Host/network-based anti-malware on host and vm
    - User training
    - Continual monitoring
    - Updates/patches

- Internal Threat Mitigations
    - Good hiring practices
    - Job rotation, mandatory vaca
    - Separation of duty/least privilege
    - Data masking
    - Egress monitoring
    - Behavioral analysis

- External Threat Mitigations
    - Hardened machines
    - Access control
    - Know your data
    - Threat intelligence

- Man-in-the-middle Mitigations
    - Encrypt data in transit
    - Secure session technology and enforcement

- Theft/loss of device mitigation
    - Encryption of stored material
    - Strict physical controls
    - Inventory and monitoring
    - Remote wipe and kill

- Contractual Failure Mitigations
    - Full offsite backups

- Regulatory Violation Mitigations
    - Trained straff, strong legal
    - DRM

    - Encryption, obfuscation, masking

- Rogue Admin Mitigations
    - Additional administration controls for privileged access
    - Locked racks, video surveillance, financial monitoring

- Loss of privilege control mitigations
    - Strong contract
    - Audits

- Escalation of Privilege Mitigations
    - Access control and authentication
    - Review of log data

- Cloud-specific BIA Concerns
    - New dependencies
    - Regulatory failure
    - Data breach/disclosure
    - Vendor lockin/lockout

- Options for Cloud Backup
    - Private architecture using cloud services as backup
    - Cloud Operations with cloud provider as backup
    - Cloud Operations with 3rd party cloud backup provider

- **Chapter 6 – Responsibilities in the cloud**

    - Cloud Provider Responsibilities - Physical
        - Secure hardware components
        - Manage hardware config
        - Set hardware to log events and incidents
        - Determine compute component composition by customer need
        - Secure administrative access

    - Cloud Provider Responsibilities - Logical
        - Installation of virtual OS
        - Secure config of virtualized elements

    - Cloud Provider Responsibilities – Networking
        - Firewalls
        - IDS/IPS
        - Honeypots
        - Vulnerability assessments

- Hardening OS
  - Remove unnecessary services and libraries
  - Close unused ports
  - Antimalware
  - Limit administrators
  - Remove default access
  - Event/incident logging

- System and Organizational Control (SOC) Report
  - Created by AICPA
  - Ensure compliance with SOX
  - Three SOC report levels

- SOC1
  - Auditing financial reporting instruments

- SOC2
  - Type 1 – Reviews design of controls
  - Type 2 – Reviews implementation of controls

- SOC 3
  - Seal of approval by an auditing company

- **Chapter 7 – Cloud Application Security**

  - Cloud Secure SDLC
    - Defining
    - Designing – user stories, identifying programming language
    - Development
    - Testing

  - ISO/IEC 270341
    - Standard for secure app development

  - ISO/IEC 270341 – Organizational normative framework (ONF)
    - Business context
    - Regulatory context
    - Technical context
    - Specifications
    - Roles, responsibilities, qualifications
    - Processes
    - Application security control library (ASC)

- ISO/IEC 270341 – Application Normative Framework (ANF)
  - ONF used to create ANF for a single application used to achieve app required level of trust

- Policy management
  - Helps achieve access management
  - Enforcement arm of authN/authZ and is established based on business needs and senior management decisions

- Web of trust
  - Form of FIM where each member has to review and approve member for inclusion of federation

- Third party identifier
  - Form of FIM where member organizations outsource responsibility to approve/review each other

- Database Activity Monitoring (DAM)
  - Watches database for unusual behavior and alert or stop it

- Deception Technology
  - Works with WAF/DAM to quietly re-route attack traffic to honeypot

- API Gateway
  - Proxy
  - Access control
  - Limit connections (DDoS)
  - Logging
  - Metrics
  - Additional security filtering

- XML Gateway
  - Similar to API gateway but works around how sensitive data/services are exposed to API

- REST
  - Lightweight
  - Simple URLs
  - Not reliant on XML
  - Scalable
  - Outputs to JSON/CSV
  - Efficient w /small message
  - Good for limited bandwidth

  - Stateless operations
  - Caching

- SOAP
  - Standard-based
  - Reliant on XML
  - Highly intolerant of errors
  - Slower
  - Built-in error handling
  - Asynchronous processing
  - Stateful operations
  - Formatted

- Application Specific Integrated Circuits (ASIC)
  - Perform cryptographic operations to offload burden from primary CPU

- Application Virtualization
  - Run apps in trusted virtual environment where full apps run in protected space
  - XenAPp, App-V, WINE

- STRIDE
  - Threat model where standardized way to describe threats by their attributes and examine app for vulnerabilities of three threat types
  - Spoofing, tampering, repudiation, Ddos, elevation of privilege

- Injection
  - Malicious user injects string of some type of data into field in order to manipulate app actions or access unauthorized data
  - SQL, LDAP, OS

- Cross Site Scripting (XSS)
  - App includes untrusted data in a new page w/o proper validation or escaping or updates to existing web page w user supplied data using browser API that can create HTML/Javascript
  - Allows attacker to execute scripts in victims browser to hijack sessions, deface websites, or redirect user to malicious sites

- Insecure Direct Object Reference
  - App provides direct access to objects based on user input bypassing AuthZ

- Invalidated Redirect and Forwards
  - Devs use redirect wo validating allowing malicious users to alter redirects and send user to malicious site

- Notorious 9
  - Data loss
  - Data breach
  - Account takeover
  - Insecure API
  - DoS
  - Insider threats
  - Abuse of cloud services
  - Insufficient due diligence
  - Shared tech issues

- QoS
  - Idea of ensuring you do not over-control environment with security measures that degrade application performance

- Vulnerability Scanning
  - Scan application for known vulnerabilities
  - Passive and based on definitions

- Penetration Testing
  - Find vulnerabilities and exploit
  - Active

- White-box testing
  - Reviews source code
  - Test while inactive

- Black-box testing
  - Test application as it functions

- Static Application Security Testing (SAST)
  - Source code, binaries, byte code tested w/o executing application
  - Useful to identify XSS, SQL injections, buffer overflows, unhandled exceptions, and backdoors

- Dynamic Application Security Testing (DAST)
  - Test while application is running
  - Effective for HTTP / HTML applications

- Software Supply Chain API Management
  - Risks of an API using other underlining APIs which may or may not be secure and consumer not being aware of it

- Runtime Application Self-Protection (RASP)

    - Application reacts to attacks by automatically reconfiguring itself w/o human interaction

- OWASP Top 9 Coding Flaws
    - Input validation
    - Source code design
    - Information leakage and improper error handling
    - Direct object reference
    - Resource usage
    - API usage
    - Best practice violations
    - Weak session management
    - Use of HTTP GET Query Strings

- **Chapter 8 – Operations Elements**

    - Uptime vs availability
        - Datacenter may be up and running but customers ISP connectivity is not working causing issues with availability
    - Uptime Institute Standards
        - Four tiers of ascending levels of durability
        - 12 hours of fuel stored is requirement for all four tiers
    - UI Tier 1
        - Basic site infrastructure
        - Little to no redundancy
        - Good for cold site or hot/warm for backup data
        - Least expensive
        - Downtime "will happen"
    - UI Tier 2
        - Redundant Site Infrastructure Capacity Components
        - Good option for small organizations
        - Downtime "may happen"
    - UI Tier 3
        - Concurrently Maintainable Site Infrastructure
        - Dual power supplies
        - Unplanned loss of component may cause downtime while system loss will
        - Planned maintenance may cause downtime but risk of downtime is increased at this time
    - UI Tier 4
        - Fault Tolerant Site Infrastructure
        - Every element of system and facility has redundancy
        - "Will not"
    - Loosely Coupled vs Tightly Coupled Architecture

    - Tightly shares same physical hardware backplane which increases performance but limits agility
    - Loosely coupled is connected logically allowing for scale and agility
- Bit splitting
    - AKA data dispersion
    - Data sliced into chunks and encrypted w/ parity bits and then dispersed across cloud cluster
- Awareness
    - Informal, voluntary presentation of material for purpose of reminding
    - Example: Posters
- Training
    - Formal presentation of materials by internal SME
    - Specific to organization
- Education
    - Formal presentation of material in academic environment
    - Credit for degree
- Threat Modeling
    - View application from perspective of attacker
- Training Types
    - Initial - new employees
    - Recurring - continual updating of security
    - Refresher - you f-d up and now you need training

• Chapter 9 – Operations Management

- Temperature, Humidity, Dew Point
    - Temperature 64 - 81 degrees F
    - Humidity 60%
    - Dew Point 42-59 degrees F

- Maintenance Mode Requirements
    - All operational instances are removed from system or device
    - Prevent new logins
    - Ensure logging is continued and increased

- Updated Process
    - Document how, when, why
    - Move through CM process
        - Maintenance mode
        - Apply update and update asset inventory
        - Verify update
        - Validate modification
        - Return to normal

- Update vs Upgrade
  - Updates are applied to existing systems and components where upgrades are replacement of old components

- Change Management
  - Modification of network such as deployment of new tech or disposal of old

- Configuration Management
  - Modification to known set of parameters such as settings

- Baselining
  - Change -> depiction of network and systems based on inventory
  - Config -> standard build of OS and settings

- CM Policy
  - Composition of CM board
  - Process in detail
  - Documentation requirement
  - Instructions for exceptions
  - Assignment of CM tasks, validating, scanning, analysis
  - Procedure for addressing deviations
  - Enforcement measures and responsibilities

- CM Initial Process
  - Full asset inventory
  - Codification of baseline
  - Secure baseline build
  - Deployment of asset

- CM Normal Operation
  - CMB meeting
  - CMB testing
  - Deployment
  - Documentation

- Business Continuity
  - Concerned with maintaining critical operations during any interruption of service

- Disaster Recovery
  - Focused on resumption of operations after interruption due to disaster

- Event
  - Unscheduled adverse impact to operating environment

    - 3 days or less

- Disaster
    - Event that lasts greater than 3 days

- Continuity Main Focuses
    - Connectivity
    - Utilities
    - Processing capacity

- BC/DR Plan
    - List of items from asset inventory deemed critical
    - Circumstances under which disaster declared
    - Who is authorized to make declaration
    - Points of contact
    - Detailed actions and tasks

- BC/DR Kit
    - Replicate to at least one other location
    - Current copy of plan
    - Communication equipment
    - Architecture diagrams
    - Software
    - Emergency contact info
    - Documentation tools and equipment
    - Emergency essentials
    - Fresh batteries to last 24 hours

- Maximum Allowable Downtime (MAD)
    - How long before interruption in service kills organization

- RTO
    - How long to recover operations after interruption in service
    - Must be less than MAD

- RPO
    - Maximum allowable lost data in a time measurement

- UPS
    - Must last long enough for graceful shutdown of affected systems

- **Chapter 10 – Legal and Compliance Part 1**

    - Bodies of Law

    - Criminal
    - Civil
    - Administrative
    - Uniform Code of Military Justice

- Criminal Law
    - All legal matters where govt is in conflict w/ person, group, or org that violated statutes
    - Includes federal and state courts where punishment can include monetary fines, imprisonment, or death
    - Govt prosecutes and conducts law enforcement activities

- Statute
    - Rules that define conduct prohibited by government and are designed to provide for safety and well being of public

- State Law vs Federal Law
    - In state law jurisdiction stops at state line vs federal law includes entire country
    - State law is superseded by federal law but the most strict law applies unless there is strict jurisdiction

- Civil Law
    - Set of rules that govern private citizens and disputes
    - Strictly private entities such as individuals, groups, and organizations
    - Body of law that deals with community-based laws
    - Punitive measures are restitution of monetary damages or requirement to perform actions

- Contract
    - Agreement between two parties to engage in some specific activity, usually for mutual benefit
    - Applies to SLA, OLA, PLA, and PCI-DSS contracts
    - Disputes general handled in civil court and involve reparative restitution in event of loss

- Contract Components
    - Finite duration
    - List of parties
    - Means for dispute resolution
    - Jurisdiction law under which contract will be subject

- (OLA) Operating Level Agreement

    - Used internally for service provide to detail responsibilities, process, and time frames in support of SLA
    - Must be more strict timeframe than SLA

- (UC) Underpinning Contract
    - Contract between service provider and third-party vendor/provider

- Tort Law
    - Body of rights, obligations, and remedies that have been set for reliefs for persons who have been harmed as result of wrongful acts by others
    - Shift cost away from victims to person that hurt the victim
    - Deterrent to careless and risky behavior

- Common Law
    - Existing set of rulings and decisions by court informed by cultural norms and legislation
    - Create precedents

- Administrative Law
    - Created by executive decision and function
    - EXAMPLE: IRS administers federal tax law

- Intellectual Property
    - Intangible assets that are property of the mind (ideas)

- Copyrights
    - Used to protect expression of an idea like an artistic work or software
    - Person who first expresses the idea immediately becomes the copyright owner and can additionally register the copyright with the United States Copyright Office
    - Lasts for 75-125 years after the death of the copyright owner

- Trademarks
    - Intellectual property used to identify a brand
    - Issued by state government or USPTO
    - Last as long as property still being used

- Patents
    - Used to protect a formula, process, pattern, invention, etc
    - Last for 20 years
    - Granted by USPTO

- Trade Secret

    - Intellectual property that is private business material like a client list, recipe, process
    - Is perpetual as long as owner uses and attempts to keep a secret

- How are intellectual property rights enforced?
    - Owner must enforce the rights
    - Criminal law can come into play if it is theft

- Doctrine of the Proper Law
    - Process associated with determining what legal jurisdiction will hear a dispute
    - Typically which jurisdiction is closest to the damages

- Restatement (Second) Conflict of Law
    - Developments in common law which help courts stay up to date with changes
    - Restatements used to determine which laws should be enforced
    - Laws that fit best or most restrictive influence the decision

- Stored Communication Act (SCA)
    - Part of ECPA
    - Restrict government from forcing ISP to disclose customer data ISP may have

- Graham-Leach Baily Act (GLBA)
    - Allowed banks and financial institutions to merge
    - Customer account info must be kept secure and private and customers can opt out of information sharing between entities
    - Requires information security plan and ISO
    - Administered by FDIC/FFIEC and enforced by FDIC/DFI

- SOX
    - Increased transparency into publicly traded corporations financial activities
    - Includes provisions for securing and maintaining confidentially, integrity, and availability
    - External auditors added to protect against abuse by publicly traded orgs

- Family Educational Rights and Privacy Act (FERPA)
    - Prevents academic institutions from sharing data with anyone but parents or the student
    - Administered by DoE and enforced by the DoE

- Digital Millennium Copyright Act (DMCA)
    - Updated copyright provisions to protect owned data in Internet world
    - Crack of access controls is a crime
    - Allows copyright owner to take down websites that include their content

- Health Insurance Portability and Accountability Act (HIPAA)
  - Administered by DHHS and enforced by Office of Civil Rights (OCR)
  - Privacy Rule and Security Rule (Driven by HITECH)
  - Primary purpose was to make it easier for people to keep health insurance policies, protect confidentiality and security of healthcare info, and help healthcare industry control administrative costs
  - ePHI can be stored in the cloud but must have adequate security and private protections in place
- PII
  - Information that can be used to identify an individual
  - In EU this includes name and cell phone number, IP address, cookies, DNA
  - GLBA defines PII as customer account number and balances

- Organization for Economic Cooperation and Development (OECD)
  - Standards org made up of reps from multiple countries
  - Released set of principals Data Directive is based of
  - Non-legally binding

- EU Data Protection 95/46 EC (Superseded by GDPR)
  - Privacy law for EU
  - Notice, choice, purpose, access, integrity, security, enforcement
  - Handling of all personal/private info of EU citizens
  - "right to be forgotten" allows user to request data be deleted

- Safe Harbor (Superseded by Privacy Shield)
  - w/I Data Directive and outlines what American companies must do in order to comply with EU laws
  - Program administered by DoC or DoT
  - US company must voluntarily agree to comply with Data Directive
  - US company must sign up with federal enforcement entity that would administer program

- General Data Protection Regulation (GDPR)
  - Enacted in May of 2018 and supersedes Data Protection Directive
  - Child consent rose from 13 to 16
  - Expands identifiable info to IP address, cookies, DNA
  - Processing criminal data requires official authority
  - Data subjects have right to not be subject to automated decision making and profiling
  - Data subjects have right in relation to processing of personnel data
  - Member states can scope balance of right to private w/ freedom of expression and information

- Privacy Shield

  - Agreement between EU and US and Swiss and US to transfer data from EU/Swiss to US
  - Companies voluntarily agree to principles and are then audited by DoC/DOT and enforced by FTC/DOT as law
  - Requirements
    - Notice
    - Choice
    - Accountability of onward transit
    - Security
    - Data integrity and purpose limitation
    - Access
    - Recourse enforcement liability
    - Supplemental principals

- Binding corporate rules/ standard contractual clauses
  - Alternative for US companies instead of Privacy Shield
  - Company explicitly states full compliance with GDPR
  - All EU countries must approve of company policy

- Australian Privacy Act of 1988
  - Regulates handling of citizen personal information
  - Transparency, rules of collection, correctness and integrity
  - Aligns with EU

- Canadian Personal information Protection and Electronic Documents Act (PIPEDA)
  - Protection of personal information
  - Aligns with EU

- Argentina Personal Data Protection Act
  - Ensures compliance with GDPR
  - Aligns with EU

- European Free Trade Association (EFTA)
  - Four nation body including Switzerland, Norway, Liechtenstein, and Iceland
  - Regulations are recognized to be stringent enough to protect EU data

- Asia-Pacific Economic Corporation (APEC) Privacy Framework
  - Goal to work toward economic growth and cooperation with its members
  - Agreements are not legally binding; voluntary compliance
  - Enhance free markets through common adherence to PII protection principals

- ISO 27017:2015
  - Guidelines for information security controls applicable to provision and use cloud services

    - Standards for providing services and how cloud customer information and privacy should be controlled

- Regulation
    - Rules created by either other department of government or external entities empowered by the government
    - Contractual regulations such as PCI-DSS

- ISO/IEC 27037:2012
    - Guide for collecting, identifying, and preserving electronic evidence

- ISO/IEC 27041:2015
    - Guide for incident investigations

- ISO/IEC 27042:2015
    - Guide for digital evidence analysis

- ISO/IEC 27043:2015
    - Incident investigation principles and processes

- ISO/IEC 27050:2016
    - Overview of principals of eDiscovery

- NIST SP 800-122
    - Insight into definition of PII as information about person such as name, DOB, SS#

- Gap analysis
    - Audits begin here and creates an accurate frame of reference

- ISMS
    - Model for development and implementation of policies, procedures, and standards
    - Top down approach to addressing and managing risk
- Right to Audit
    - Used to mean consumer organization could demand to audit provider organization but now has evolved to mean getting copies of audit reports for due diligence
- SAS 70
    - AICPA audit standard that was replaced by SSAE 16 which outlines SOC 1, SOC 2, and SOC 3 audit reports

- **Chapter 11 – Legal and Compliance Part 2**
    - Risk tolerance

    - Acceptable variation in outcome related to specific performance measures linked to objectives entity seeks to achieve
    - Level of risk an org can accept per risk
- Risk appetite
    - Total risk an org can accept given a risk profile
- Key Risk Indicators (KRIs)
    - Indicators that something is wrong and a risk may be surfacing
    - EXAMPLE: new vulnerability surfaces that could impact cloud provider
- Risk profile
    - Comprehensive analysis of risks an organization is exposed to
- ISO 31000:2009
    - International standard focusing on designing, implementing, and reviewing risk management processes and practices
- European Union Agency for Network and Information Security (ENISA) -> Cloud Computing: Benefits, Risks, Recommendations for Information Security
    - 35 risks a cloud customer should consider
    - Loss governance
    - Lock in
    - Isolation failure
    - Compliance risk
    - Management interface failure
    - Data protections
    - Malicious insider
    - Insecure or incomplete data deletion
- Service Level Agreement (SLA)
    - List of defined, specific, numerical metrics used to determine whether provider is meeting contract terms during a period
    - Pay attention to quality of the service and the interruptions per period
- SLA Elements
    - Performance
    - Security and privacy considerations
    - Logging and reporting
    - DR metrics (RPO, RTO, MAD)
    - Location of data
    - Data format and structure
    - Data portability
    - Problem identification and resolution procedures
    - Change management process
    - Dispute mediation process
    - Exit expectations
- ISO 15408-1:2009
    - Provides assurance to customers that cloud security products have been tested by third parties
- Cloud Certification Schemes List (CCSL)

    - Shows main characteristics of certificate scheme such as underlining standards, who issues the certification, is the CSP audited, and who conducts the audit (internal or external)
- Cloud Certification Scheme Metaframework (CCSM)
    - High-level mapping of security requirements of customer to security objectives in existing schemes
- CSA Security, Trust, and Assurance Registry (STAR)
    - Framework for evaluating cloud providers
    - Consists of Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ)
    - Three levels -> Self assessment, CSA Star Attestation, CSA START Continuous Monitoring
- ISO 28000:2007
    - Certification against certain elements of supply chain risk
    - Security management policy
    - Organizational objectives
    - Risk management practices
    - Documented practices and records
    - Supplier relationships
    - Roles, responsibilities, and authorities
    - Organizational procedures and processes