Legal Risk and Compliance

Constitution

- Supreme in any country
- Amendments are not straight forward; requires a lengthy and difficult process to amend a constitutional right
- Right to privacy is not in US constitution, but there are legislations in different states that talk about privacy
- 4th Amendment of US constitution talks about Privacy

Legislation

- Most of the privacy and security laws are from the standard legislative process in US
- Bills are passed by both houses and then signed into Law
- These laws are enforceable only if it does not conflict with the constitution
- Laws passed by US Congress is effective and enforceable in all states
- States can also pass legislations that are effective and enforceable in respective states alone

Code Law

- **Rule-based law** not precedence based
- Focused on codified law – or written law
- Lower courts are not compelled to follow the decisions made by the higher courts
- Most widespread legal system in the world and most common in Europe

Common (case) Law

- It is based on previous interpretations of law
- It reflects the community's morals and expectations
- Uses judges and juries of peers
- Case law decisions are binding on the courts making the decision and any subordinate courts
- Constitutional law and legislative law override aspects of the common law
- Broken down into civil, criminal, and administrative

Administrative Law

- Policies, procedures and regulations that govern the daily operations of the agency
- Administrative law does not require an act of legislation but must comply with all existing civil and criminal laws

Civil / Tort Law

- It is based on common law
- Defendant owes a legal duty to the victim
- Designed to provide for an orderly society and govern matters that are not crimes
- Incumbent on the person wronged to file a lawsuit
- Damages can be financial penalties
- **Strict liability**: A person is responsible for the consequences of his actions, even if they could not reasonably anticipate the adverse outcome.

Criminal Law

- It is based on common law
- Addresses behavior harmful to society
- Punishment involves a loss of freedom, monetary fines, community service
- Responsibility is on the prosecution to prove guilt
- Govt, through law enforcement agencies, brings about charges against the individual/organization that is accused of violation
- Penalties include, jail term, community service, monetary fines

Contract Law

- Legally binding agreement between parties
- When two parties have agreed to enter into a contract, they are legally liable to hold their obligation
- As long as the terms of contract does not violate the constitution, it is enforceable in court
- Contracts should spell out the specific liability that each party has for violations of the contract
- Contract violation disputes are handled in the Civil Court

Theory of Liability for negligence

- There must be a duty of due care:
    - The person accused of negligence must have an established responsibility to the accuser
- There must be a breach of that Due-care
- There must be damages involved
- There must be causation: The injury caused to the plaintiff must be a result of the breach of duty by the accused.

Theory of Invasion of Privacy

- There are 4 legal torts that may result in successful claim of Invasion of Privacy
  - Invasion of Solitude
  - Public disclosure of private facts
  - False light
  - Appropriation

Analysing a law

- First thing to analyze is to determine the jurisdiction of the law
  - It is the geographic area to which the law applies
  - Courts also have jurisdictional boundaries to render legal judgements
  - Federal courts have jurisdiction only over federal law, whereas state courts have jurisdiction only over state law.

Analysing a law

- Scope and applicability of the law to your own organization needs to be determined
- **FERPA** – regulates education institutions handling student records.
- **HIPAA** – regulates handling of medical records by health care institues and its business associates.

US privacy and Security Laws

Health Insurance Portability and Accountability Act (HIPAA)

- Provides a framework and guideline to ensure security, integrity and privacy when handling confidential medical records
- It outlines how security should be managed for any facility that creates, accesses, shares or destroys medical information
- Mandates steep penalties for noncompliance

HIPAA Scope

- HIPAA applies to Covered entities and to certain healthcare transactions
- Covered Entities:
  - Health Insurance Plans
  - Healthcare clearing houses
  - Healthcare Providers
- It also extends to any third-party individual or organization that works with the covered entity to fulfill health-care related functions and has access to PHI
- Covered entities should have written contracts (Business associate agreement) with any third-party that fulfill health-care related functions and has access to PHI

HIPAA Privacy Rule

•Privacy rule lays guidelines for protecting the privacy of PHI

•All Covered entities and business associates are subject to the privacy rule

•Covered entities are required to retain any records related to their privacy policies and related activities for six (6) years

- Requires the implementation of Information Privacy practices
- Limits use and disclosure of data without patient notification
- Gives patients additional rights to their medical information

HIPAA Security Rule

•Established to provide an information security framework for implementation of HIPAA

• The rule applies to both the covered entities and the business associates

• Both the security rule and privacy rule are enforced by the Office of Civil Rights (OCR)

• Requires that covered entities implement data controls, complete regular risk analysis

HITECH Act

- Provides incentives for healthcare organizations to use electronic health records
- HITECH also applies to covered entities and Business associates
- **Breach notification rule**: requires entities to notify victims about data breaches

HITECH Act – Breach Determination

- The type of information involved and whether individual patient can be identified
- The parties who used or accessed the information
- The likelihood PHI was actually acquired or viewed by an unauthorized party
- How well the PHI is secured

HITECH Act – Breach Notification

- Covered entities need to notify the individuals within 60 days of knowing about a data breach
- If more than 500 individuals are affected, then the CE must notify media outlets and also notify HHS
- Business associates must notify the covered entities within 60 days of notice

Gramm-Leach-Bliley Act (GLBA)

- Mandates financial institution develop privacy notices and give customers option to prohibit sharing their information with non-affiliated parties
- Applicability is based on two factors
    - The formality of offering financial services
    - The frequency of offering financial services
- BoD is responsible, all employee should be trained and security controls should be tested
- Major components
    - **Financial privacy rule**: provide each customer with privacy notice. Provide opt-out clause
    - **Safeguards rule**: develop written information security plan
    - **Pretexting Protection**: Implement safeguards against social engineering

GLBA – Privacy Rule

- Customer: entity that has an ongoing regular relationship with the financial institution
- Consumer: entity that may conduct only isolated transactions with the financial institution
- Intended to protect Privacy
- Must share the privacy notice when the customer starts the relationship and continue to provide updated information annually
    - The notice must describe the privacy policy and how the customer information will be collected, used and shared
    - The notice also should inform the third-parties to whom their information may be shared *(only inform not request consent)*
    - For customers, provide the full privacy notices as mandated in GLBA
    - For consumers, provide a summary of Privacy notice

GLBA - Safeguards Rule

- Provides framework for protecting information security
- Requires implementation of Information security programs
- Requires financial institutions to anticipate threats
- Emphasizes protecting against threats the consumer may be harmed
- Required declaring an Information security officer
- Emphasizes three categories of information security controls:
  - Workforce training
  - Securing of Information Systems
  - Ongoing monitoring of Information systems

FedRAMP

- US Federal program that mandates a standardized approach to security assessments, authorization and continuous monitoring of cloud products / Services.
-

Breach Notification

- Breach: a breach is occurred when an organization has determined that unauthorized third-party has accessed the information (can include PII/PHI)
- Conditions for Notification:
    - Who to notify
    - When to notify
    - How to notify

GDPR

- Promulgated in European Union
- Aims to protect data for everyone in the EU
- Personal Data:
    - Any information that can help identify an individual
    - Name, IP address, geolocation, etc.
- GDPR prohibits the transfer of data to non-EU countries unless the recipient offers the same level of privacy protections as the EU

GDPR – Data Subject Rights

- Right to erasure / Right to be forgotten
- Right of access
- Right to rectification
- Right to restriction of processing
- Right to data portability
- Notification obligations
- Right to Object
- Automated individual decision-making, including profiling

GDPR – Binding Corporate Rules

- Each party agrees to abide by GDRP standards
- The agreement must be legally binding in all concerned jurisdictions
- An EU organization, that acts a processor or controller, must assume liability
- BCRs require approval by an EU member state supervisory authority

GDPR – Standard Contractual clauses

- A contract that obligates the non-EU entity to be fully compliant to GDPR practices
- The EU company that is planning to transfer the data is referred to as **Data Exporter**
- The non-EU company that is receiving the data is referred to as **Data Importer**
- The SCCs must be used exactly as provided by the EU Commission and must not be altered

GDPR – Other transfer Mechanisms

- **Derogations**
    - Describes the specific and limited exemption when limited data needs to be transferred for a one-off case
- It can be done only on the following circumstances:
    - Consent from the data subject
    - To fulfill contractual obligation
    - For “Important reasons of public interest”
    - To safeguard the vital interests of the data subject
    - If the information is already open to public

GAPP

- 10 Generally Accepted Privacy Principles (GAPP)
  - Management
  - Notice
  - Choice and consent
  - Collection
  - Use, Retention and disposal
  - Access
  - Disclosure to Third-parties
  - Security for Privacy
  - Quality
  - Monitoring / Enforcement

GAPP - Management

- Criteria
    - Creating Privacy policies and communicating those policies
    - Assigning responsibility and accountability
    - Establishing privacy procedures
    - Ensuring policies are consistent with laws / regulations / contractual obligations
    - Assessing privacy risk when implementing any change
    - Creating and maintaining privacy incident management process
    - Conducting Privacy awareness training

GAPP - Notice

- Criteria
  - Include notice practices in the privacy policies
  - Notifying individuals on the purpose of collection and organization policies
  - Writing privacy notices in plain simple language and posting them conspicuously

GAPP – Choice and Consent

- Criteria
  - Allowing individuals to retain control over the use of their information
  - Include choice and consent practices in the privacy policy
  - Informing individuals about choice and consent options
  - Obtaining implicit and explicit consent at or before collection of data
  - Obtaining explicit consent when collecting sensitive personal information

GAPP – Collection

- Criteria
  - Include collection practices in the privacy policy
  - Informing individuals their data will be used only for identified purposes
  - Mentioning the methods of collection and the types of data collected
  - Collecting using fair and lawful means and only for intended purposes
  - Confirming that any third-party involved have collected it fairly and lawfully and the information is reliable

GAPP – Use, Retention and Disposal

- Criteria
  - Include collection practices in the privacy policy
  - Informing individuals their data will be used only for identified purposes
  - Informing individuals that their data will be retained for specific time period
  - Informing individuals that their data will be disposed off safely after its use

GAPP – Access

- Criteria
    - Include individual access practices in the privacy policy
    - Informing individuals about the procedures for reviewing, updating and correcting their personal information
    - Providing mechanism for the individuals to check if their information is held by the organization
    - Authenticating an individual's identity before providing the access
    - Providing access to information in an understandable format
    - Informing individuals clearly on why any request was denied
    - Providing a mechanism for individuals to update or correct their records

GAPP – Disclosure to Third-Parties

- Criteria
  - Include Third-party disclosure practices in the privacy policy
  - Informing individuals of any third-party disclosure risks and its purpose
  - Informing third-parties to comply with the organization' privacy policies

GAPP – Security for Privacy

- Criteria
  - Informing individuals that the organization takes percautions to protect the privacy of their personnel information
  - Including security practices in the privacy policies
  - Developing, documenting and implementing an information security program

GAPP – Quality

- Criteria
  - Informing individuals that they bear responsibilities in providing the organization with accurate and complete personal information
  - Including data quality practices in the privacy policies
  - Maintaining personal information that is accurate, complete and relevant for the purpose

GAPP – Monitoring and Enforcemnet

- Criteria
  - Including monitoring and enforcement practices in the privacy policies
  - Informing individuals how they should contact the organization for any issues with regards to their data
  - Maintaining dispute resolution process
  - Reviewing compliance with privacy laws
  - Developing and implementing remediation plans

Cloud Forensics

Forensics Requirements

- ISO standards for digital forensics:
  - ISO 27037:2012 – Guide for collecting, identifying and preserving electronic evidence
  - ISO 27041:2015 – Guide for incident investigations
  - ISO 27042:2105 – Guide for digital evidence analysis
  - ISO 27043:2015 – Incident investigations principles and processes
  - ISO 27050-1:2016 – Overview and principles of eDiscovery

Cloud Forensic Challenges

- Collection and Acquisition
  - There are multiple owners of the resources
  - Ownership rights of system/ resources may not always be with the customer
  - Third-party data may be affected by forensic collection
  - Participation / Support from Cloud provider is very important

eDiscovery Considerations

- eDiscovery should be considered a security requirement when evaluating a cloud service provider
- Data residency and system architecture are important considerations for eDiscovery in cloud
- ISO 27050 – Practices and procedures needed to collect data, perform analysis and present findings
- CSA – has done cross-mapping of relevant ISO standards for cloud computing
- NISTIR 8006 - focuses on common issues and solutions needed to address DFIR in clud

Cloud Vendor Management

Impact of Geo Locations

- Challenges in cloud
    - Data processing, storage, and computing each occur in different geographies
    - Difficulties in assessing data actors
    - Difficulties in locating data

Security Policy Framework

Security Policy

- Strategic plan for implementing security
- Defines the scope of security needed for the organization
- Defines the main security objectives and outlines the security framework
- Identifies major functional areas of data processing
- Broadly outlines the security goals and practices that should be employed
- Its is used to assign responsibilities, define roles, specify audit requirements, outline enforcement process, indicate compliance requirements, and define acceptable risk levels

It's a compulsory document

Standards / Baselines / Guidelines

Standard

- Define compulsory requirements
- Provides a course of action for uniform deployment of technology
- Tactical documents

Baseline

- Defines minimum level of security that every system must meet
- System-specific
- Establishes common secure state

Guideline

- Offers recommendations on implementation
- Servers as an operating guide
- Flexible – can be customized for each unique system

Procedure

- Final element of the formalized security policy structure
- Detailed step-by-step document describes actions necessary to implement security mandates
- System and software specific
- Purpose is to ensure integrity of business process

Risk Management

Risk Management

- Process of identifying and assessing risk, reducing it to an acceptable level
- Two primary elements of Risk Management
  - Risk Assessment
  - Risk Response

Risk Management Process

4 Interrelated components that comprise the risk management process

- **Frame Risk:**
  - Defines the context within which all risk activities takes place
- **Assess Risk:**
  - Most critical aspect of the process; assessing the risks to determine mitigation strategies
- **Respond to Risk:**
  - Determining the risk response options available
- **Monitor Risk:**
  - Continuously monitor the effectiveness of controls against the risks as well as look for new risks.

Risk Assessment (Analysis)

- **Risk Assessment** – Method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement the security controls
- It ensures security is cost-effective, relevant, timely and responsive to the threats
- Helps prioritize risks and shows management the number of resources needed to protect in a sensible manner

Risk Analysis

4 main goals of risk analysis

- Identify Assets and their values to the organization
- Identify vulnerabilities and threats
- Quantify the probability and business impact of these potential threats
- Provide cost benefit analysis of the safeguard

- Risk Analysis must be supported and directed by senior management
- Management must define the purpose and scope of analysis, appoint a team to carry out assessment and allocate necessary resources

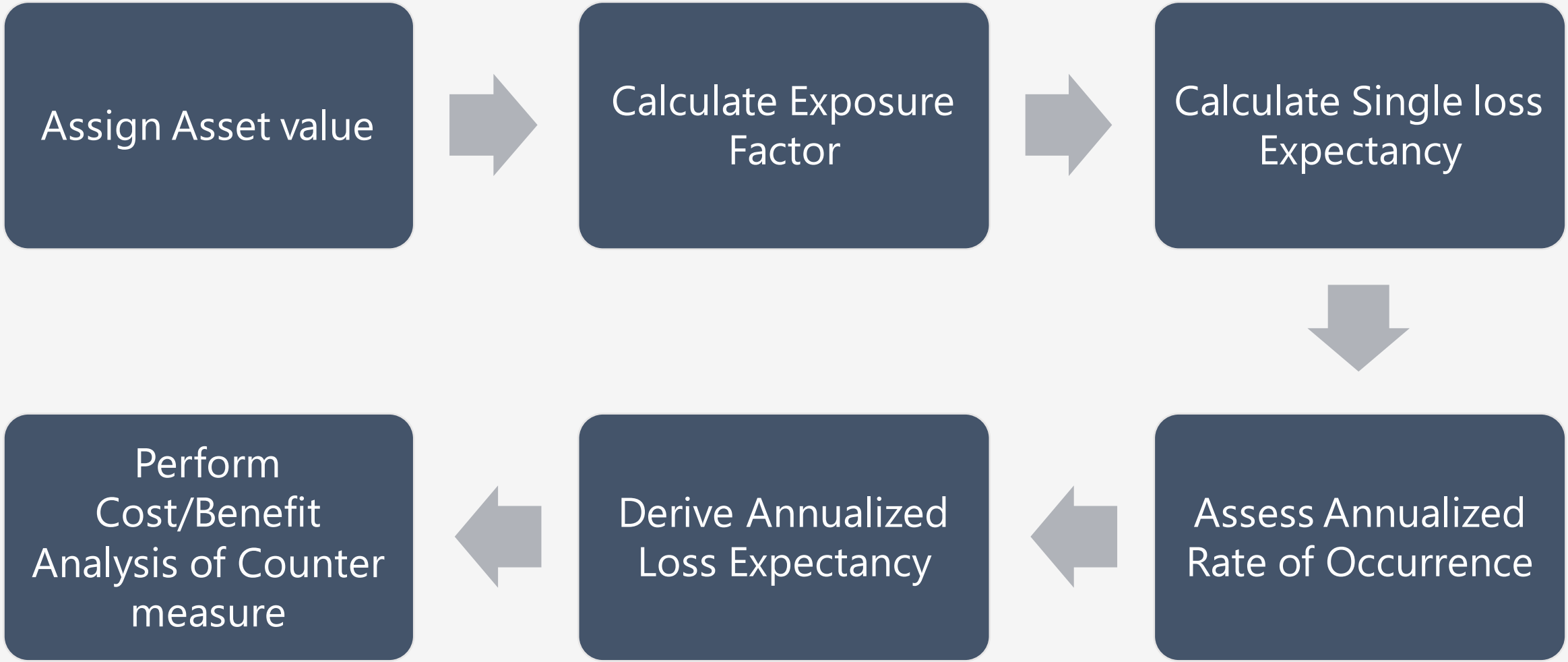
Risk Analysis Approaches

- **Two Primary Risk Assessment Methods**
  - Quantitative Risk Assessment
  - Qualitative Risk Assessment

Quantitative Risk Assessment

- Assigns monetary and numeric values to all elements of the Risk analysis process
- More scientific or mathematical approach to Risk Assessment
- Uses risk Calculations to attempt to predict the level of monetary loss, and the probability for each type of threat
- The reports are fairly user friendly
- However, not all elements can be quantified

Quantitative Risk Assessment - Steps



Key Terms in Quantitative Risk assessment

Exposure Factor (EF)	• % loss the organization would suffer if a single realized risk materializes • Also referred to as loss potential
Single Loss Expectancy (SLE)	• Cost associated with a single realized risk against a specific asset • SLE = AV * EF • It is represented in ₹ value
Annualized Rate of Occurrence (ARO)	• Frequency with which a specific threat will occur within a single year • Range from 0 (threat will not occur) to very large numbers • It is also known as probability determination
Annualized Loss Expectancy (ALE)	• Possible yearly cost of all instances of a specific threat realized against a specific asset • ALE = SLE * ARO
Annual Cost of Safeguard (ACS)	• It's the cost associated in procuring, developing, maintaining a control against a potential threat • The ACS should not exceed the ALE

Asset Valuation

- It starts with Inventorying all the assets in the Organization; Goal is to assign value to the assets

- Aspects to consider when assigning value to the assets
  - Cost to acquire or develop
  - Cost to maintain and protect
  - Value to owner and users
  - Value to adversaries
  - Market valuation
  - Price others are willing to pay
  - Cost to replace the asset if lost
  - Operational and production activities affect if the asset is not available
  - Liability issues if the asset is compromised
  - Usefulness and role of the asset in the organization

Asset Valuation – Benefit

- Helps in performing effective cost/benefit analysis
- Helps select specific countermeasures and safeguards
- Determine the level of insurance coverage to purchase
- Understand what exactly is at risk
- Comply with legal and regulatory requirements

Asset Valuation – Two key points

- **Loss Potential**
    - What the company will loose if a threat agent takes advantage of a vulnerability
    - Eg: data corruption, destruction, information disclosure
- **Delayed Loss**
    - Its is secondary in nature and takes place well after a vulnerability is exploited
    - May include damage to reputation, loss of market, accrued penalties etc.

Cost Benefit Analysis

- **ALE before Safeguard – ALE after Safeguard – Cost of Safeguard = Value of the safeguard to the company**
- If the above result is negative the safeguard is not financially reasonable to be implemented
- It is also important to consider the issues of legal responsibility and prudent due care

Qualitative Risk Analysis

- Uses a softer approach to Risk analysis
- It does not quantify the data, does not use calculations
- It is more opinion and scenario based and uses rating system
- Techniques include judgement, best practices, intuition, and experience
- **Methods**
  - Brainstorming, Delphi technique, storyboarding, focus groups, surveys, questionnaire, checklists, one-on-one meetings, Interviews

Qualitative Risk Analysis methods

Brainstorming

- A group decision-making technique designed to generate a large number of creative ideas through an interactive process.

Delphi Technique

- Delphi is based on the principle that decisions from a structured group of individuals are more accurate than those from unstructured group
- The experts answer questionnaires in two or more rounds. After each round, a facilitator provides an **anonymous** summary of the experts' decision from the previous round as well as the reasons they provided for their judgments

Storyboarding

- Processes are turned into panels of images depicting the process, so that it can be understood and discussed

Focus Groups

- Panels of users evaluate the user impact and state their likes and dislikes regarding the safeguard being evaluated

Scenario

- Uses a single major threat scenario and evaluated in detail to assign a threat level, loss potential, and advantages of a safe guard

Questionnaires

- Limit the responses of participants more than surveys, so they should be used later in the process

Checklist

- Used to make sure safeguards being evaluated cover all aspects of the threats

Comparison

Qualitative	Quantitative
• Requires no calculations • Involves high degree of guess work • Provides general areas and indications of risk • Does not allow Cost/benefit analysis • Based on opinions of individuals • Eliminates the opportunity to create a dollar value for Cost/benefit analysis • Hard to develop a security budget from the results	• Does more complex calculations • Mathematical and statistical calculations • Uses independently verifiable and objective metrics • Allows cost/benefit analysis • It is easier to automate • Used in Risk management performance tracking • Without automated tools, the process is very difficult • More preliminary work is needed to gather detailed information about the environment

Total Risk vs Residual Risk

- **Total Risk** = Threats * Vulnerability * Asset Value

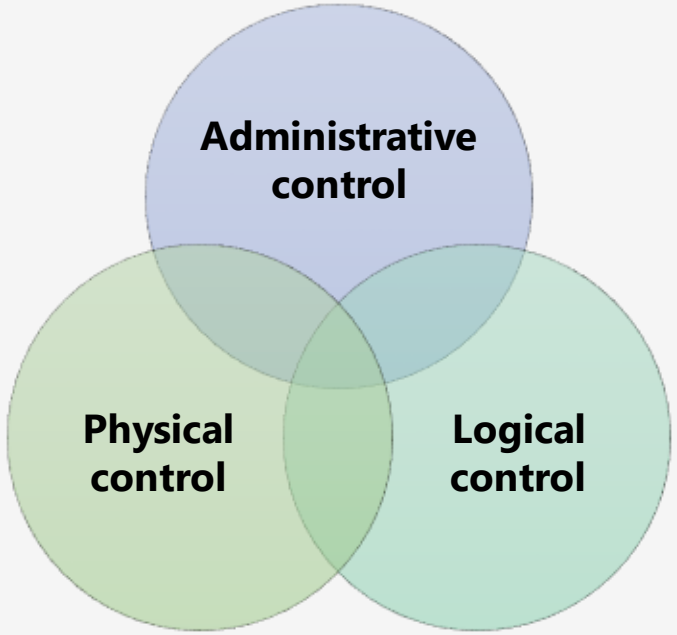
- **Residual Risk** = (Threats * Vulnerability * Asset Value) * control gaps

  - **Residual Risk** = Total Risk – countermeasures

Risk Response

Reduce the risk	Risk Assignment or Transfer	Risk Acceptance	Risk Avoidance	Risk Rejection or Ignore
• Implement safeguards to eliminate or vulnerabilities or block threats	• Placement of the cost of risk to another entity	• Conscious decision to live with the risk	• Terminate the activity that is introducing the risk	• Unacceptable response to risk is reject or ignore the risk

Countermeasure Categories



Administrative Control

- Policies and procedures defined by an organization
- Also referred as **management controls**
- **Focuses on personnel and business practices**
- Eg: policy, Hiring practice, training, Data classification.

Technical control

- **Involves the hardware and/or software** mechanisms used to manage and provide protection
- Eg: firewall, password, biometric, authentication systems, IDS, routers, AV

Physical Control

- Physical mechanisms deployed to prevent, monitor, detect contact with systems or facilities
- Eg: guards, fences, CCTV, dogs, mantraps, alarms

Countermeasure Types

Deterrent	Preventive	Detective	Compensating	Corrective	Recovery	Directive
• Discourage violation • Deployed against individuals • Eg:Policy, locks, fences, guards, dogs	•Stop unwanted or unauthorized action • Fences, locks, biometrics, encryption, firewall	•Deployed to discover unwanted or unauthorized action •Operates after the fact • CCTV, Audit logs, Job rotation, Mandatory vacation, IDS	• Any control used in addition to or in place of another control • Usually implemented if the primary control cannot be implemented or exceeds the ALE	• Modifies the environment to return systems to normal state after an unwanted activity • Attempts to correct any problem that has occurred	•Extension of corrective control but have more advanced abilities • Backup and restore	•Deployed to direct, confine or control actions of the subjects on the object • ATM, posters, monitoring, supervision

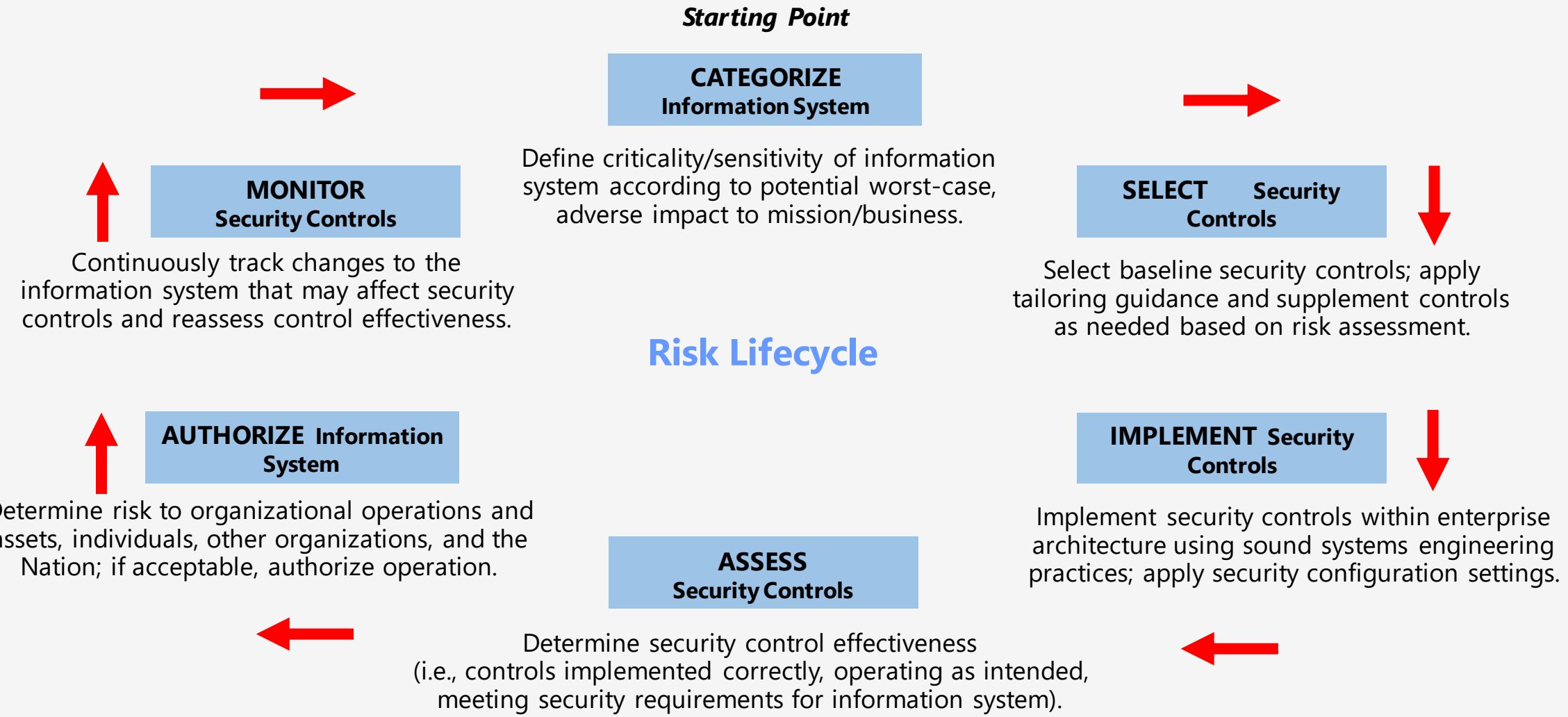
Countermeasure Selection

Modularity	Should provide uniform protection	Provide override functionality	Default to least privilege	Flexibility and security
Should not panic users	Clear distinction between user and admin	Minimum human intervention	Easily upgraded	Auditing functionality
Output should be in useable format	Testable	Should not introduce new compromise	System and user performance	

Risk Management Framework

- A guideline of how a Risk should be assessed, resolved and monitored
- Two key frameworks
  - RMF – NIST 800-37
  - CSF – Cyber Security Framework

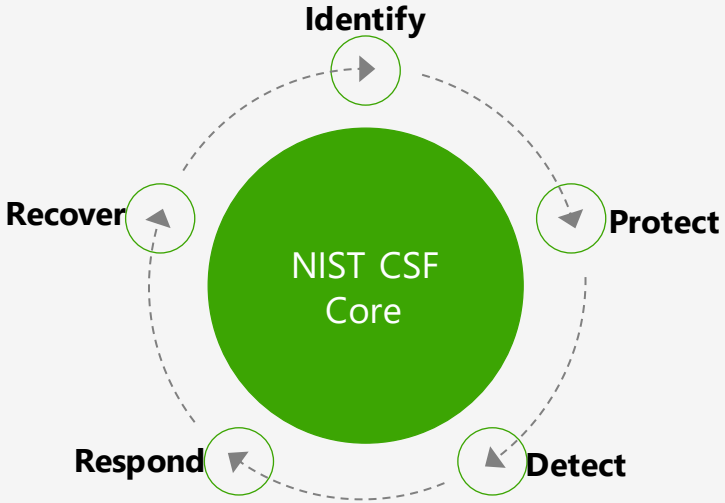
NIST 800-37

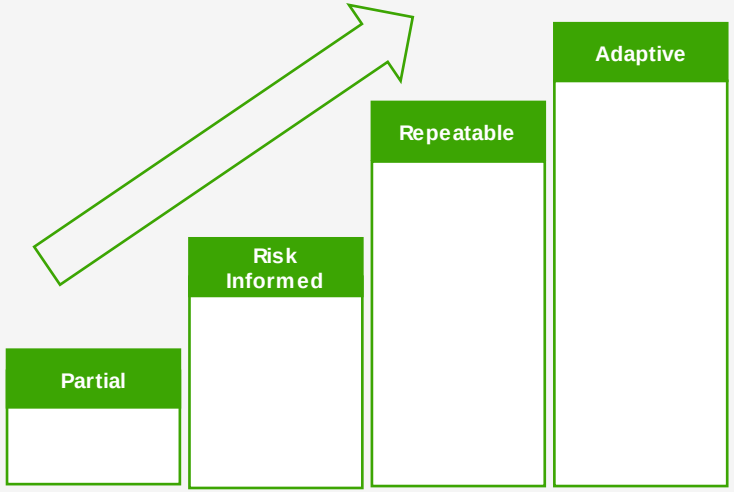

Starting Point
CATEGORIZE
Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.
SELECT Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.
IMPLEMENT Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.
ASSESS
Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).
AUTHORIZE Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.
MONITOR
Security Controls
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
Risk Lifecycle

Cyber Security Framework

- The Framework was designed to enhance cybersecurity posture, providing a scalable format for executives, management, and staff.

Core	Tiers	Profiles
• 5 ‘Functions’ • 22 ‘Categories’ • 98 ‘Subcategories’	• Partial • Risk Informed • Repeatable • Adaptive	• Current • Target





Source: Risk_Compliance_Update_2_25_2016

Audit

CSA STAR

- STAR Two levels
  - **Level 1**
    - Self assessment provided by the CSP
    - Weak form of assurance
  - **Level 2** – Third-party audit report given to CSP
  - **Level 3** – Third-party continuous monitoring

All the best