Secure Software Design and Engineering
(CY-321)

Protection Needs Elicitation (PNE)

Dr. Zubair Ahmad

A kind Reminder

- **Attendance?**

  - Active Attendance
  - **Dead Bodies.**
  - **Active Minds**
  - Mobiles in hands -> Mark as absent
  - 80% mandatory

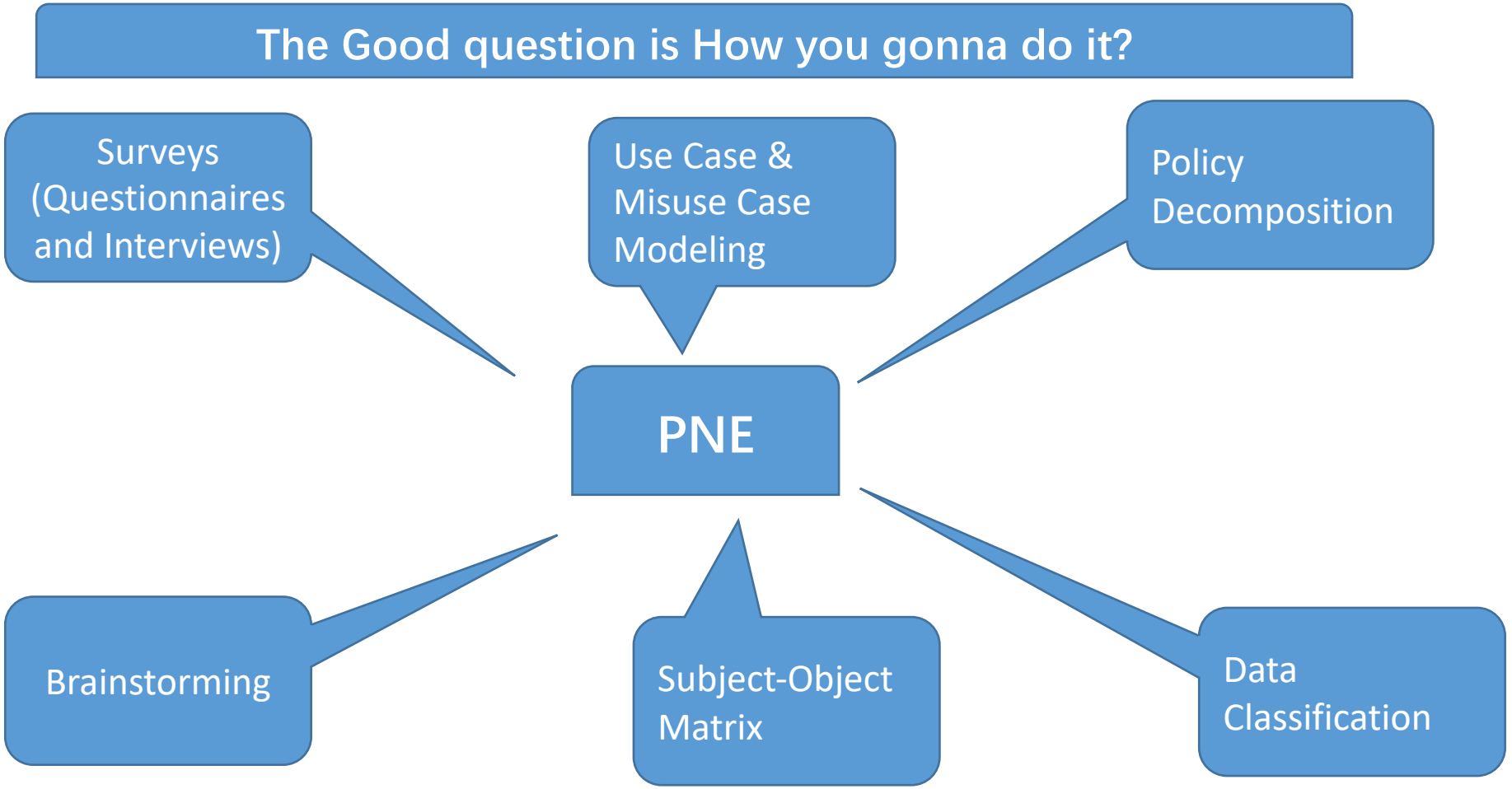
Protection Needs Elicitation (PNE)

The determination of security requirements

The discovery of assets that need to be protected from unauthorized access and users

- **Engage the customer**
- **Seek customer acceptance**
- **Prioritize based on customer needs**
- **Information management modeling**
- **Conduct threat modeling and analysis**
- **Develop information protection policy**

Protection Needs Elicitation (PNE)



Protection Needs Elicitation (PNE)

Brainstorming → **Quick-and-dirty way**

Brainstorming is the quickest and most unstructured method to glean security requirements

In this process, none of the expressed ideas on security requirements are challenged but instead they are recorded

Shortcomings

Brainstorming solutions are usually not comprehensive and consistent because it is very subjective

High degree of likelihood that the brainstormed ideas don't directly relate to the business, technical and security context of the software

Surveys (Questionnaires and Interviews)

The effectiveness of the survey is dependent on how applicable the questions in the surveys are to the audience that is being surveyed

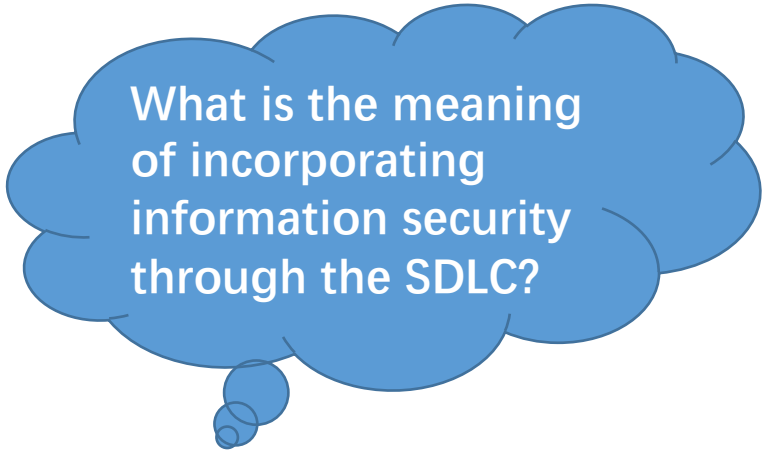
To collect functional and assurance requirements.

The questionnaires are not a one size fits for all type of survey

Both explicitly specified questions as well as open ended questions should be part of the questionnaire

Protection Needs Elicitation (PNE)

Policy Decomposition



One of the sources for security requirements is internal organizational policies that the organization need to comply with

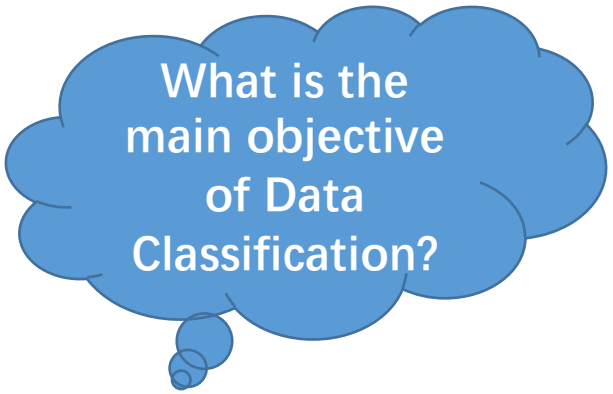
the decomposition process is objective and compliant with the security policy, and not merely someone's opinion

Policy Decomposition

Policy Documents Internal & External	High level Objectives	Security Requirements	Software Security Requirements
SOX	Confidentiality	Information Classification & Handling	Input Validation
PCI DSS	Secure Transmission	Identity Management	Exception Handling
Authentication Policy	Privacy		Output Encoding
HIPAA			

Data Classification

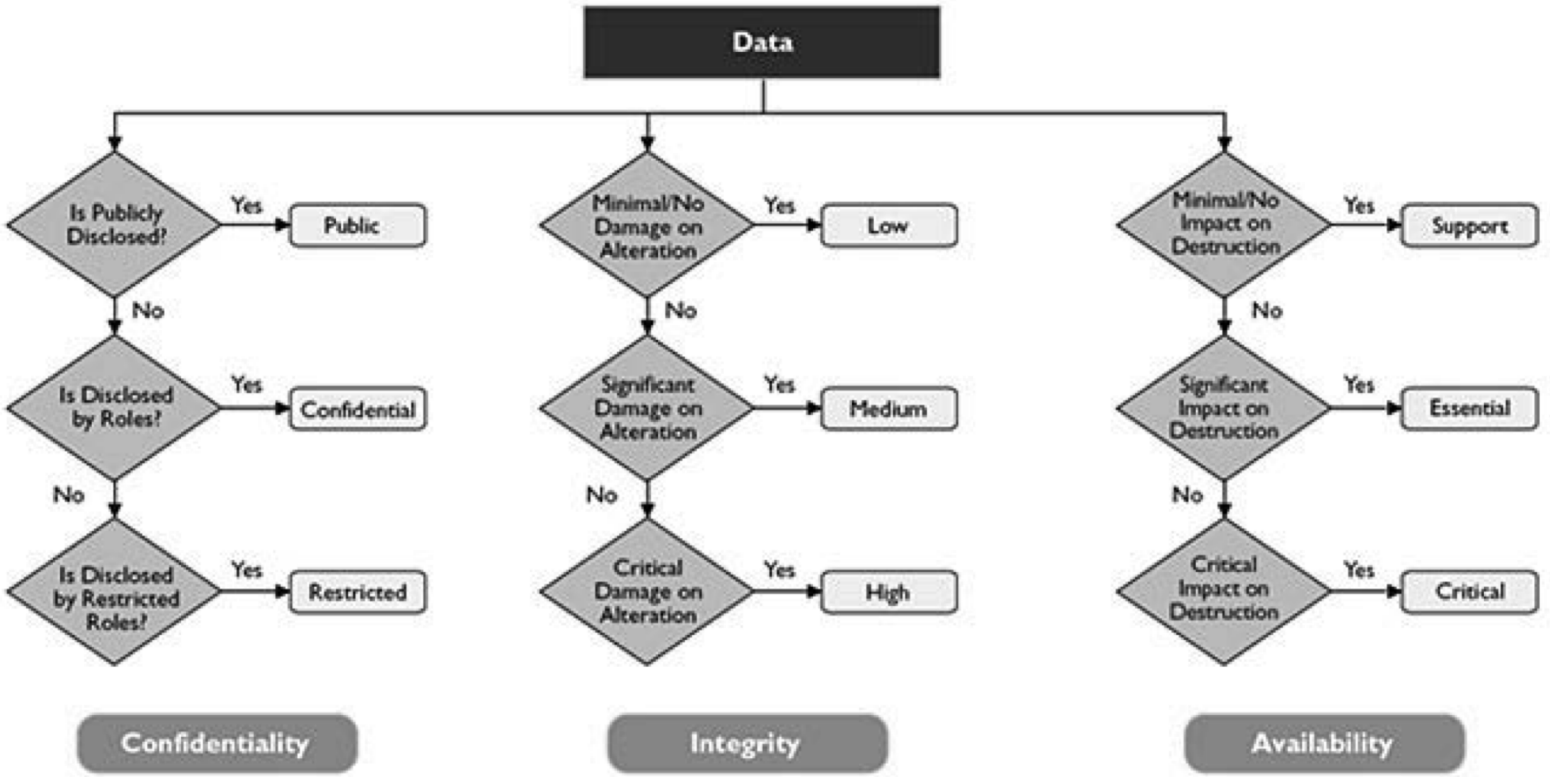
Data classification is based on CIA



Data classification can also assist in increasing the quality of risk based decisions

The data quality and characteristics are known upon classification, decisions that are made to protect them can also be made appropriately.

Data Classification



Data Lifecycle Management (DLM)

Same like *Information Lifecycle Management (ILM)?*

DLM products primarily deals with data attributes such as file types and age of files

ILM products can usually handle more complex situations, including contents within the stored data

Generated (i.e., created) and **Used** (i.e., processed), **Transmitted**, **Stored**, and **Archived**

Subject/Object Matrix

A subject-object matrix is a two-dimensional representation of roles and components

The subjects or roles are listed across the columns and the objects or components are listed down the rows

A subject-object matrix is a very effective tool to generate misuse cases

Protection Needs Elicitation (PNE)

Use Case & Misuse Case Modeling

Use Cases

A use case models the intended behavior of the software or system

The sequence of actions and events that are to be taken to address a business need

Use case modeling is meant to model only the most significant system behavior

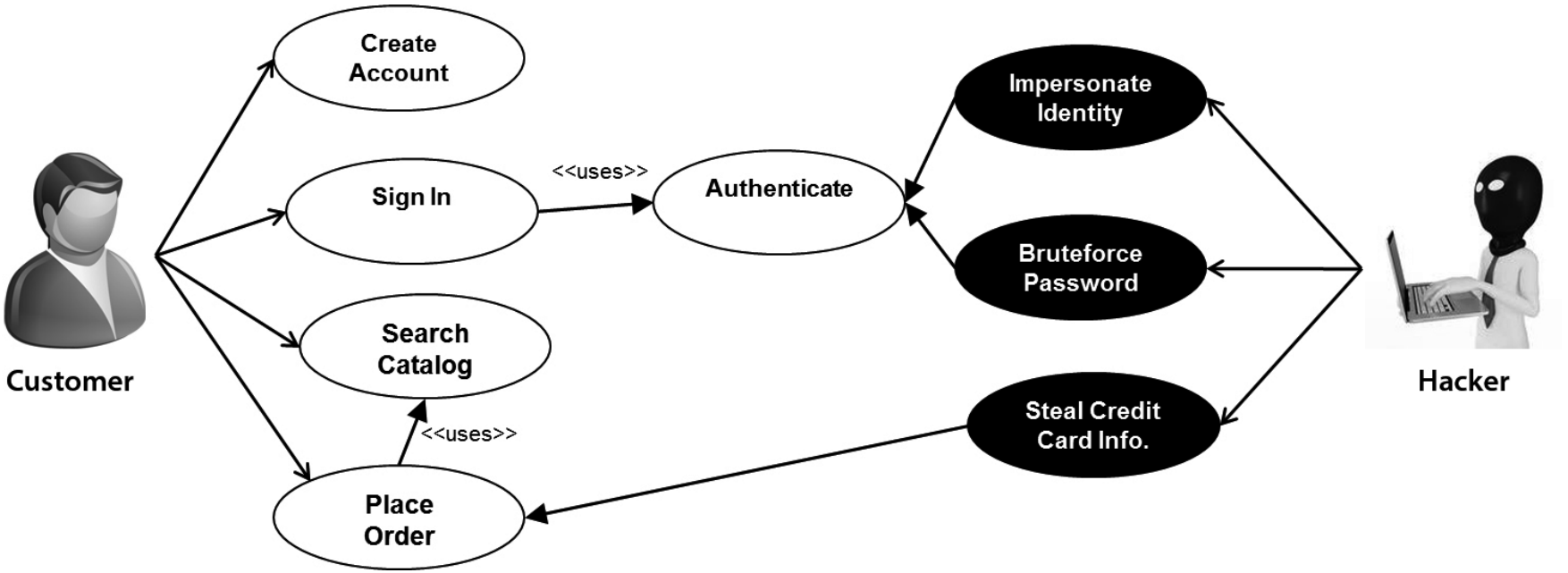
Use case modeling includes **identifying actors**, intended system behavior (use cases), and sequences and relationships between the actors and the use cases

Misuse Cases

Misuse cases, also known as abuse cases help identify security requirements by modeling negative scenarios.

Misuse cases can be created through brainstorming negative scenarios like an attacker

Use Case & Misuse Case Modeling



Requirements Traceability Matrix (RTM)

Key Benefits

Ensures that No scope creep occurs, i.e., the software development team has not inadvertently or intentional added additional features that were not requested by the user

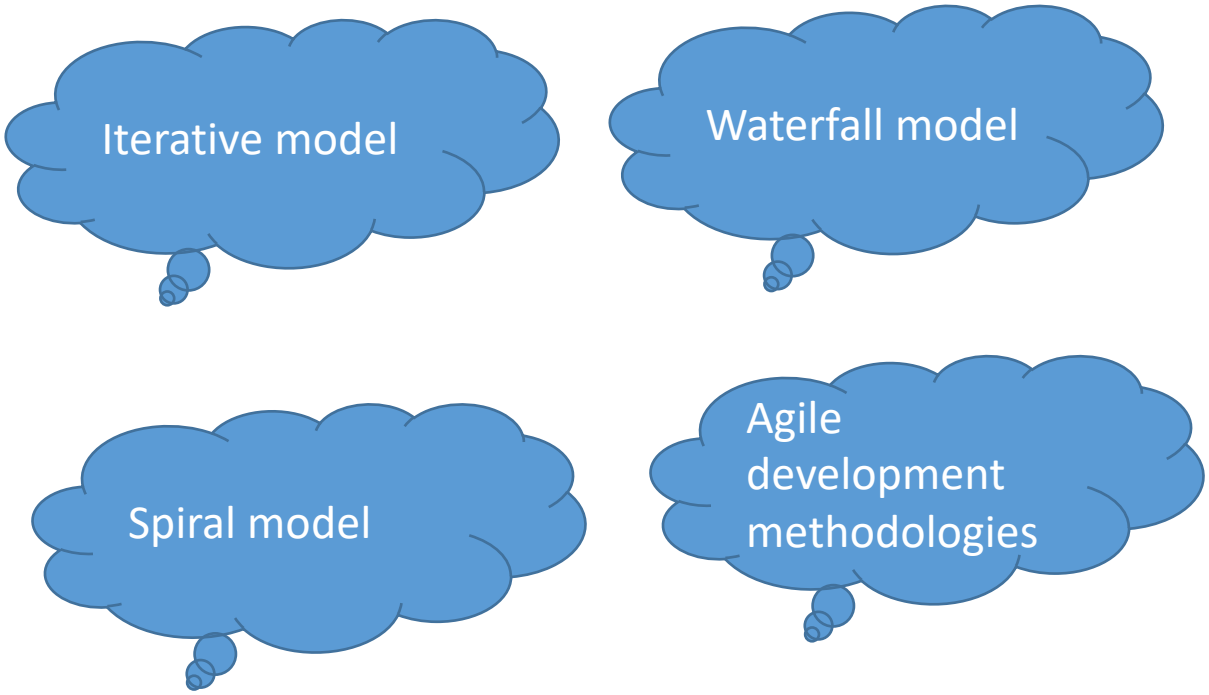
Assures that the design satisfies the specified security requirements

Ensures that implementation does not deviate from secure design

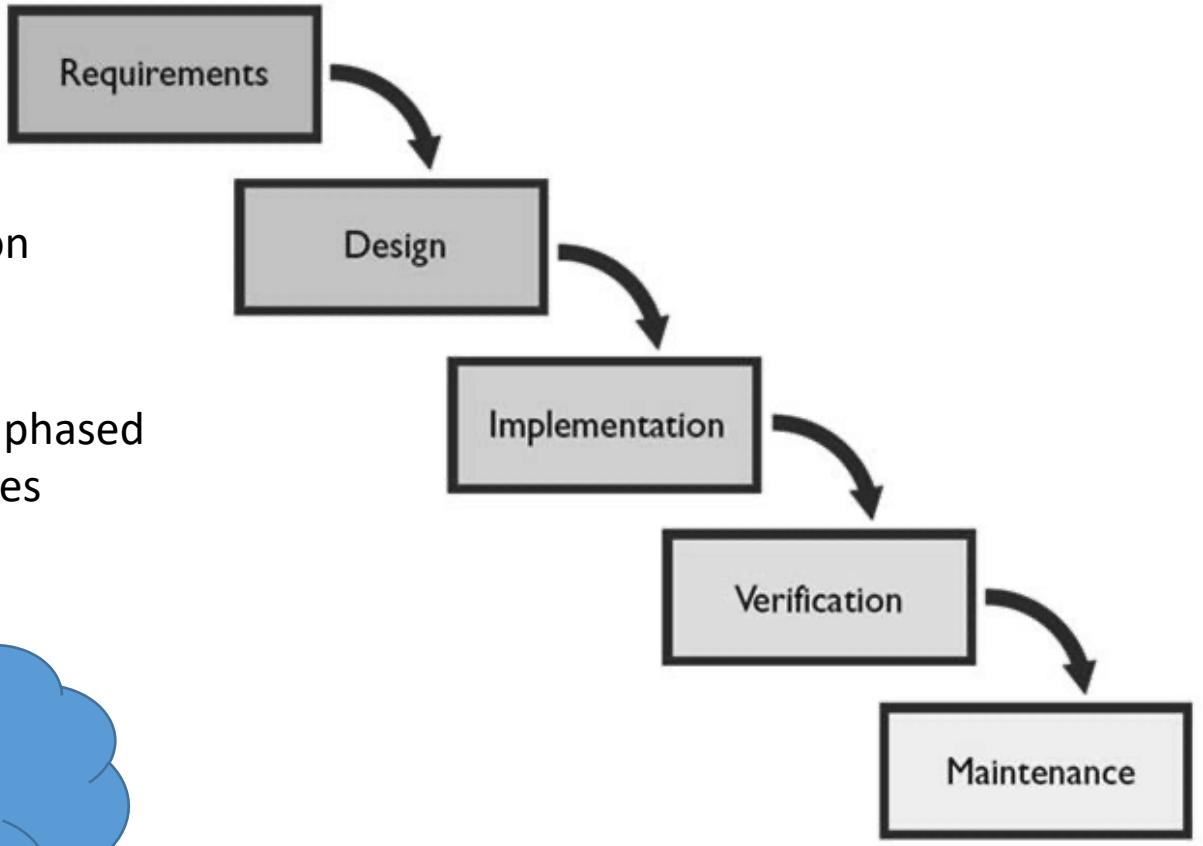
Provides a firm basis for defining test cases

SDLC models

A structured and methodical process that requires the interplay of people expertise, processes and technologies



Waterfall Model



Just as water can flow in only one direction down a waterfall,

Highly structured, linear and sequentially phased process characterized by predefined phases

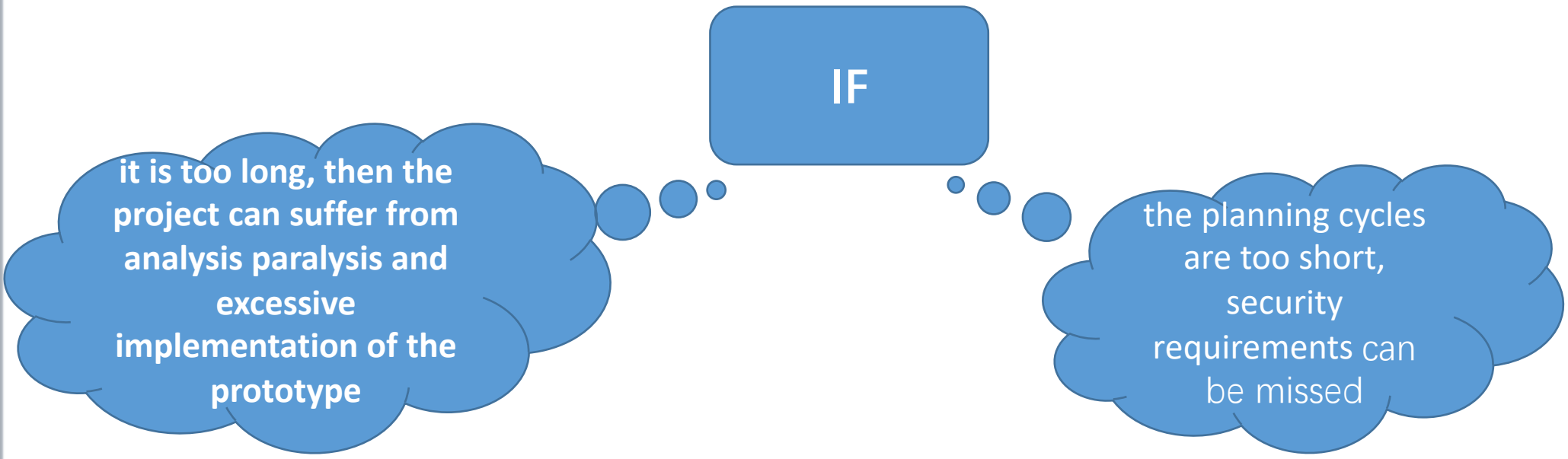
What if you miss anything to a specific stage?

Iterative Model

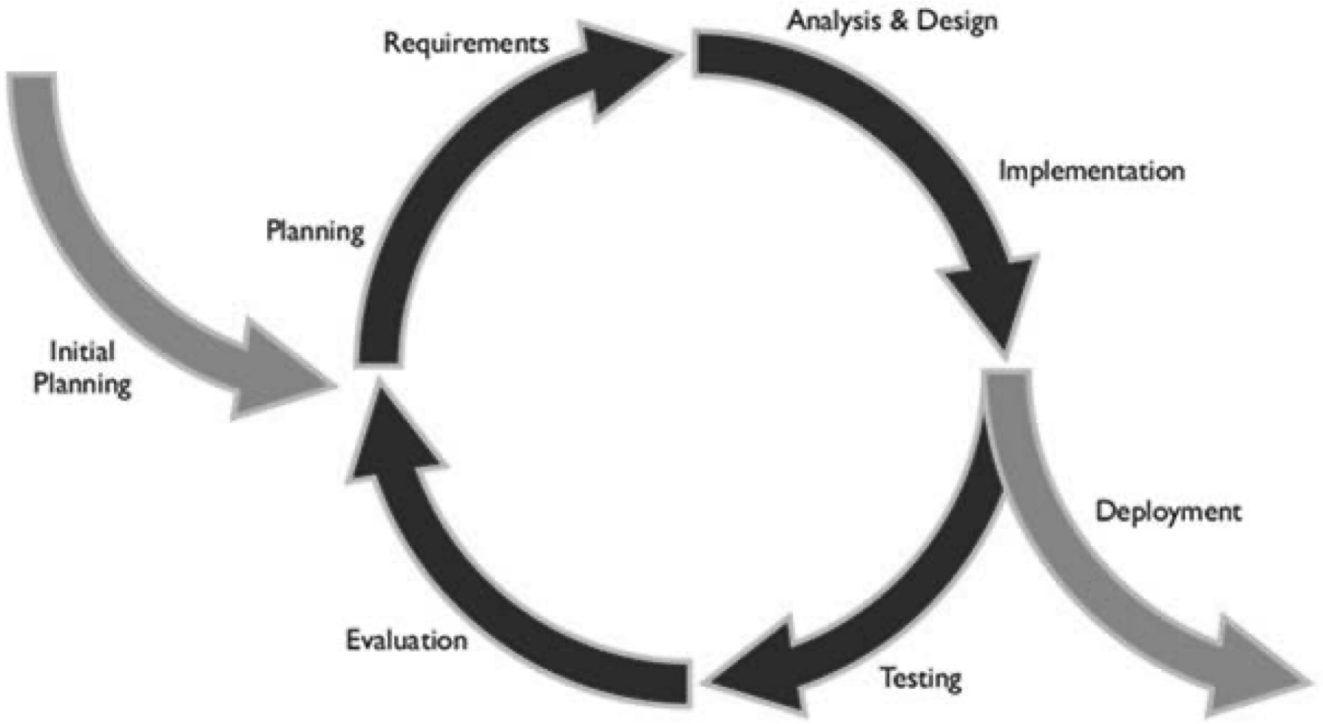
Prototyping model in which each version is a prototype of the final release

The project is broken into smaller versions and developed incrementally

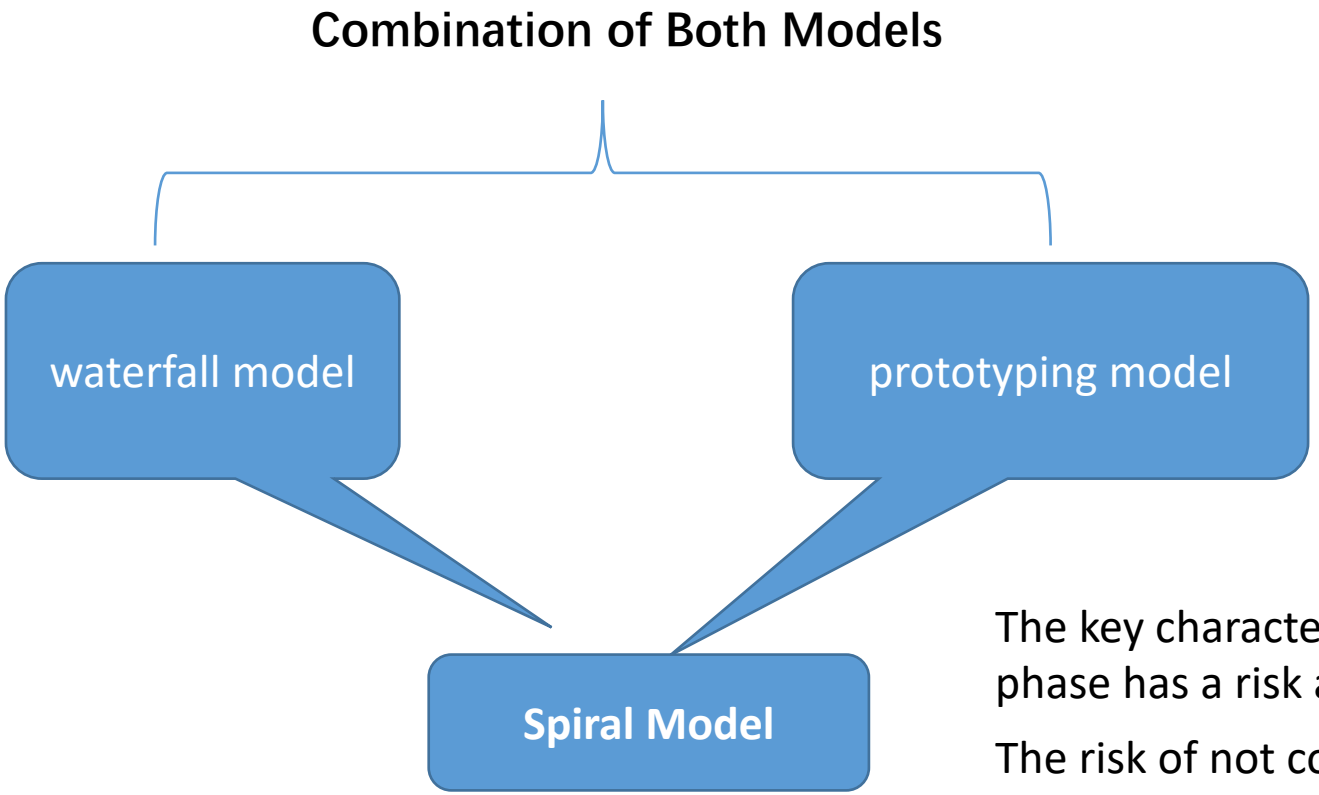
Prototypes can be built to clarify requirements and then discarded or they may evolve into the final version



Iterative Model



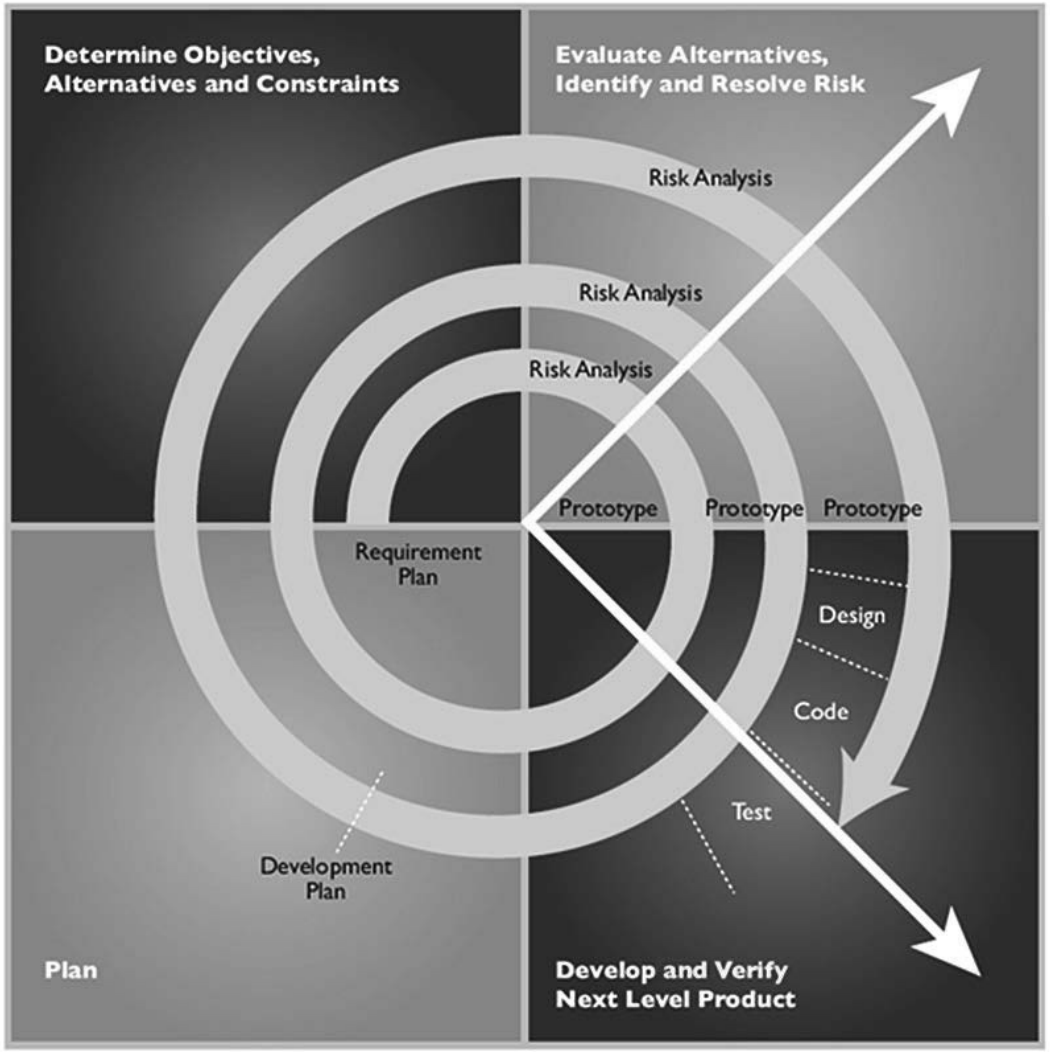
Spiral Model



The key characteristic of this model is that each phase has a risk assessment review activity

The risk of not completing the software development project within the constraints of cost and time is estimated and the results of the risk assessment activity is used to find out if the project needs to be continued or not

Spiral Model



Agile Development Methodologies

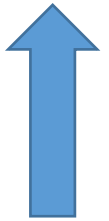
Iterative development with the goal of minimizing software development project failure rates by developing the software in multiple repetitions (**iterations**) and small timeframes (called **timeboxes**)

Each iteration includes the full SDLC

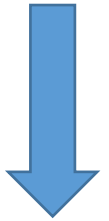
Extreme Programming (XP) model

Scrum programming approach

changes can be made quickly



Primary Benefits



Uses feedback that is driven by regular tests and releases of the evolving software as its primary control mechanism

Agile Development Methodologies

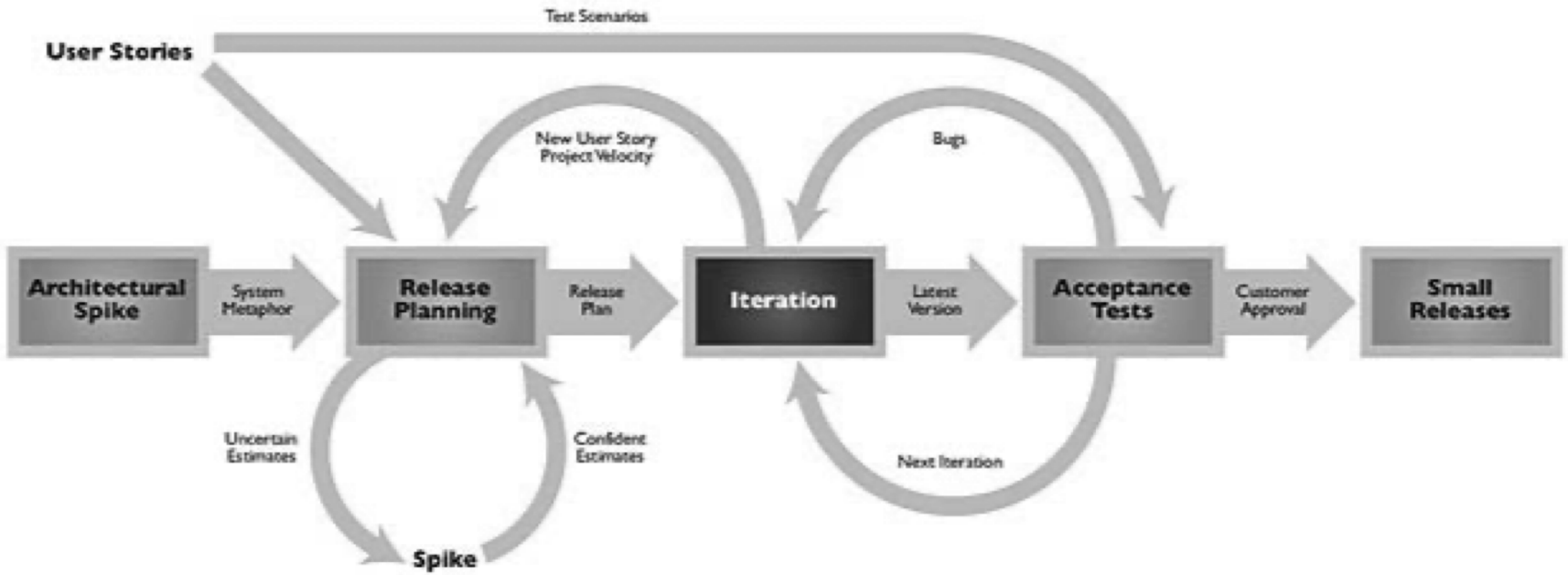
Extreme Programming (XP) model

“people-centric” model of programming and is useful for smaller projects

storyboards and architects user requirements in iterations and validates the requirements using acceptance testing

Agile Development Methodologies

Extreme Programming (XP) model

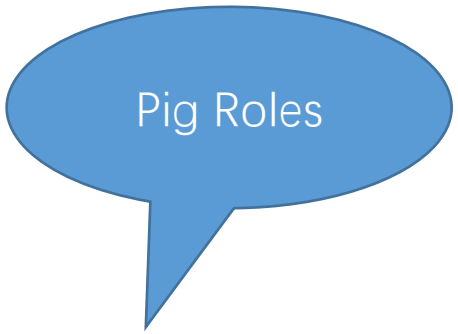


Agile Development Methodologies

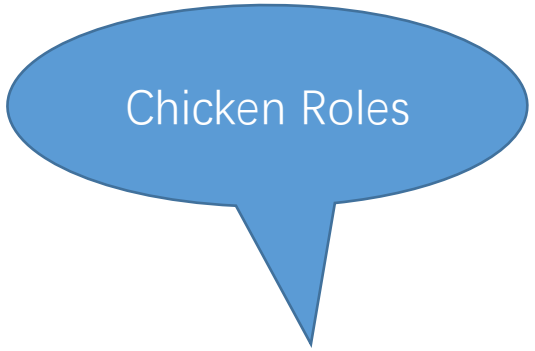
Scrum programming approach

Call for 30-day release cycles to allow the requirements to be changed on the fly, if necessary

A prioritized list of high level requirements is first developed which is known as a **Product Backlog**



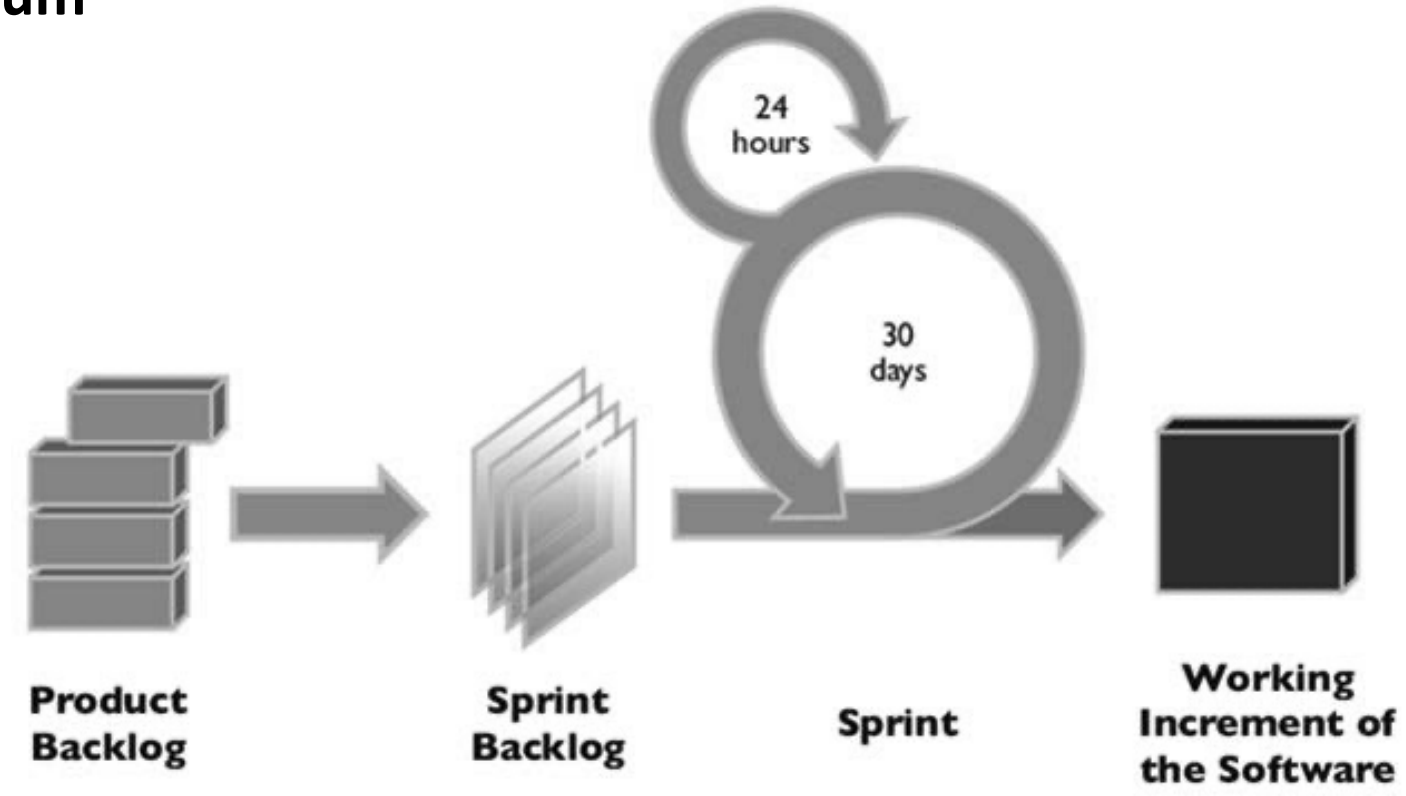
Those who are committed



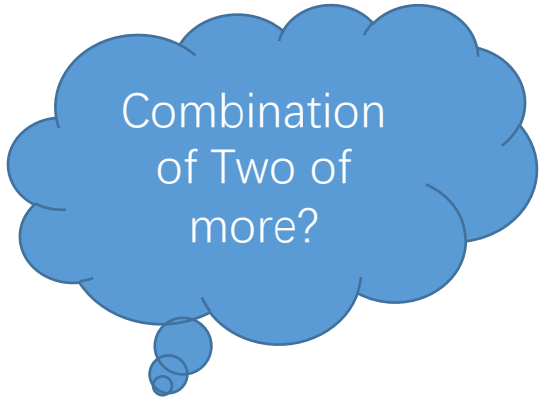
The users who will use the software being developed, the stakeholders (the customer or vendor) and other managers

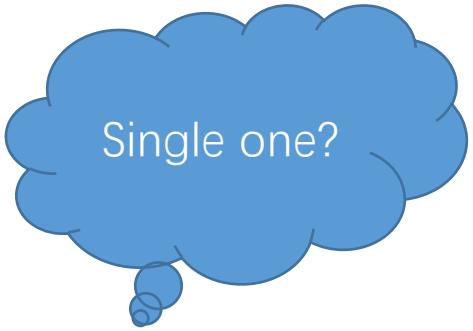
Agile Development Methodologies

Scrum



Which Model Should We Choose?





Yes

Data anonymization assures privacy

Key Guidelines

If you need to collect it for processing only, collect it only after you have informed the user that you are collecting their information and they have consented, but don't store it

If you have the need to collect it for processing and storage, then collect it, with user consent, and store it only for an explicit retention period that is compliant with organizational policy and/ or regulatory requirements

If you have the need to collect it and store it, then don't archive it, if the data has outlived its usefulness and there is no retention requirement.

Privacy and Software Development

Replacement → **(Pseudonymization)**

Replaces identifiable data with an artificial identifier (pseudonym)

The original data is stored separately and mapped via a key

Common in **medical research** where user tracking is required without revealing identities.

Use Case?

Suppression

Completely removes or masks specific parts of data that could lead to identification

Used when **partial data exposure is acceptable** but sensitive details need protection

Use Case?

Generalization

Replaces specific values with broader categories to reduce identifiability

Preserves some level of utility for analysis while reducing re-identification risks

Use Case?

Generalization

k-Anonymity

A privacy model that ensures that each individual in a dataset is indistinguishable from at least **k−1** other individuals based on their **quasi-identifiers** (QIs)

Quasi-identifiers are attributes that, while not directly revealing identity, can be used to re-identify individuals when combined

Perturbation

Alters data slightly (adds noise) while maintaining statistical accuracy

Ensures individual values cannot be traced back to original subjects

Applied in **machine learning models** to train on private data while reducing risk of exposure.

Use Case?

Perturbation

Differential Privacy (DP)

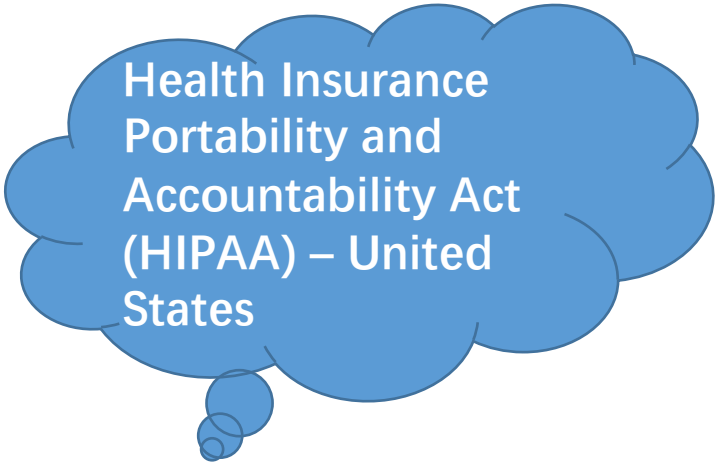
A mathematical framework that ensures that the presence or absence of an individual in a dataset does not significantly affect the results of queries on the dataset

Used in **machine learning, statistics, and data analysis** to provide strong privacy guarantees.

Disposition

Final action taken on data at the end of its lifecycle. It involves either securely **retaining, deleting, archiving, or destroying** data based on legal, regulatory, and organizational requirements

Major Privacy Regulations



General Data Protection Regulation (GDPR) – European Union (EU)

- Right to Access
- Right to Rectification
- Right to Erasure ("Right to be Forgotten")
- Right to Data Portability
- Right to Restrict Processing
- Right to Object
- Rights Related to Automated Decision-Making

Fines up to **€20 million** or **4% of global annual revenue**

General Data Protection Regulation (GDPR) – European Union (EU)

The Guardian

Int

News | Opinion | Sport | Culture | Lifestyle

World Europe US Americas Asia Australia Middle East Africa Inequality Global development

Data protection

This article is more than 1 year old

Facebook owner Meta fined €1.2bn for mishandling user information

Penalty from Ireland's privacy regulator is a record for

Facebook's owner, Meta, has been fined a record €1.2bn (£1bn) and ordered to suspend the transfer of user data from the EU to the US.

Invited Talk!!

Drilling Deep: Automatic Security Testing for JavaScript Sandboxes

Abdullah Alhamdan

Ph.D. Scholar at CISPA Helmhotz Center of Information Security Germany

Paper Link:

https://www.usenix.org/conference/usenixsecurity23/presentation/alhamdan

Research Area: Software Security, Program Analysis

Venue: Will share soon

Questions??

zubair.ahmad@giki.edu.pk

Office: G14 FCSE lobby