TRAINING

CSSLP

2021

AGENDA

Domain 2 : Secure Software Requirements

- Sources
- Types
- Elicitation
- Traceability Matrix

Without software requirements, software will fail and without secure software requirements, organizations will

SOFTWARE QUALITY ATTRIBUTES

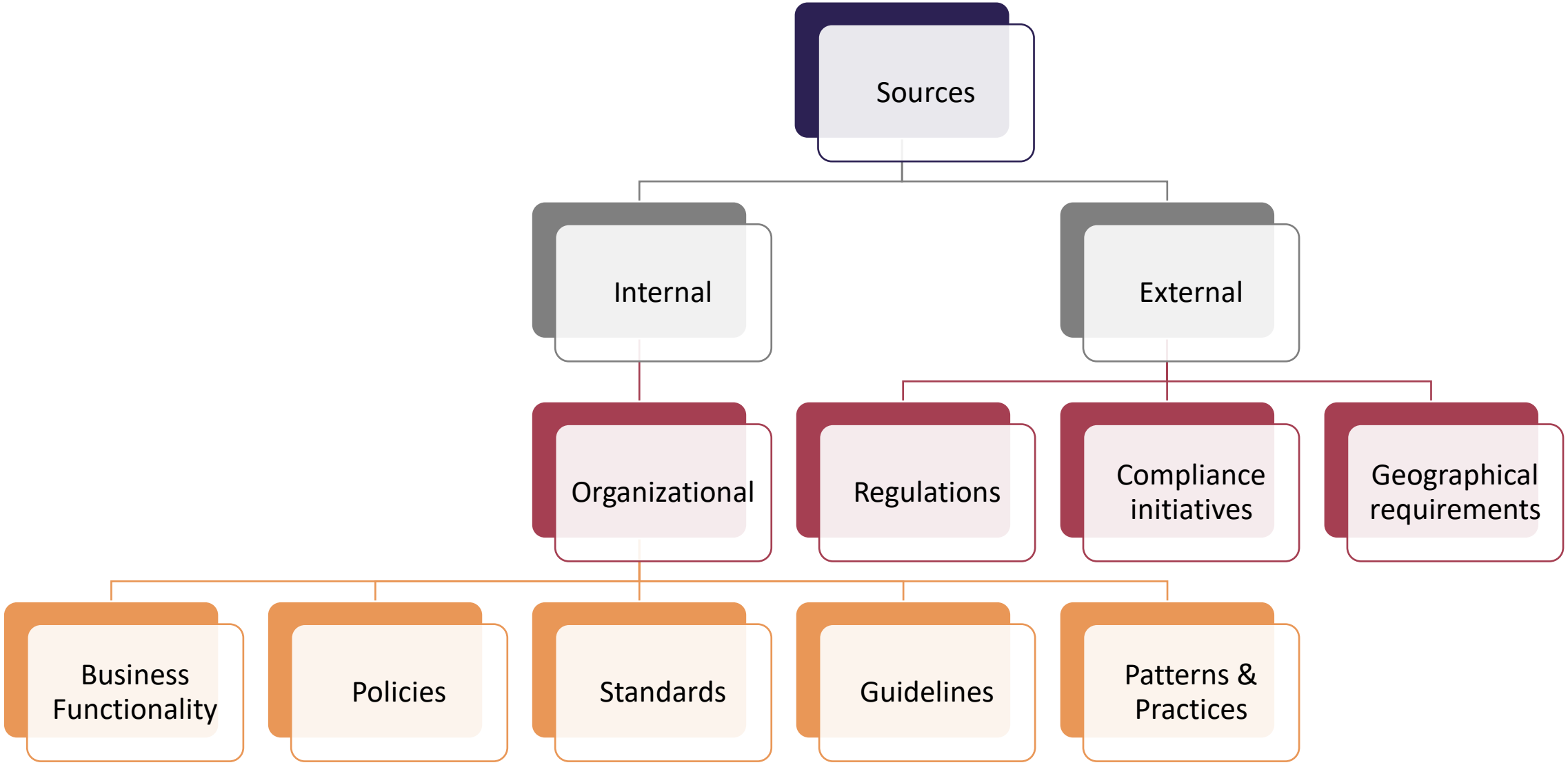
Characteristics of quality

- Reliability : Functions as expected
- Resiliency : Ability to withstand the actions of threat agents
- Recoverability : Ability to restore operations

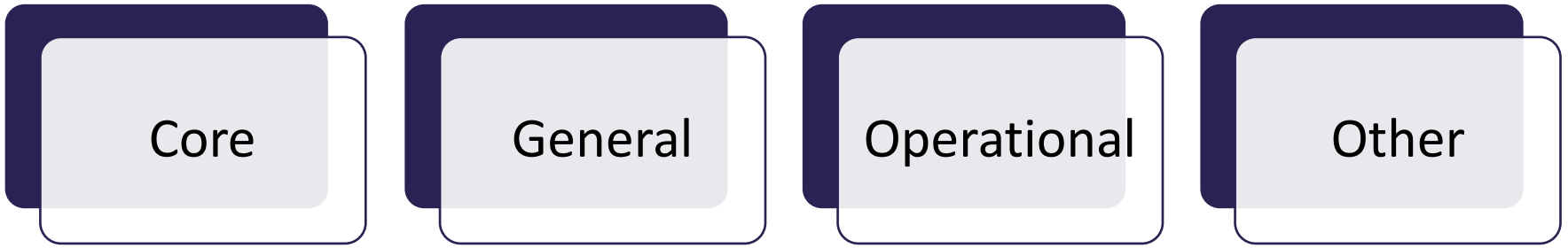
SOURCES

SECURE SOFTWARE REQUIREMENTS

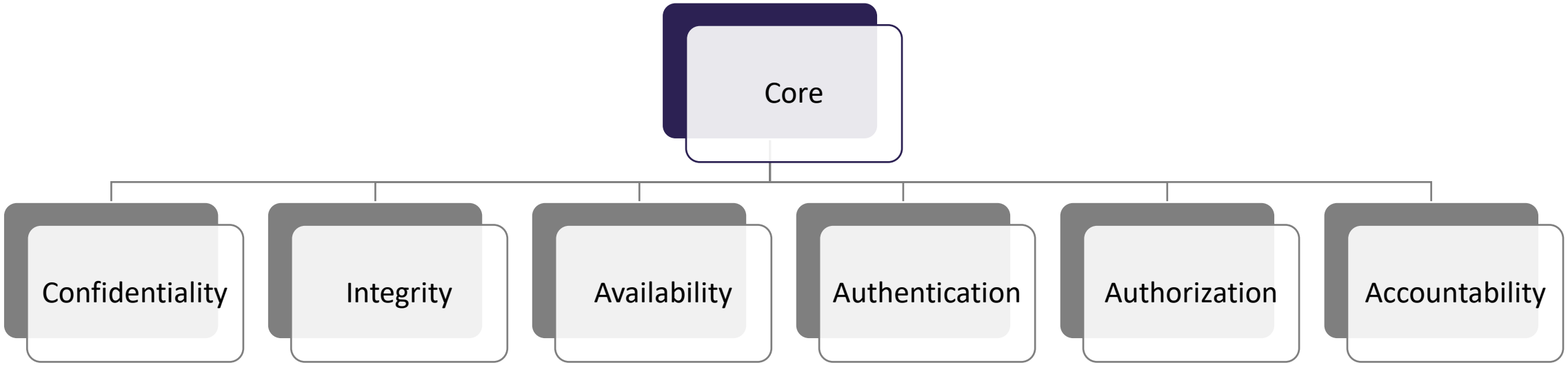
SOURCES


Sources
Internal
External
Organizational
Regulations
Compliance initiatives
Geographical requirements
Business Functionality
Policies
Standards
Guidelines
Patterns & Practices

TYPES OF SECURITY REQUIREMENTS



TYPES OF SECURITY REQUIREMENTS



CONFIDENTIALITY REQUIREMENTS

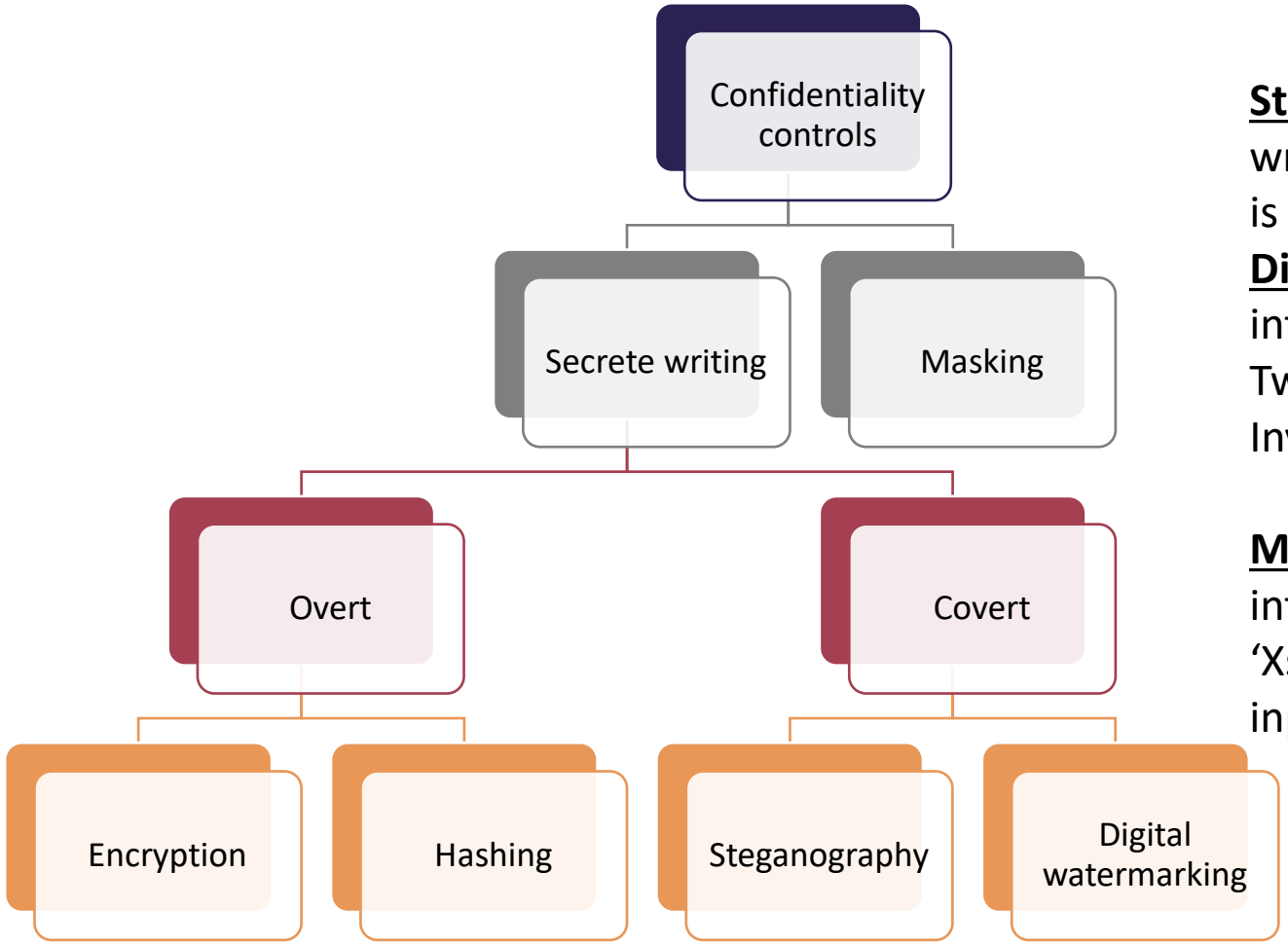
Requirements that address the protection against the unauthorized disclosure of data that is either private or sensitive in nature

Public data

Non-Public data

Any non-public data warrants protection against unauthorized disclosure, so those software requirements must be defined!

CONFIDENTIALITY PROTECTION MECHANISMS

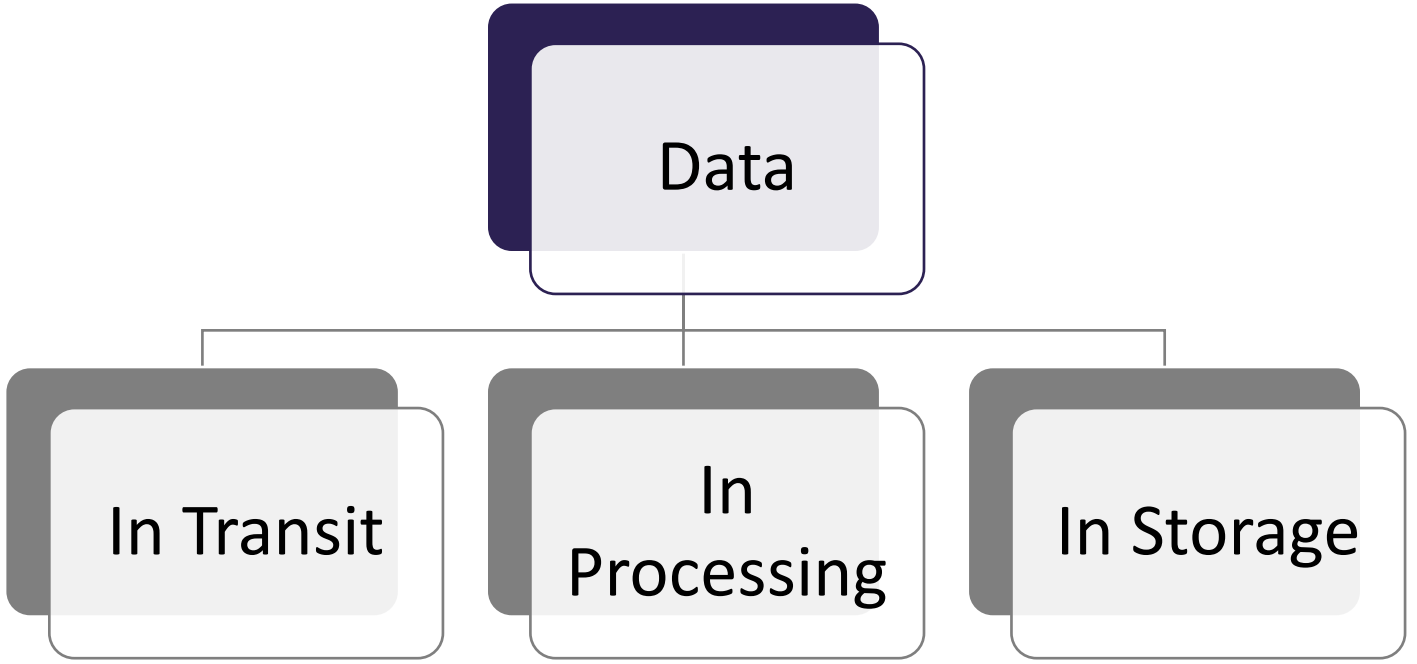


Steganography: Invisible ink writing (Existence of message is hidden)
Digital Watermarking: embed into audio, video or pictures
Two types – Visible and Invisible

Masking : Original information is replaced with 'Xs' or dots like in password input fields.

CONFIDENTIALITY PROTECTION

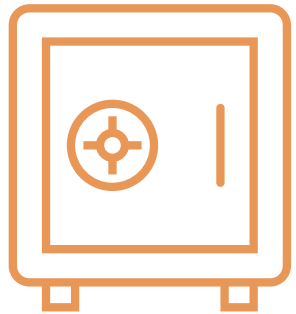
Where to protect?



INTEGRITY REQUIREMENTS

Requirements that addresses

- Reliability assurance
- Protection against unauthorized modifications



System Integrity

Data Integrity

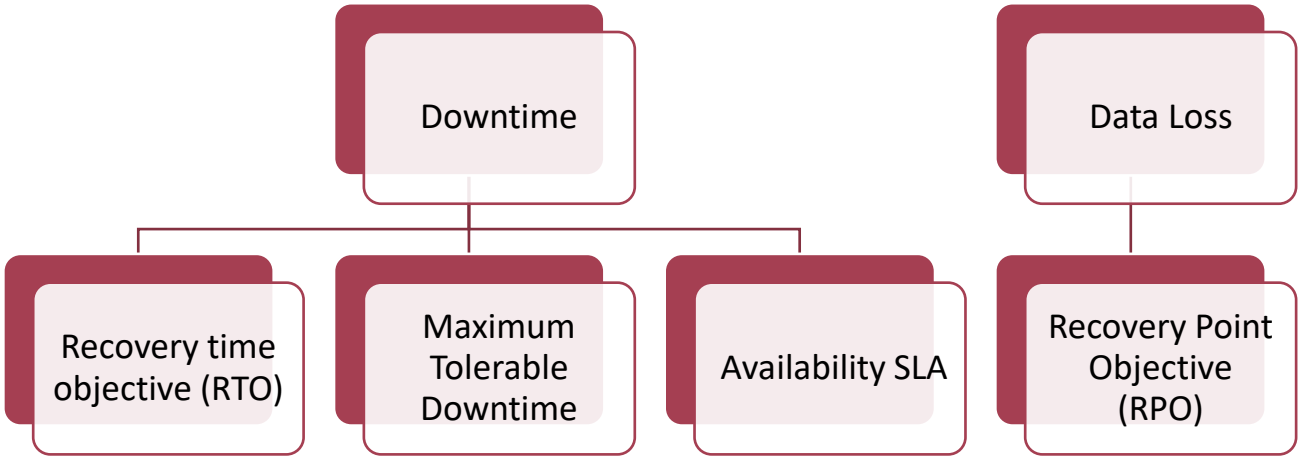
INTEGRITY PROTECTION MECHANISMS

- Validation
- Parity bit checking
- CRC (Checksum)
- Hashing

AVAILABILITY REQUIREMENTS

- Business continuity
- Disaster recovery

SHOP



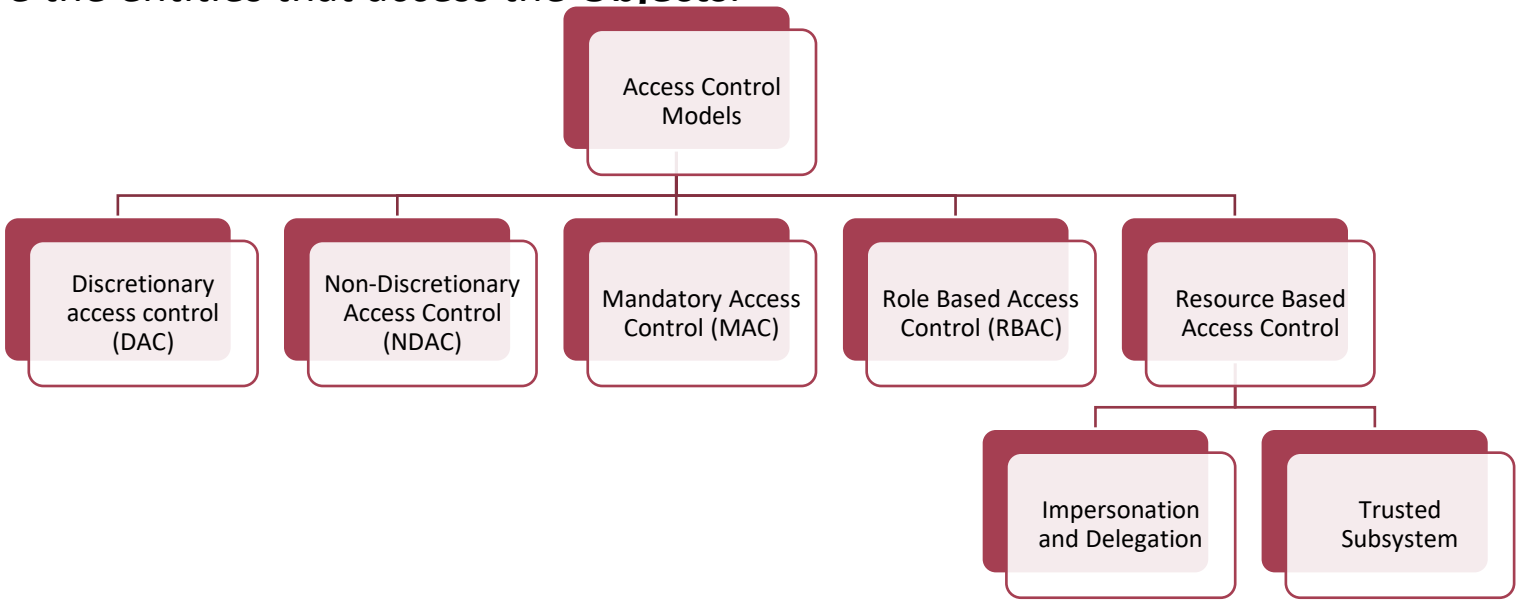
AUTHENTICATION REQUIREMENTS

Process of validating entities claim.

- Anonymous
- Basic
- Digest
- Integrated
- Client Certificates
- Forms
- Token
- Smart Cards
- Biometrics

AUTHORIZATION REQUIREMENTS

Validating the needed rights and privileges to access and perform actions.
Subjects are the entities that access the **Objects**.



Restricted Access

ACCOUNTABILITY REQUIREMENTS

Accountability requirements

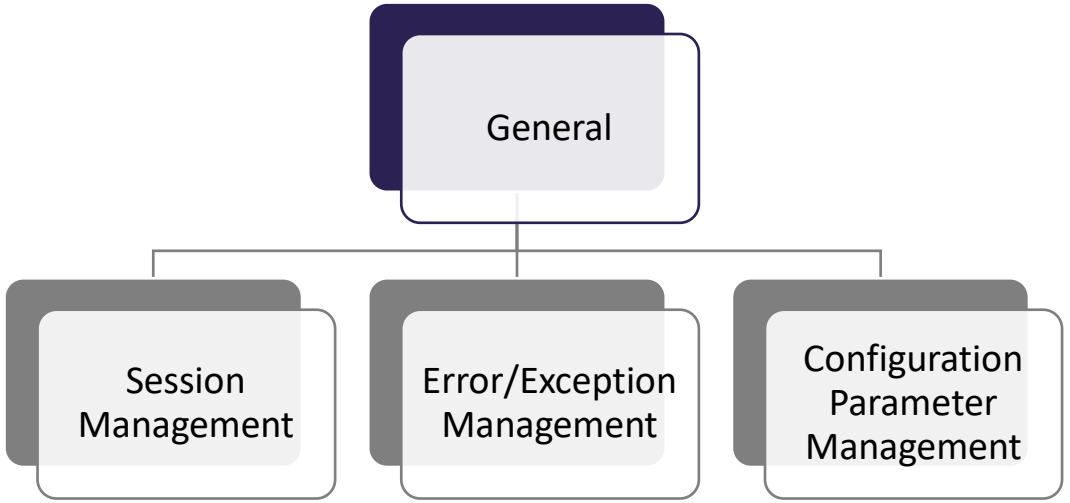
Historical record of user actions to help in Audit Trails.

- Who
- What
- Where
- When

Note: Audit logs must be protected against tampering

Legal

GENERAL SECURITY REQUIREMENTS



Errors and Exception Management requirements

- Potential source of information disclosure

Session Management

Points to Consider

- State Management
- Psychological Acceptability

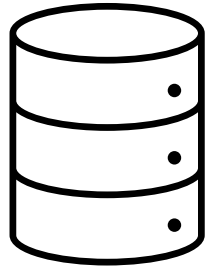
Session Management Requirements Assure that

- Brute force attacks
- Predictability attacks
- Man-in-the-middle hijacking attacks

Configuration Parameter requirements

Software code – Configuration parameters

- Database connection strings
- Internal Threats



Database

REQUIREMENTS - EXAMPLES

Session Management Requirements

“Each user activity will need to be uniquely tracked.”
“The user should not be required to provide user credential once authenticated within the Internet banking application.”
“Sessions must be explicitly abandoned when the user logs off or closes the browser window.”
“Session identifiers used to identify user sessions must not be passed in clear text or be easily guessable.”

Errors & Exception Management Requirements

“All exceptions are to be explicitly handled using try, catch and finally blocks.”
“Error messages that are displayed to the end user will reveal only the needed information without disclosing any internal system error details.”
“Security exception details are to be audited and monitored periodically.”

Configuration Parameters Management Requirements

“The web application configuration file must encrypt sensitive database connections settings and other sensitive application settings.”
“Passwords must not be hard-coded in line code.”
“Initialization and disposal of global variables need to be carefully and explicitly monitored.”
“Application and/or Session OnStart and OnEnd events must include protection of configuration information as a safeguard against disclosure threats”

OPERATIONAL REQUIREMENTS

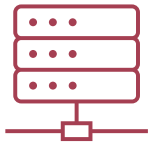
Deployment Environment

Archiving

Anti-Piracy

Deployment Environment

- Internet facing? Or Intranet?
- Behind Demilitarized Zone?
- Privileges in production environment?
- Ports and Protocols?
- Transmitting sensitive or confidential information?
- Load balancing and clustering?
- SSO?
- Event logging and Auditing ?



Archiving Requirements

Either for Business continuity or regulatory requirements or organizational compliance policy

- Where data is stored?
- How long?
- Storage capacity?
- Read-Only
- Time to retrieve?
- Clear text or Cypher?
- Protection on archival data?

Anti-Piracy

COTS PaaS vs SaaS (Online Services)

- Code Obfuscation
- Code Signing
- Anti-Tampering
- Licensing
- IP Protection

REQUIREMENTS - EXAMPLES

Operational Requirements

“Cryptographic keys that are shared between applications should be protected and maintained using strict access controls.”

“Data backups and replications must be protected in secure logs with least privilege implemented.”

“Patching of software must follow the enterprise patch management process and changes to production environments must be done only after all necessary approvals have been granted.”

“Discovered vulnerabilities in the software, that can impact the business and the brand, must be addressed and fixed as soon as possible, after being thoroughly tested in a simulated environment.”

“Incident management process should be followed to handle security incidents and root cause of the incidents must be identified.”

“The software must be continuously monitored to ensure that it is not susceptible to emerging threats.”

Anti-Piracy Requirements

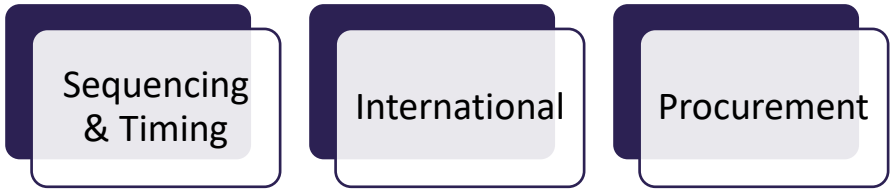
“The software must be digitally signed to protect against tampering and reverse engineering.”

“The code must be obfuscated, if feasible, to deter the duplication of code.”

“License keys must not be statically hard-coded in the software binaries as they can be disclosed by debugging and disassembly.”

“License verification checks must be dynamic, preferably with phone-home mechanisms and not be dependent on factors that the end-user can change.”

OTHER SECURITY REQUIREMENTS



International Requirements

- Legal – Country specific laws
- Technological – example Character encoding

Sequencing and Timing

- Race Condition
- Time of Check
- Time Of Use

Common Sources of race condition

- Undesirable Sequence of Events
- Multiple unsynchronized threads
- Infinite Loops

Procurement Requirements

- Legal protection mechanisms
- Software escrow
- SLAs

PROTECTION NEEDS ELICITATION (PNE)

First step in Information Assurance Technical Framework (IATF) by US National Security Agency(NSA) is PNE

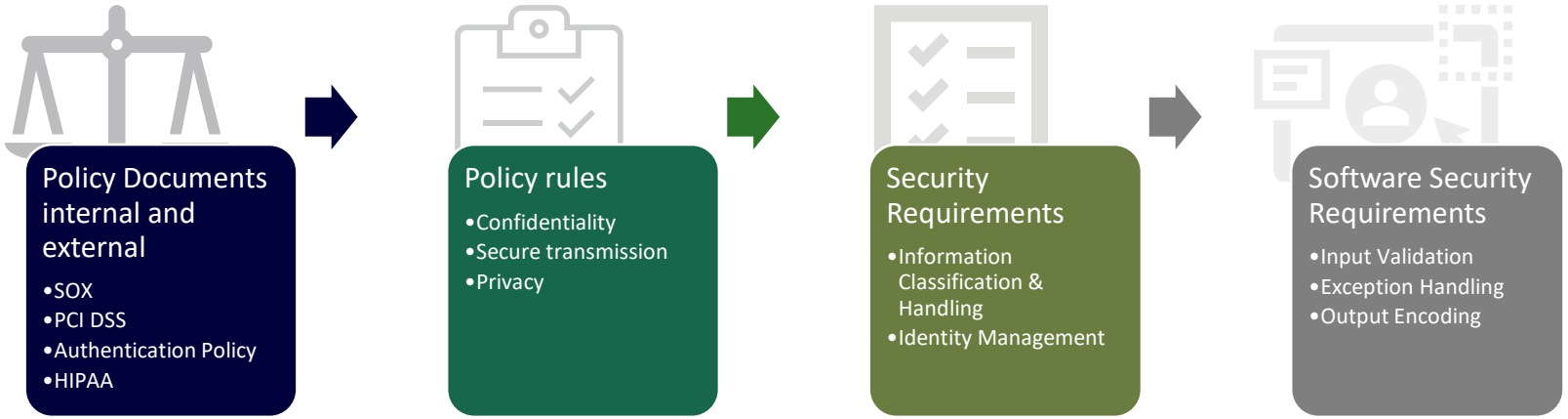
PNE should be conducted in the following order

1. Engage Customer
2. Information Management Modeling
3. Identify least privilege applications
4. Conduct threat modeling and analysis
5. Prioritize based on customer needs
6. Develop Information protection policy
7. Seek customer acceptance

PNE TECHNIQUES

- Brainstorming
- Surveys and Questionaries
- Policy Decomposition
- Data Classification
- Subject-Object Matrix
- Use Case and Misuse case Modeling

PNE - POLICY DECOMPOSITION

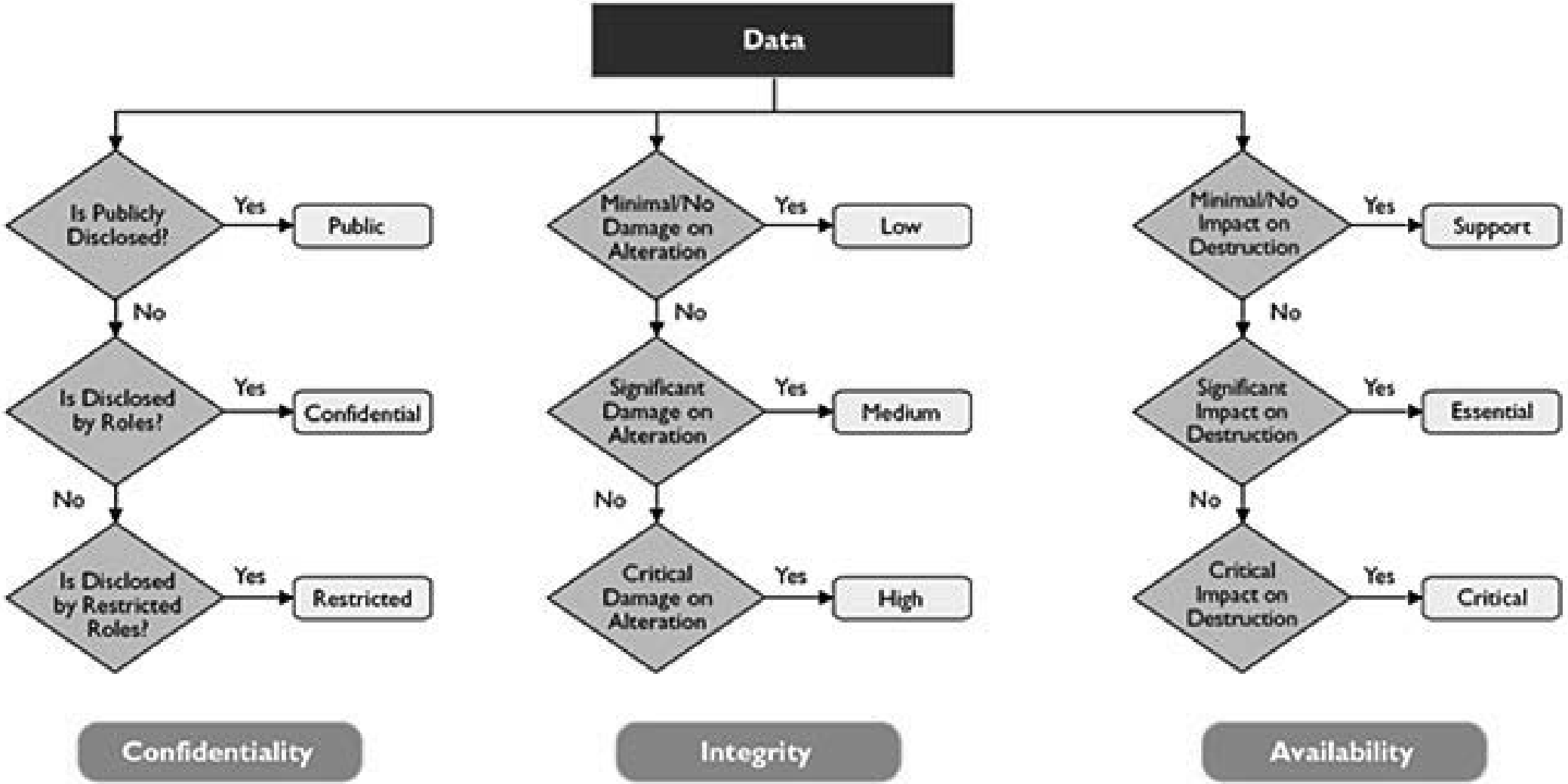


DATA CLASSIFICATION

- **Types of Data**
  - Structured
    - Columns and Rows
    - Organization of data in an identifiable structure also makes the data contents relatively more searchable by data type
  - Unstructured
    - unstructured data has no identifiable structure
      - Examples of unstructured data include images, videos, emails, documents and text.

- **Labelling**
  - Objective of data classification is to lower the cost of data protection and maximize the return on investment when data is protected. Example: Not need to encrypt publicly available data.
  - Assign labels (a level of sensitivity) to information (data) assets, based on potential impact to confidentiality, integrity and availability (CIA), upon disclosure, alteration or destruction.
  - NIST Special Publication 800-18: A framework for classifying information assets based on impact to the three core security objectives, i.e., confidentiality, integrity and availability.
  - Labelling is highly qualitative - High, Medium and Low
  - Categorization is then used to determine security requirements and the appropriate levels of security protection by category.

DATA CLASSIFICATION



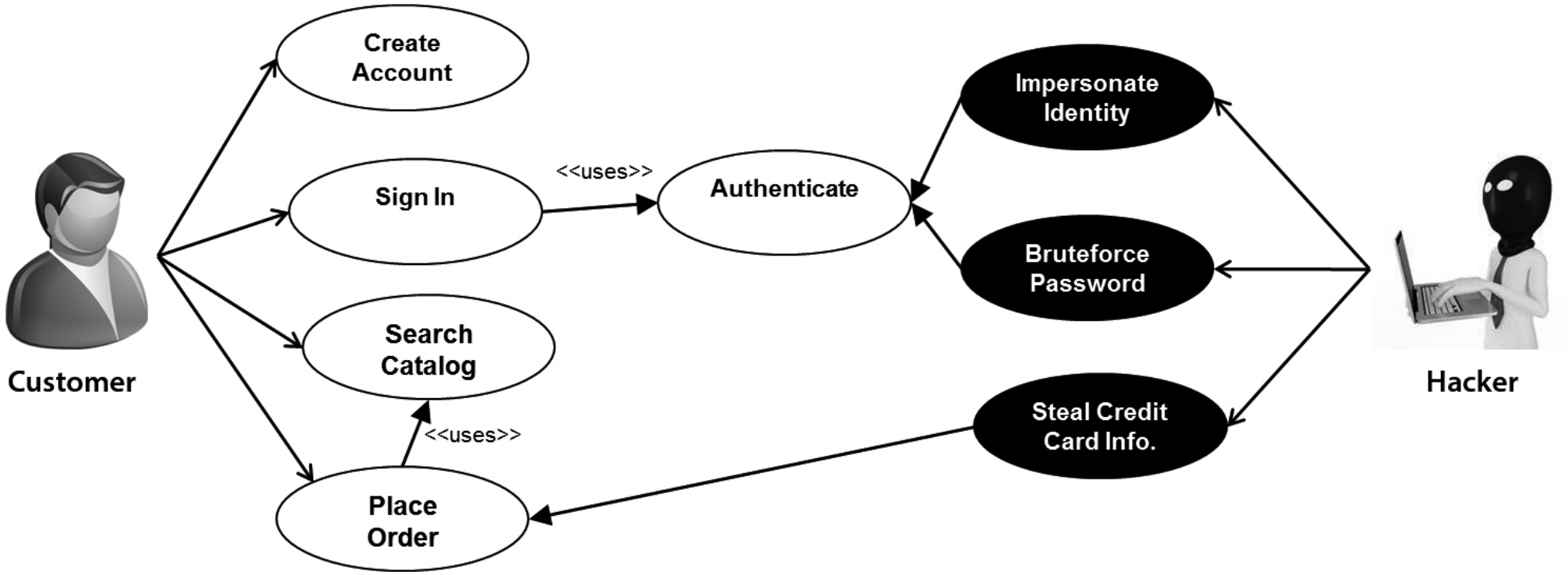
DATA OWNERSHIP AND ROLES

- **Business Owner/Data Owner**
  - Ensure that information assets are appropriately classified.
  - Validate that security controls are implemented as needed by reviewing the classification periodically.
  - Define authorized list of users and access criteria based on information classification. This supports the Separation of Duties principle of secure design.
  - Ensure appropriate backup and recovery mechanisms are in place
  - Delegate as needed the classification responsibility, access approval authority, backup and recovery duties to a data custodian.
- **Data Custodian (Appointed by Data Owner)**
  - Perform the information classification exercise
  - Perform backups and recovery as specified by the data owner
  - Ensure records retention is in place according to regulatory
  - requirements or organizational retention policy

DATA LIFECYCLE MANAGEMENT (DLM)

- Information Lifecycle Management (ILM)
- DLM is a policy based approach
- Defines procedures and practices, to protect data throughout the information life cycle: from the time it is created to the time it is disposed or deleted.
- Protection and Access control all at stages of data life cycle
  - Generated (i.e., created)
  - Used (i.e., processed)
  - Transmitted
  - Stored
  - Archived

USE CASE / MISUSE CASE



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.
- Master list of allowable actions and another master list of denied actions.
- Useful in creating appropriate use and misuse cases, respectively.

REQUIREMENTS TRACEABILITY MATRIX

RTMs help to :

- 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.

Questions

THANK YOU