Republic of Yemen
Ministry of Higher Education & Scientific Research
AL-Rasheed Private University
Computer Science & Information Technology

Administrative Tools Subsystem for Judicial Management System

Lab 03 :

Subsystem Name: project name

Group Names:

1. Mohammed Qasabah
2. Mazen Al-ammari
3. Mohanned Shaaf
4. Mohammed Al-howshabi

Exercise 1: Decision Matrix for SDLC Methodology

Decision Matrix

Complete the table to determine the most suitable SDLC methodology for your subsystem.

Criteria	Options	Selected Option	Rationale (Justify your choice)
Team Size	Small, Medium, Large	Small	5 members
Requirement Stability	Stable, Unstable, Mixed	Unstable	we don't know clearly the requirement of administrative tools subsystem
Project Complexity	Low, Medium, High	High	high integration needs with other subsystems and technical challenges with how to chose administrative tools and determined them
Time Sensitivity	High, Medium, Low	High	before the term end
Security Requirements	High, Medium, Low	Medium	no financal damage
Expected Changes	Frequent, Occasional, Rare	Rare	because it's for learning
Stakeholder Involvement	High, Medium, Low	Low	there is no stakeholders
Project Size	Small, Medium, Large	Small	Limited scope and no budget, with short duration. and an experienced team.
Risk Tolerance	High, Medium, Low	Low	Risk-averse, with a focus on stability and predictability.
Project Duration	Short (<6 months), Medium (6–12 months), Long (>12 months)	Short	<3 months
Flexibility	High, Medium, Low	Medium	some things may change
Deliverables	Iterative, Final Deliverable, Mixed	Mixed	we deliver some documents in the semester and we have the final presentation
Customer Feedback	Frequent, Occasional, Rare	Frequent	the doctor help us every time

Based on the table above, what is the suitable Methodology for your Project?

The Agile methodology is the most suitable approach for our project due to several key factors. With a small team of 5 members, Agile promotes collaboration and communication. The unstable requirements and high project complexity benefit from Agile's flexibility and iterative development. Given the high time sensitivity and short duration (<3 months), Agile enables faster delivery of functional components. Medium security requirements and low stakeholder involvement align well with Agile's focus on team collaboration. Additionally, the project's medium flexibility and mixed deliverables can be effectively managed through Agile iterations, while frequent feedback from the instructor supports continuous improvement. Overall, Agile allows for adaptation to changing requirements while delivering valuable increments.

Helping Notes for Exercise 1

Team Size

- **Small:** 1–5 members. Suitable for tightly focused teams or projects with low complexity.
- **Medium:** 6–15 members. Allows for more specialization but requires better communication.
- **Large:** >15 members. Suitable for large-scale projects, but coordination challenges may arise.

Requirement Stability

- **Stable:** Requirements are clearly defined and unlikely to change during the project.
- **Unstable:** Requirements are evolving or unclear at the start.
- **Mixed:** Some requirements are fixed, while others may change.

Project Complexity

- **Low:** Straightforward tasks with minimal technical or business challenges.
- **Medium:** Moderate complexity, with some technical challenges or integration needs.
- **High:** Complex tasks with high integration needs, technical challenges, or regulatory constraints.

Time Sensitivity

- **High:** Strict deadlines with little room for delay.
- **Medium:** Some flexibility in timelines.
- **Low:** Deadlines are flexible, with an emphasis on quality.

Security Requirements

- **High:** Critical systems where security breaches can have significant consequences.
- **Medium:** Security is important but not the topmost priority.
- **Low:** Minimal security needs.

Expected Changes

- **Frequent:** Regularly changing requirements.
- **Occasional:** Minor changes anticipated.
- **Rare:** Requirements are unlikely to change after the initial phase.

Stakeholder Involvement

- **High:** Stakeholders are actively engaged throughout the project.
- **Medium:** Stakeholders provide input during key phases.
- **Low:** Minimal stakeholder involvement during the project lifecycle.

Project Size

- **Small:** Limited scope and budget, with short duration.
- **Medium:** Moderate scope, budget, and timeline.
- **Large:** Broad scope, significant budget, and extended timeline.

Risk Tolerance

- **High:** Willing to take risks for innovation or speed.
- **Medium:** Balanced approach between risk and caution.
- **Low:** Risk-averse, with a focus on stability and predictability.

Project Duration

- **Short:** Less than 6 months.
- **Medium:** Between 6–12 months.
- **Long:** Over 12 months.

Flexibility

- **High:** Can easily adapt to changes in requirements or scope.
- **Medium:** Some flexibility in adapting to changes.
- **Low:** Fixed plan with little room for changes.

Deliverables

- **Iterative:** Deliverables are provided incrementally over time.
- **Final Deliverable:** One complete deliverable at the end of the project.
- **Mixed:** Combines both iterative and final deliverable approaches.

Customer Feedback

- **Frequent:** Continuous feedback loop with the customer.
- **Occasional:** Feedback is collected at specific stages.
- **Rare:** Feedback is gathered only at the end.

Exercise 2: Apply Secure SDLC Practices

Scenario:

As part of the **Document Management** subsystem, the system must allow users to upload, review, and store sensitive legal documents securely. The documents will include case files, evidence, and personal information. The system must also support e-signatures and document verification. Security is a critical requirement to protect the confidentiality and integrity of the data.

Instructions:

1. **Select a Secure SDLC practice** (such as Threat Modeling, Risk Assessment, misuse cases, Secure Design Principles, Secure Code Review, Security Testing, etc.) for each phase of the SDLC (Requirements, Design, Development, Testing, Deployment) for the **Document Management** subsystem.
2. Fill in the table below with the secure SDLC practices you would apply at each stage.

SDLC Phase	Secure SDLC Practice	Description
Requirements	Risk Assessment	Identify and analyze potential risks associated with sensitive legal documents to define security requirements.
Design	Secure Design Principles	Apply principles such as least privilege, fail-safe defaults, and separation of duties to ensure that sensitive documents are adequately protected during design.
Development	Secure Code Review	Conduct reviews of the code to identify vulnerabilities, ensuring that secure coding practices are followed, especially for document upload and storage functions.
Testing	Security Testing	Perform penetration testing and vulnerability assessments on the Document Management subsystem to identify and mitigate security flaws before deployment.
Deployment	Continuous Monitoring	Implement monitoring tools to track access and changes to sensitive documents, ensuring any

		suspicious activities are detected and addressed promptly.

Exercise 3: Determine the User Types for the Subsystem

Description:

Every subsystem in JMS serves a specific set of users. Identify the user types and their roles for your subsystem.

Exercise:

- Brainstorm to list potential users for the subsystem (e.g., litigants, lawyers, judges, admin staff).
- Describe the main actions each user can perform within your subsystem.

Deliverable:

A user classification table with details on roles, and responsibilities. Example to help you understand the deliverable table.

User Type / Role	Arabic Meaning	Responsibilities
Judge	قاضٍ	Review case details, schedule hearings, issue judgments.
Lawyer	محامي	Submit case documents, communicate with clients, present arguments in court.
Litigant	متقاضي	File cases, track case progress, access court decisions.
Case Manager	مدير القضايا	Assign cases, monitor case updates, schedule hearings.

User Type / Role	Arabic Meaning	Responsibilities
Administrative Officer	موظف إداري	- **User Roles**: Define and manage user roles (e.g., admin, user, guest) and permissions. - **Staff Data**: Maintain staff records, including personal information, roles, and performance history. - **System Configurations**: Configure system settings related to user access and notifications.
IT Specialist	متخصص تكنولوجيا المعلومات	- **User Roles**: Create and modify user accounts and assign roles based on job functions. - **Staff Data**: Ensure the integrity and security of staff data, implementing data protection measures. - **System Configurations**: Manage system infrastructure settings, including network configurations and security protocols.

Court Manager	مدير المحكمة	- **User Roles**: Assign specific roles to court staff, such as judges, clerks, and bailiffs. - **Staff Data**: Oversee and update records related to court personnel and their qualifications. - **System Configurations**: Adjust court management system settings for case management processes and reporting requirements.

Helping Notes for Exercise 3

Group 1: Case Management

Identify roles like **Judges**, **Lawyers**, **Case Managers**, and **Clerks**.

Focus on their responsibilities related to filing, tracking, and managing cases.

Group 2: Document Management

Include roles like **Judges**, **Lawyers**, **Evidence Custodians**, and **Litigants**.

Highlight responsibilities for uploading, reviewing, storing, and verifying documents.

Group 3: Courtroom Scheduling

List roles like **Presiding Judges**, **Clerks**, and **Case Managers**.

Detail their tasks in dynamic assignment of judges, rooms, and scheduling hearings.

Group 4: Litigant Portal

Identify users such as **Litigants**, **Public Relations Officers**, and **Support Staff**.

Describe their roles in accessing case status, filing complaints, and viewing decisions.

Group 5: Lawyer Portal

Include roles like **Lawyers**, **Clerks**, and **Case Managers**.

Document their responsibilities for managing cases, submitting documents, and client communication.

Group 6: Judges' Dashboard

Focus on **Judges** and **Case Managers**.

Describe their roles in accessing schedules, case details, and managing workflows.

Group 7: Administrative Tools

Include **Administrative Officers**, **IT Specialists**, and **Court Managers**.
Define tasks related to managing staff, roles, and performance metrics.

Group 8: Reporting and Analytics

List roles like **Judges**, **Administrative Officers**, and **Analysts**.
Detail responsibilities for generating reports and monitoring performance indicators.

Group 9: Search and Retrieval

Identify **Lawyers**, **Judges**, and **Clerks**.
Explain their responsibilities for searching and retrieving case-related information.

Group 10: External System Integration

Include roles like **Police Officers**, **Prosecutors**, and **IT Specialists**.
Document their tasks in integrating external systems and maintaining data flow.

Group 11: Security and Role Management

Focus on **IT Specialists**, **Security Officers**, and **Court Managers**.
Highlight responsibilities for managing access controls and securing data.

Group 12: Local Data Center

Include **Data Center Administrators** and **IT Specialists**.
Define roles related to data storage, backups, and ensuring data sovereignty.

Group 13: Prosecutor's Office Integration

List roles like **Prosecutors**, **Police Officers**, and **Clerks**.
Highlight tasks for managing cases, evidence, and court interactions.

Group 14: Police Department Integration

Include **Police Officers**, **Prosecutors**, and **Judges**.
Define responsibilities for submitting case reports, updating investigations, and evidence sharing.

Table 1. Responsibility Example for each subsystem

Group	Subsystem	Responsibility Examples
Group 1	Case Management	Case Details, Case Status, Deadlines
Group 2	Document Management	Uploaded Documents, Verified Documents, Signed Docs
Group 3	Courtroom Scheduling	Hearing Slots, Courtroom Allocation
Group 4	Litigant Portal	Case Statuses, Complaints, Court Decisions
Group 5	Lawyer Portal	Case Files, Client Communications, Evidence Submitted
Group 6	Judges' Dashboard	Case Details, Schedules, Performance Metrics
Group 7	Administrative Tools	User Roles, Staff Data, System Configurations
Group 8	Reporting and Analytics	Case Statistics, Workload Reports, Dashboards
Group 9	Search and Retrieval	Case Records, Archived Files, Judgments
Group 10	External System Integration	Case Reports, Investigation Updates, Evidence

Exercise 4: Subject-Object Matrix

Objective: The **Subject-Object Matrix** maps user roles (subjects) to system resources (objects) to define access control and security for the system.

Instructions:

1. **List Subjects (User Roles):**
   - Identify and list all the user roles (subjects) in the system (e.g., judges, lawyers, litigants, administrators).
2. **List Objects (System Resources):**
   - Identify and list the key system resources or objects (e.g., case details, documents, schedules, court decisions).
3. **Define Access Control:**
   - For each subject-object pair, define the level of access that the user has (e.g., **Read**, **Write**, **Delete**, **Execute**).

Outcome: You will have a matrix showing which roles have access to which system resources and the type of access they have.

Subject/Object Matrix Example

Subject (User Role)	Case Details	Uploaded Documents	Schedules	Court Decisions	Hearing Slots
Judge	Read, Update	Read	Read	Read	Read, Execute
Lawyer	Read	Read, Write	No Access	Read	No Access
Litigant	Read	No Access	No Access	Read	No Access
Clerk	Read, Update	Read, Write	Update	No Access	Update
Case Manager	Read	No Access	Update	No Access	Update

Subject (User Role)	User Accounts	Staff Data	System Configurations	Case Management System	Performance Metrics Reports
Administrative Officer	Read, Write	Read, Write	Read	Read	Read
IT Specialist	Read, Write, Delete	Read, Write	Read, Write, Execute	Read, Write, Execute	Read
Court Manager	Read	Read	Read	Read, Write	Read, Write

Exercise5: Misuse Case and Use Case Modeling

Objective: Misuse cases and use case modeling help identify the system's functional requirements and potential security risks or misuse scenarios.

Instructions:

1. **Create Use Case Diagrams:**
   - Identify key use cases for the system (e.g., case filing, document upload)
   - For each use case, define the steps involved and the user types who interact with the system.
2. **Create Misuse Case Diagrams:**
   - For each use case, identify potential misuse scenarios (e.g., tampering with documents).
   - Define who the potential attacker is and the possible attack methods.

Outcome: You will have a complete set of use case and misuse case diagrams that highlight both functional and security requirements for the system.

Example:

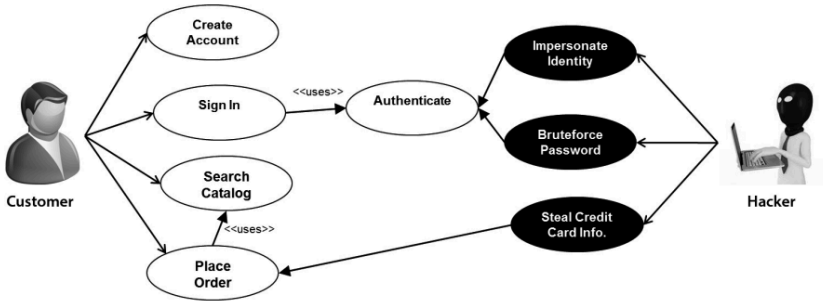

Figure 2.13 – **Example of an Online eCommerce Store Use case and Misuse case**