Mid Term CSC-580 Winter 2025

Name: Ehtasham Nasir, James Kessler, Philip Haapala, and John Tempey

Q1:Scope Perspective (Planner's View)

What Context (Data)	1. File types (e.g., text files, spreadsheets, presentations, and multimedia files).
	2. Metadata for searching and categorization (e.g., document title, author, data created/modified, department/category, and confidentiality level)
	3. Version and Revision data (e.g., log of changes and restore previous versions)
	4. Security & access control information (e.g., tracks who has access to which documents, encryption status, and audit logs)
	5. Workflow & approval data (e.g., responsible party to approve the document, approval status, and comments/feedback)
	6. Integration data (e.g., emails or messages, potential external system connections, and other collaboration tools).
	7. User data (e.g., user profile and role/position in organization hierarchy)
How Context (Function)	1. The system will ingest documents, spreadsheets, presentations, and multimedia files created by the user into the centralized repository.
	2. The system will give users the ability to review, approve, and distribute documents
	3. Documents will have tags.
	4. When a document is edited, a new version is saved.
	5. The system will restrict access based on job roles.
	6. Users will be able to share encrypted documents.
	7. The system will allow for comments, feedback, and real-time co-authoring.
	8. Users will need to authenticate using passwords, multi-factor logic and so forth to access the system.
Where Context (Location)	1. The EDMS will be hosted either on-premise servers or on a private cloud. A hybrid approach is also another consideration.
	2. Primary data stored in corporate data centers.
	3. Backup copies stored in geographically separate locations.
Who Context (Users/ Stakesholders)	1. Employees
	2. Managers & leads
	3. IT administrators
	4. Compliance officers
	5. Security officers
	6. External stakeholders (e.g., vendors, clients, contractors)

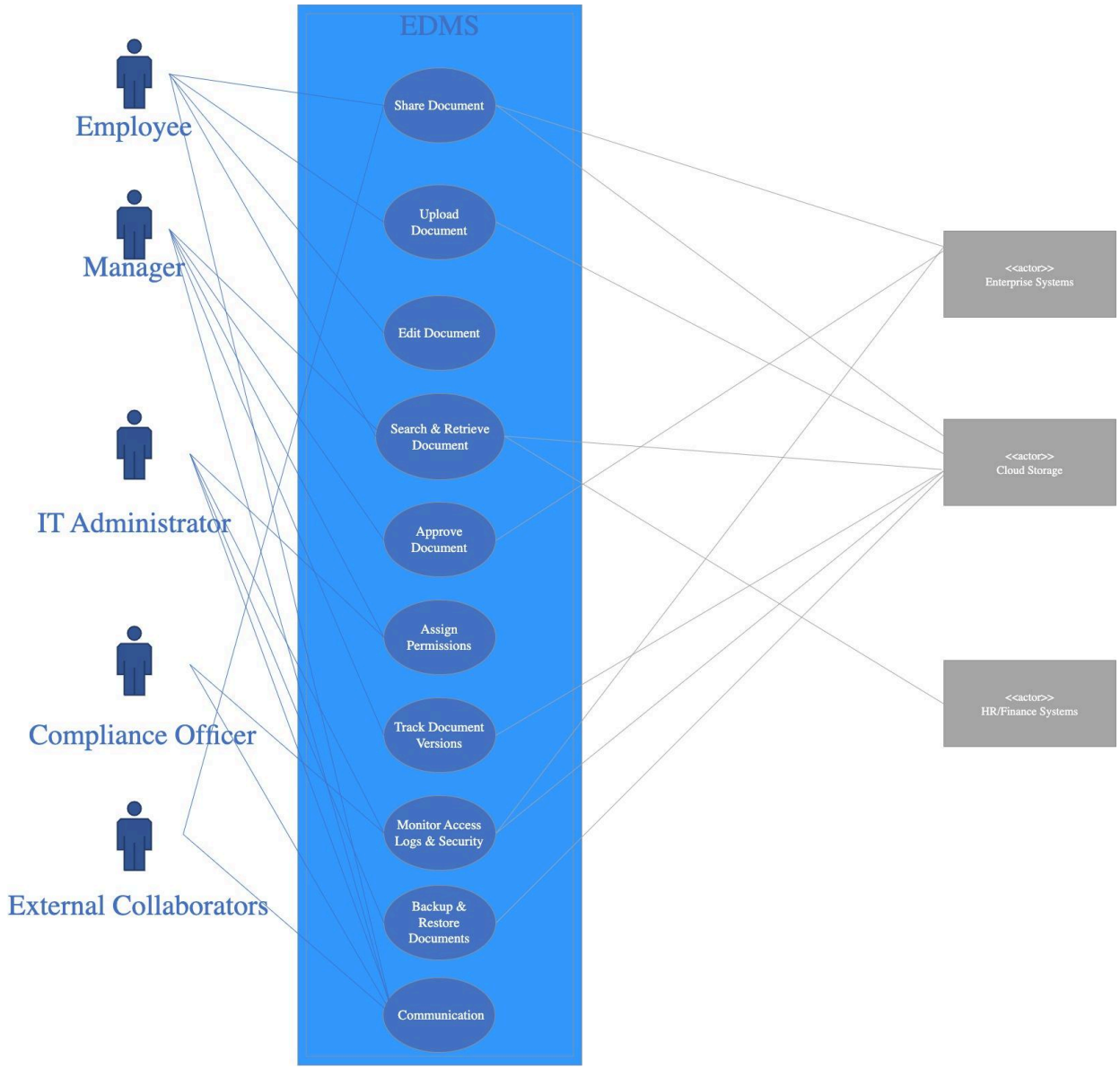
What Context (Data)	1. File types (e.g., text files, spreadsheets, presentations, and multimedia files).
	2. Metadata for searching and categorization (e.g., document title, author, data created/modified, department/category, and confidentiality level)
	3. Version and Revision data (e.g., log of changes and restore previous versions)
	4. Security & access control information (e.g., tracks who has access to which documents, encryption status, and audit logs)
	5. Workflow & approval data (e.g., responsible party to approve the document, approval status, and comments/feedback)
	6. Integration data (e.g., emails or messages, potential external system connections, and other collaboration tools).
	7. User data (e.g., user profile and role/position in organization hierarchy)
	7. Executives and other senior members

When Context (Time)	1. Users are able to upload, edit, and retrieve documents on-demand
	2. Changes to the documents are available immediately to authorized users.
	3. When a document is updated, a new version is saved automatically.
	4. Revision history can be viewed at anytime.
	5. There is a predefined schedule for approval workflows.
	6. If approvals are overdue, a notification or reminder is sent.
	7. The security team reviews logs at a predetermined time interval.
	8. When an event happens, such as accessing, downloading, or modifying, the system logs it.
	9. Backups are performed regularly (e.g., daily, weekly, or real-time).
	10. The company policy dictates when a file is archived or deleted automatically.
	11. The IT team schedules system maintenance.

Why Context (Motivations)	1. To better enhance document accessibility and organization.
	2. To improve internal (and external) collaboration and workflow efficiency.
	3. To increase security and ensure compliance.
	4. To further reduce operational costs and paper waste.
	5. To ensure version control and audit ready compliance.
	6. To support employees across the organization either at different locations or remote.
	7. To reduce risk and increase regulatory compliance.

Q2: Use Cases

Use Case Diagram



Narrative Use Cases

Employee Use Cases

Use Case #1: Upload Document

Primary Actor: Employee

Description of Usage:

1. In the EDMS, the employee selects the “Upload Document” option.
2. The system then prompts the employee to select a file.
3. The employee chooses a file and, if desired, adds metadata.
4. The system validates the file and metadata
5. The employee selects “Confirm Upload”
6. The system uploads file, creates version history, displays “Upload Successful”, and provides link

Use Case #2: Share Document

Primary Actor: Employee

Description of Usage:

1. The employee selects “Share Document.”
2. The system prompts for a recipient (internal or external)
3. The employee sets permissions.
4. The system then sends out a notification by way of the enterprise system.
5. The user clicks the link and accesses the document.

Manager Use Cases

Use Case #1: Approve Document

Primary Actor: Manager

Description of Usage:

1. Manager logs into EDMS and clicks on “Pending Approvals.”
2. The system displays the documents with “pending approval” status
3. Manager selects the document to approve.
4. The system opens the document.
5. Manager reviews the document then selects either “Approve” or “Request Changes.”
6. The system changes the document status and sends a notification to the uploader.
7. Once approved, the document moves to storage. If rejected, the item goes back for further revisions.

Use Case #2: Assign Permissions

Primary Actor: Manager

Description of Usage:

1. In the EDMS, the manager selects the “Manage Permissions” option.
2. The system then displays the current access settings.
3. The manager either adds or removes users and/or sets access level to view, edit, or download.
4. The system applies all changes and then logs them for security tracking.
5. The user receives a notification indicating changes.

IT Administrator Use Cases

Use Case #1: Backup and restore documents

Primary Actor: IT Administrator

Description of usage:

1. In the admin dashboard, the IT Admin selects “Backup & Restore.”
2. The system displays backup history and other display options.
3. The IT Admin then selects a prior backup version and proceeds with restoration.
4. The system pulls the document from file backup storage.
5. The prior document is displayed.

Use Case #2: Monitor Access Logs & Security

Primary Actor: IT Administrator

Description of usage:

1. In the EDMS, the IT admin opens “Security logs.”
2. The system lists user access logs.
3. The IT admin filters on user, date, or action type, and selects a log to review.
4. The system displays full log report
5. If the results are suspicious, IT Admin flags entry and follows up with the Compliance team.
6. The system logs the action and produces a security report.

Compliance Officer Use Cases

Use Case #1: Review Access Logs

Primary Actor: Compliance Officer

Description of usage:

1. In the EDMS, the compliance officer opens “Audit logs.”
2. The system pulls down the logs and displays them.
3. The compliance officer views the logs for issues.
4. The system prompts the user to select “Accept” or “Report Issue”
5. If an issue is found, the compliance officer reports to IT.
6. The IT administrator follows up and takes corrective action.

Use Case #2: Enforce Security Policies

Primary Actor: Compliance Officer

Description of usage:

1. In the EDMS, the compliance officer navigates to “Manage Security Policies.”
2. The system then displays policy settings.
3. The compliance officer makes the appropriate changes and saves.
4. The system notifies all relevant users and logs changes.
5. The IT administrator then reviews changes and confirms enforcement.

External Collaborator Use Cases

Use Case #1: Upload Document

Primary Actor: External Collaborator

Description of usage:

1. The system prompts the external user to log into the secure portal.
2. The external user navigates to “Upload document”
3. The system prompts the user to select a file, and any metadata, for upload
4. The external user selects the file from their device.
5. The system runs validation tests, and if passed uploads the file and sends a notification to the external user.

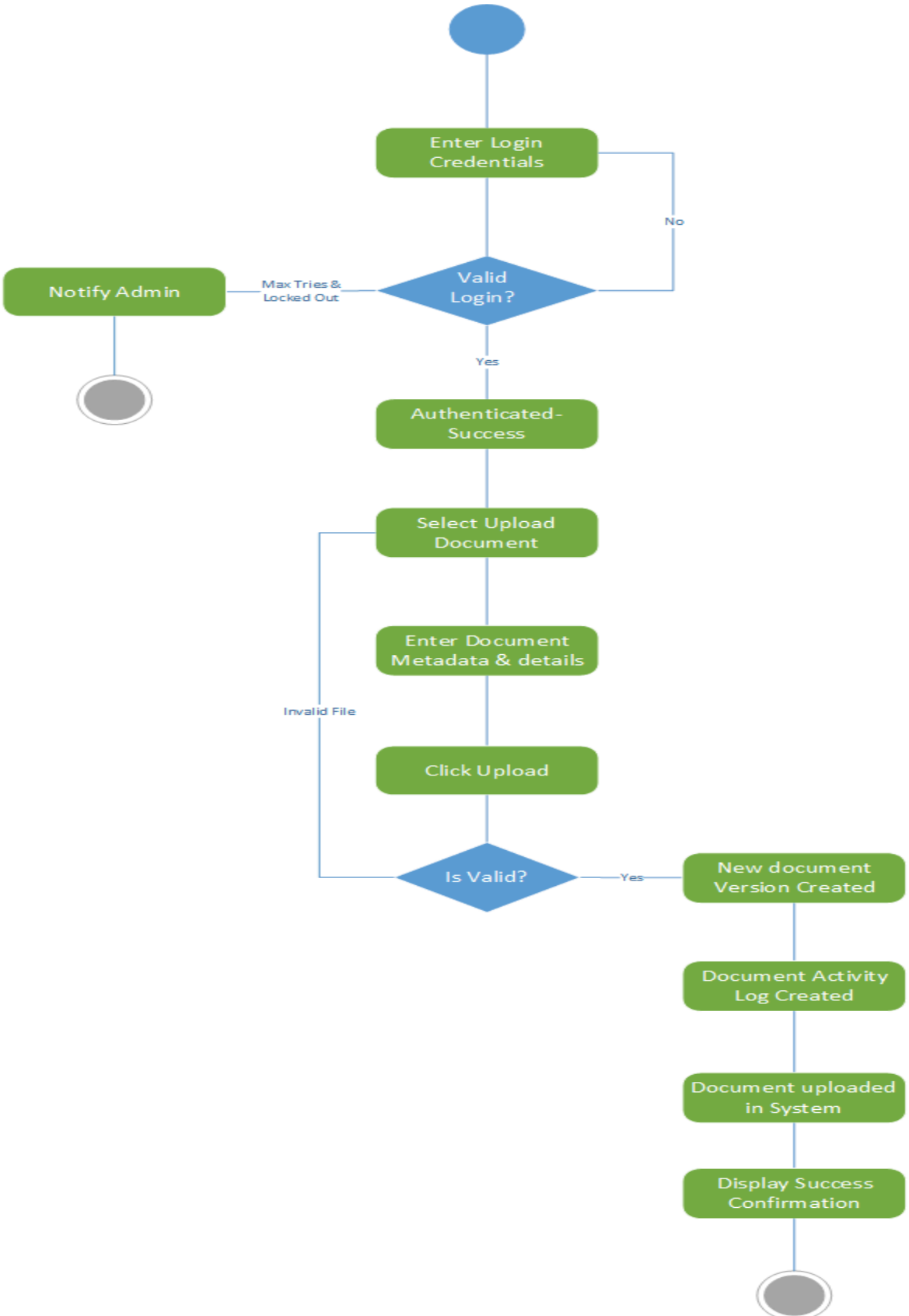
Use Case #2: Share Document with Internal Team

Primary Actor: External Collaborator

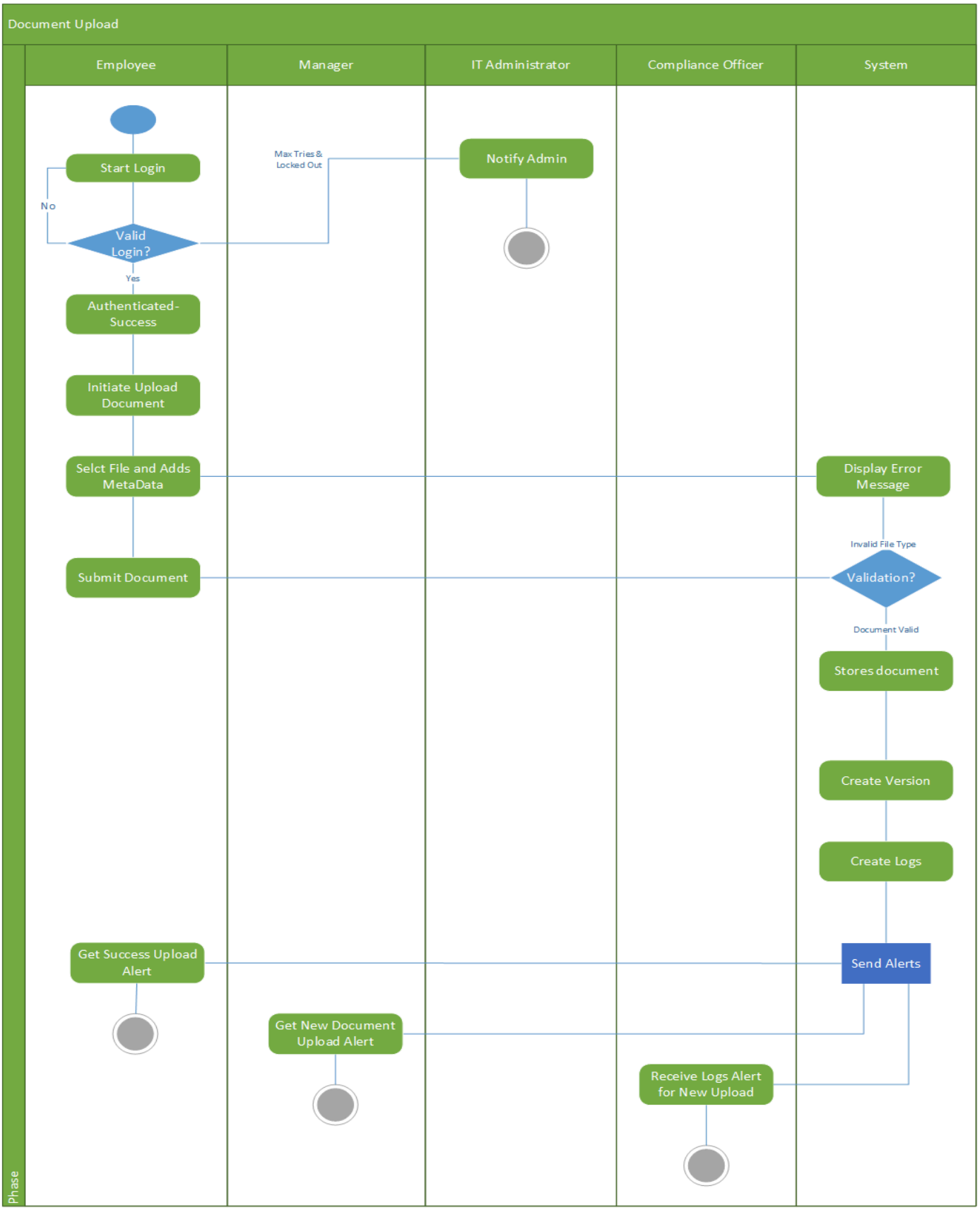
Description of usage:

1. In the EDMS, the external user selects “Share document.”
2. Before sending the document, the system prompts the user to select the recipient.
3. The external user sets access permissions.
4. Through the Enterprise system, the system sends out notification.
5. The internal employee is granted access.

Q3: Activity Diagram Document Upload



SwimLane Diagram For Document Upload



Q:4 (a) Candidate Classes

Actor Classes:

1. User (super class for actors)
2. Employee
3. Manager
4. IT Administrator
5. Compliance Officer
6. External Collaborator

Business Classes:

1. Organization Hierarchy
2. Centralized Repository
3. File
4. Metadata
5. File Templates
6. Access Control
7. Workflow Manager
8. Security

Interface Classes:

1. Authentication
2. Share
3. Upload
4. Edit
5. Comment
6. Search & Retrieve
7. Version Control (View and/or Restore)
8. DocumentStatus
9. UserRights
10. Notifications
11. Communication (Email, SMS, and Video Conferencing)

Report Classes:

1. Security Log (who accessed a file, how, and when; audit logs; data backups)

Q:4 (b) CRC Cards

User (Base Class)	**Collaborations**
Knows: K1) User_ID K2) Role K3) username K4) FullName K5) Password K6) UserRights	access_control users
Does: D1) Login() D2) Logout() D3) ResetPassword() D4) AccessRights()	Authentication()

Employee	**Collaborations**
Knows: K1) employee_ID K2) employee_role K3) employee_file_permissions K4) employee_group_access_level K5) User_Id K6) manager_id	user organization_hierarchy centralized_repository metadata access_control manager
Does: D1) SearchForFile() D2) UploadFile() D3) CreateDocument() D4) EditFile() D5) ShareFile() D6) DeleteFile()	User() File() CentralizedRepository() VersionControl() Notifications() WorkflowManager()

File (Super Class)	**Collaborations**
Knows: K1) file_name K2) file_category K3) file_contents K4) file_creator K5) file_editors	user access_control metadata organization_hierarchy centralized_repository

K6) file_readers K7) file_history K8) file_access_level K9) file_location	version_history encryption workflow_manager
Does: D1) FormatBlankFile() D2) FormatTemplate() D3) Save() D4) Validate() D5) Export() D6) Import() D7) Delete() D8) Share()	VersionControl() User() AccessControl() FileTemplates() CentralizedRepository() WorkflowManager() Communication()

Version Control	**Collaborations**
Knows: K1) current_file_version K2) file_version_history (list of dictionaries) K4) file_name K5) file_id K6) user_id K7) date K8) file_location	user file centralized_repository backup_log
Does: D1) DisplayVersionHistory() D2) RevertToPreviousVersion() D3) CompareToPreviousVersion() D4) UpdateVersionHistory() D5) MergeFiles() D6) ShowChangeSincePrevLogin()	User() File() CentralizedRepository() AccessControl() SecurityLog()

Manager	**Collaborations**
Knows: K1) manager_ID K2) manager_department	organization_hierarchy user file communication workflow_manager employee
Does: D1) ReviewFile() D2) ApproveFile() D3) RejectFile()	User() File() Employee() CentralizedRepository()

D4) AddEmployeeToGroup() D5) ShareFile() D6) CreateMeeting() D7) CreateFile() D8) DeleteFile() D9) ManageWorkflow() D10) SendMeetingInvites()	Communication() WorkflowManager() OrganizationHierarchy() AccessControl() VersionControl() Notifications()

IT Administrator	**Collaborations**
Knows: K1) administrator_id K2) encryption_keys K3) architecture_configuration K4) cloud_credentials	User() organization_hierarchy security_logs centralized_repository access_control security
Does: D1) ManageAccessRights() D2) ManageRepository() D3) ManageEmployeePermissions() D4) ViewServerLogs() D5) BackupData() D6) RestoreData()	OrganizationHierarchy() CentralizedRepository() AccessControl() SecurityLogs()

Compliance Officer	**Collaborations**
Knows: K1) compliance_officer_id K2) security_protocol K3) backup_schedule	user security_logs backup_logs
Does: D1) ViewSystemAccessLogs() D2) ViewServerLogs() D3) ViewAudit() D4) ReportSuspiciousActivity()	SecurityLogs() AccessControl()

External Collaborator	**Collaborations**
Knows: K1) external_id K2) user_id K3) external_file_permissions K4) external_group_access_level	user access_level organization_hierarchy centralized_repository

Does: D1) SearchForFile() D2) UploadFile() D3) EditFile() D4) ShareFile() D5) RequestAccess()	File() CentralizedRepository() VersionControl() AccessControl()

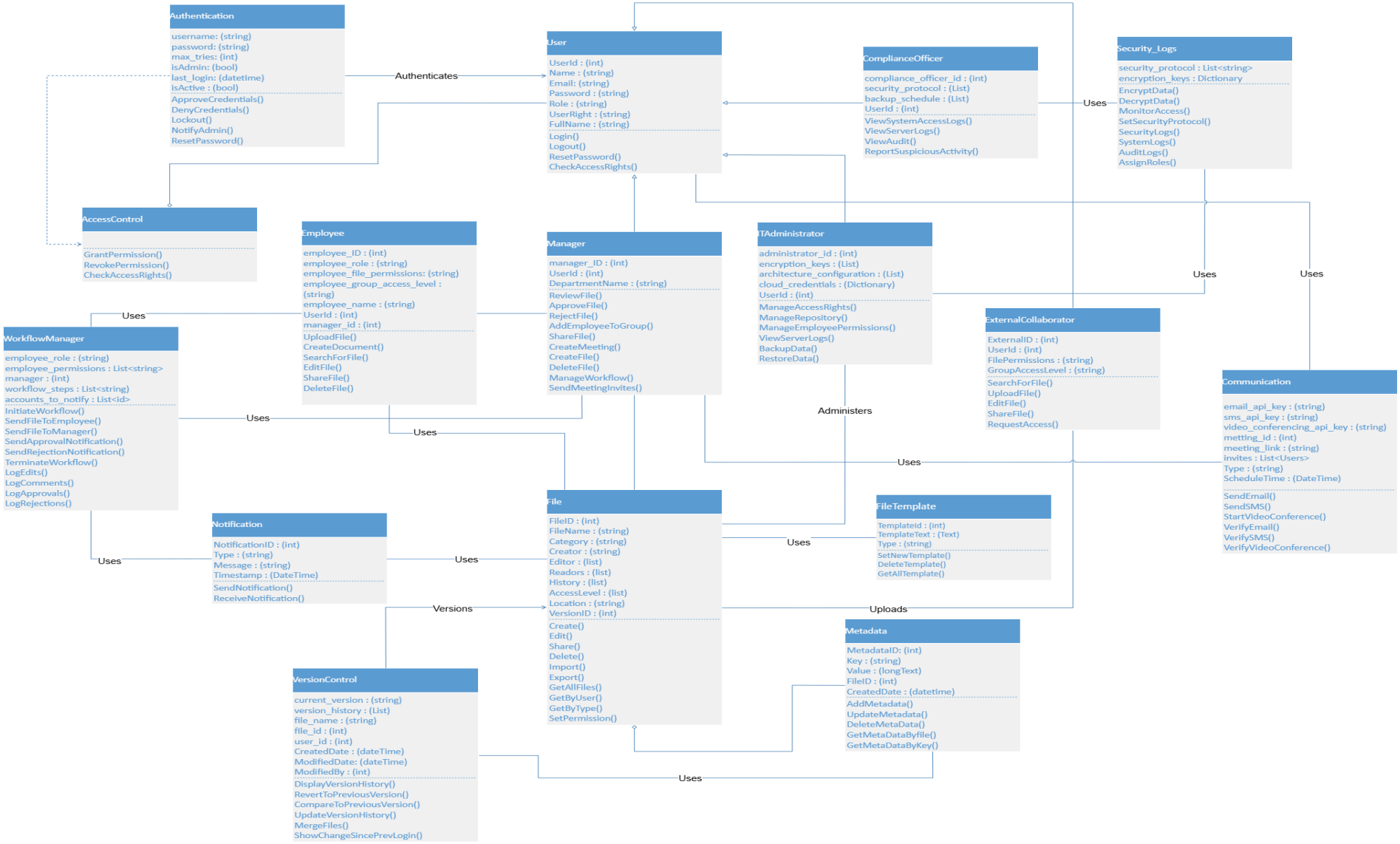
Authentication	**Collaborations**
Knows: K1) username K2) password K3) max_tries K4) admin K5) last_login	users it_administrator
Does: D1) ApproveCredentials() D2) DenyCredentials() D3) Lockout() D4) NotifyAdmin() D5) ResetPassword()	User() SecurityLogs() Notifications()

Communication	**Collaborations**
Knows: K1) email_api_key K2) sms_api_key K3) video_conferencing_api_key	user organization_hierarchy
Does: D1) SendEmail() D2) SendSMS() D3) StartVideoConference() D4) VerifyEmail() D5) VerifySMS() D6) VerifyVideoConference()	User() Security()

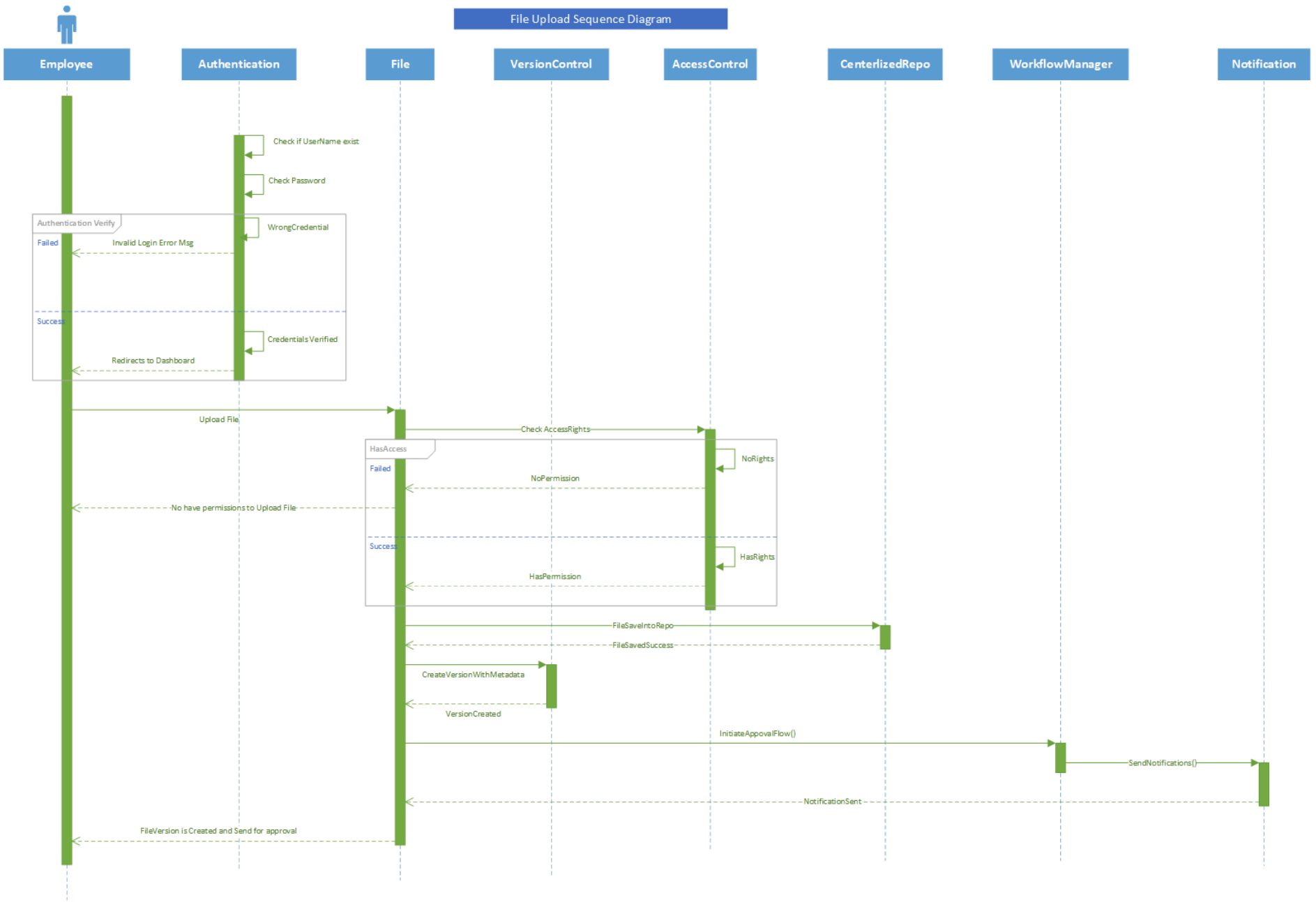
Workflow Manager	**Collaborations**
Knows: K1) employee_role K2) employee_permissions K3) manager K4) workflow_steps	employee manager organization_hierarchy access_control

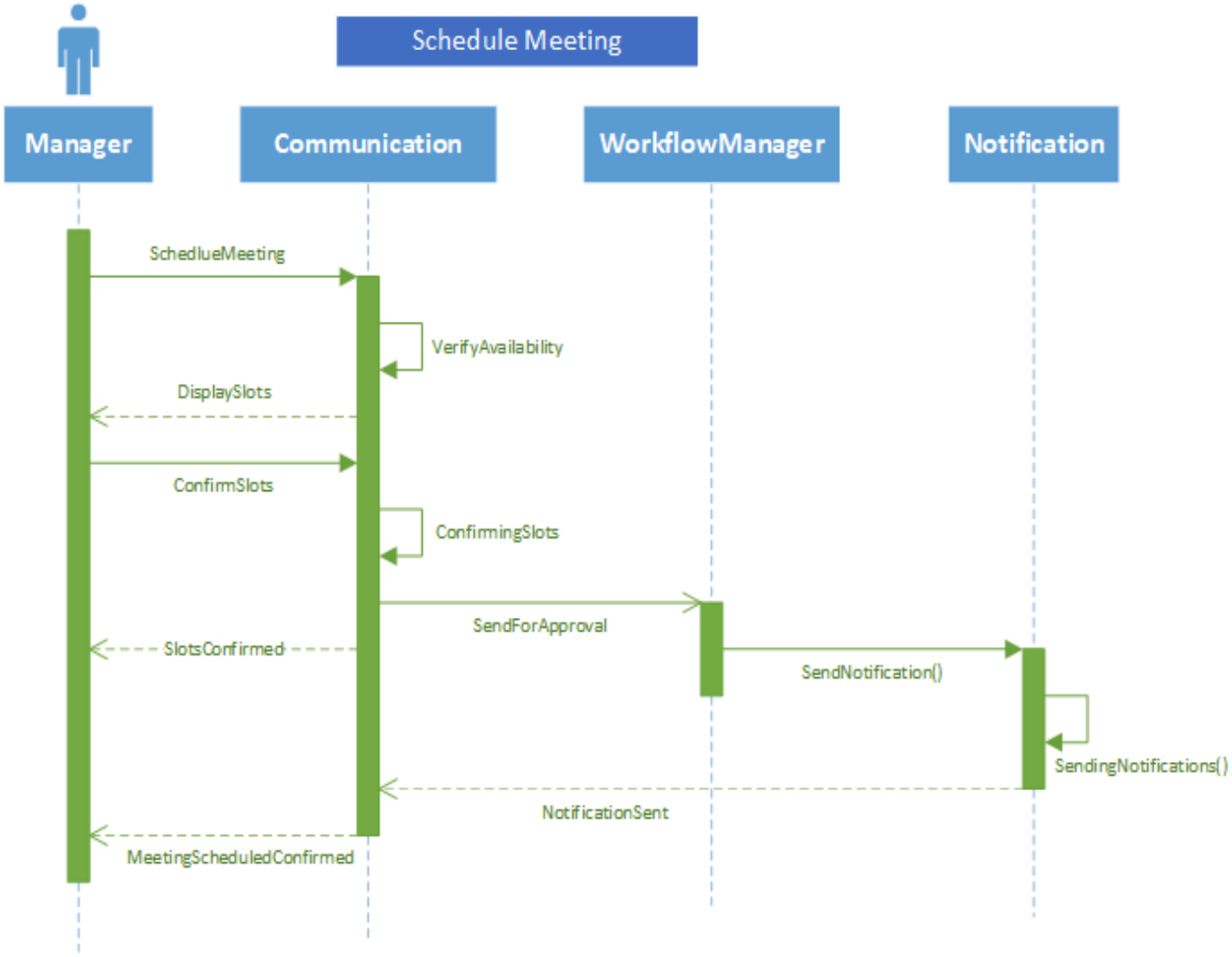
K5) accounts_to_notify	notifications
Does: D1) InitiateWorkflow() D2) SendFileToEmployee() D3) SendFileToManager() D4) SendNotificationToEmployee() D5) SendNotificationToManager() D6) TerminateWorkflow() D7) LogEdits() D8) LogComments() D9) LogApprovals() D10) LogRejections()	Employee() Manager() OrganizationHierarchy() AccessControl() Notifications() SecurityLogs()

Q:5 Class Diagram



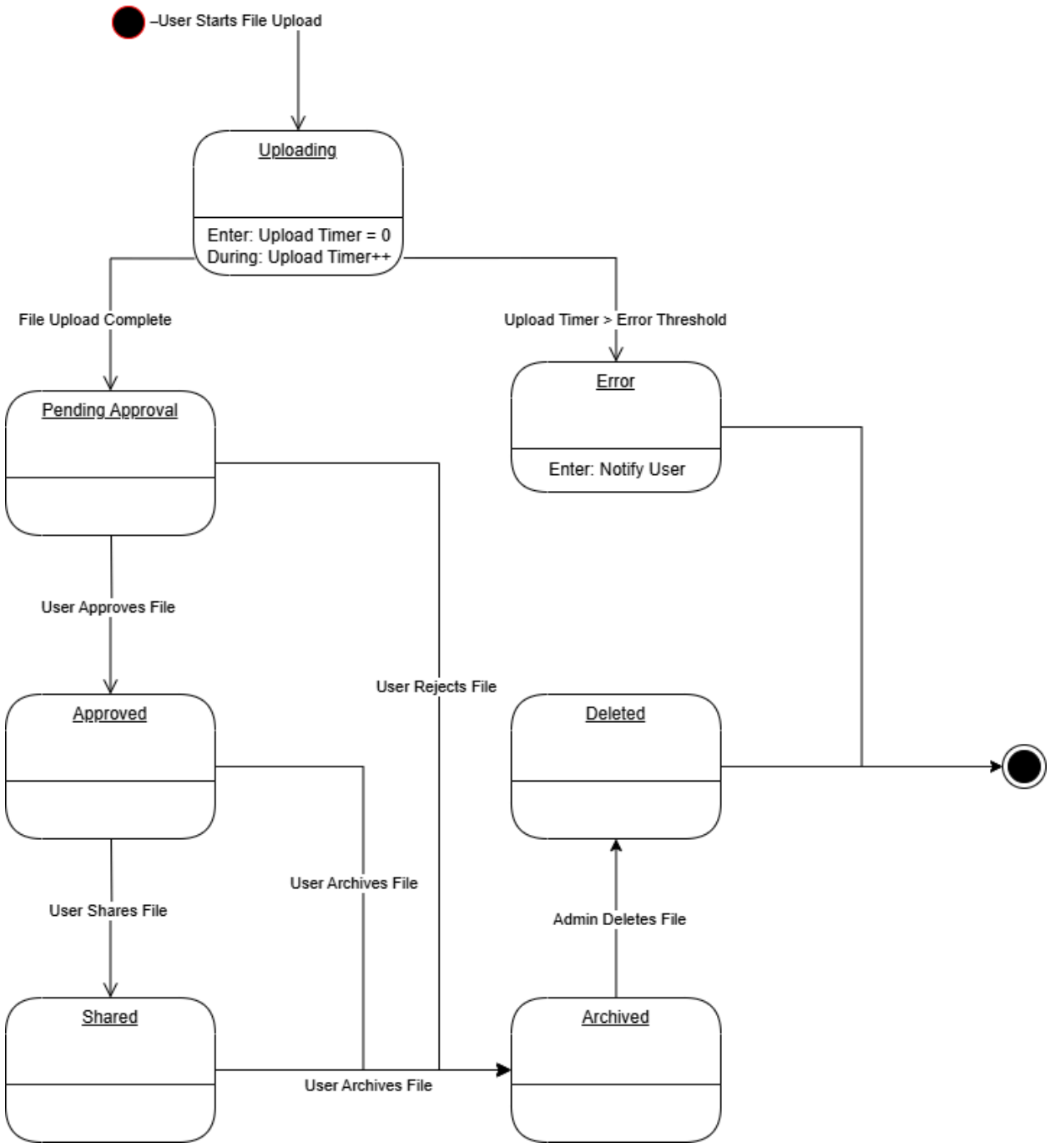
Q:6 (a) Sequence Diagram (File Upload)



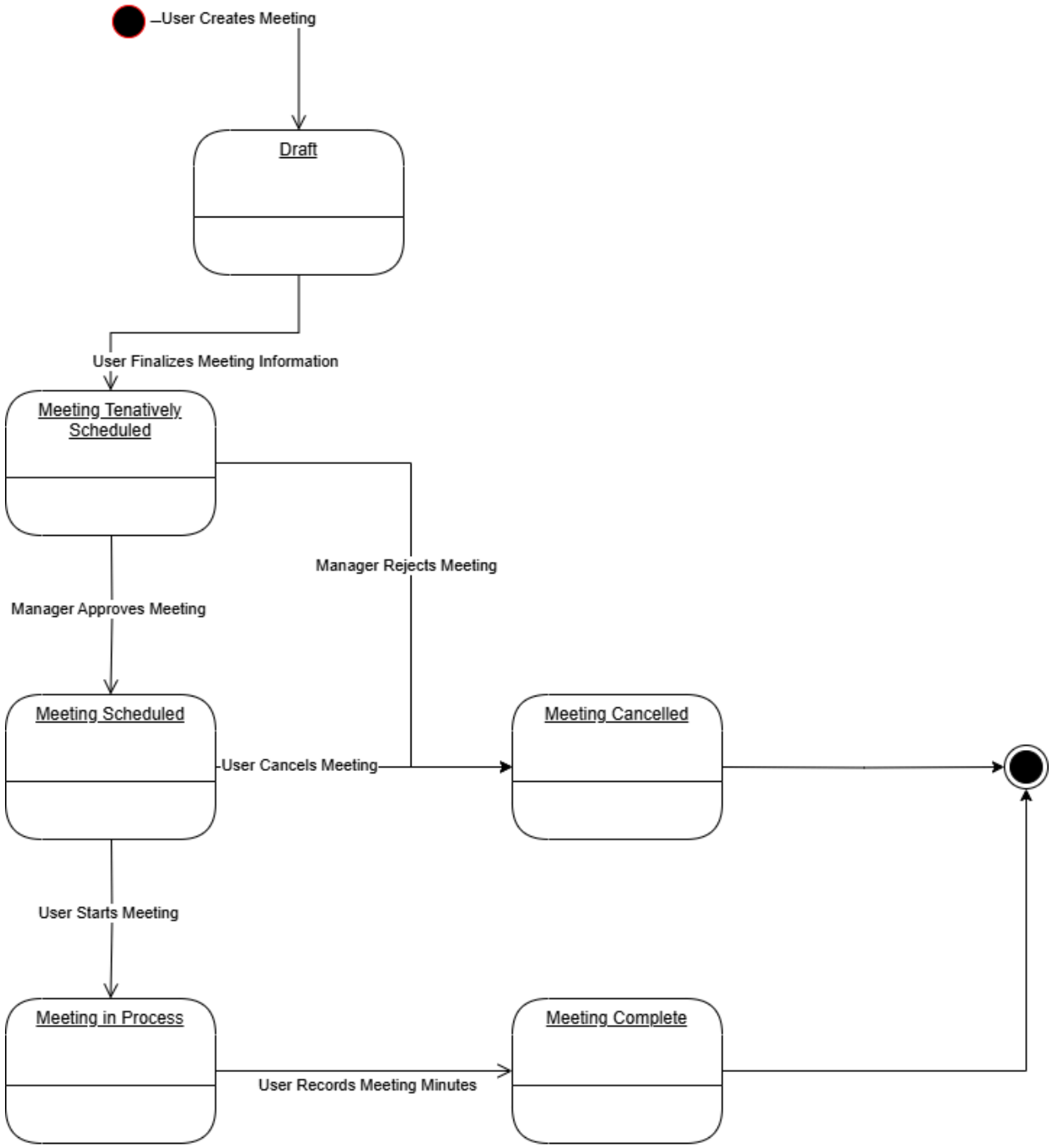

Schedule Meeting
Manager
Communication
WorkflowManager
Notification
SchedlueMeeting
VerifyAvailability
DisplaySlots
ConfirmSlots
ConfirmingSlots
SendForApproval
SlotsConfirmed
SendNotification()
SendingNotifications()
NotificationSent
MeetingScheduledConfirmed

Q:6 (b) State Diagram

File Process



Meeting Process



Question 1 and 2 were answered by Philip and Ehtasham independently then brought together by the team. Question 3 was answered by Ehtasham and reviewed by the team. James answered question 4 and the team reviewed it. Philip helped draft the response to 4. John and Ehtasham created the diagrams for question 5 based on the work from the rest of the team in the preceding questions. John completed question 6 and reviewed with the team.