项目文档

# Functional Requirement

1. Functional Requirements  
  
1.1 Email Creation Function   
 Function ID: FR-01   
 Description: The system allows the Administrator to create a new email by entering the subject, body, and selecting recipients from the Email Contact Distribution Group.   
 Input: Email subject, email body, recipient list (individual contacts or distribution groups).   
 Output: A new Email object with associated metadata stored in the system and archived in the Email Archive.  
  
1.2 Email Sending Function   
 Function ID: FR-02   
 Description: The system sends the created email to the selected recipients using the associated Email Account.   
 Input: Email content, recipient list, and the associated Email Account.   
 Output: The email is successfully delivered to the recipients, and a copy is archived in the Email Archive.  
  
1.3 Email Receiving Function   
 Function ID: FR-03   
 Description: The system detects and retrieves incoming emails to the associated Email Account and stores them in the system.   
 Input: Incoming email data from the Email Account.   
 Output: A new Email object with sender and metadata stored in the system and archived in the Email Archive.  
  
1.4 Email Viewing Function   
 Function ID: FR-04   
 Description: The system allows the Administrator to view the content and metadata of an existing email.   
 Input: Email ID or identifier selected from the Email Archive.   
 Output: Email content and metadata displayed in a read-only format.  
  
1.5 Email Deletion Function   
 Function ID: FR-05   
 Description: The system allows the Administrator to delete an email from the system and archive it in the Email Archive.   
 Input: Email ID or identifier selected from the system.   
 Output: The email is deleted from the system and archived in the Email Archive.  
  
1.6 Email Archiving Function   
 Function ID: FR-06   
 Description: The system allows the Administrator to manually archive an email to the Email Archive.   
 Input: Email ID or identifier selected from the system.   
 Output: The email is moved to the Email Archive with an associated EmailArchiveRecord.  
  
1.7 Email Recovery Function   
 Function ID: FR-07   
 Description: The system allows the Administrator to recover a previously archived email and restore it to the system.   
 Input: Email ID or identifier selected from the Email Archive.   
 Output: The email is restored to the system and associated with the relevant Email Account.  
  
1.8 Contact Creation Function   
 Function ID: FR-08   
 Description: The system allows the Administrator to create a new contact with details such as name, email address, phone number, and address.   
 Input: Contact name, email address, phone number, and address.   
 Output: A new Contact object stored in the system and associated with the Email Contact Distribution Group.  
  
1.9 Contact Update Function   
 Function ID: FR-09   
 Description: The system allows the Administrator to update an existing contact’s information.   
 Input: Contact ID, updated contact details (e.g., name, email, phone number).   
 Output: Updated Contact object stored in the system and associated with the Email Contact Distribution Group.  
  
1.10 Contact Deletion Function   
 Function ID: FR-10   
 Description: The system allows the Administrator to delete an existing contact from the Email Contact Distribution Group.   
 Input: Contact ID selected from the system.   
 Output: The contact is removed from the system and associated Email Contact Distribution Group.  
  
1.11 Contact Viewing Function   
 Function ID: FR-11   
 Description: The system allows the Administrator to view the details of an existing contact.   
 Input: Contact ID or identifier selected from the system.   
 Output: Contact details displayed in a read-only format.  
  
1.12 Distribution Group Creation Function   
 Function ID: FR-12   
 Description: The system allows the Administrator to create a new distribution group with a name, description, and associated contacts.   
 Input: Group name, description, and selected contacts.   
 Output: A new DistributionGroup object stored in the system and associated with the Email Contact Distribution Group.  
  
1.13 Distribution Group Update Function   
 Function ID: FR-13   
 Description: The system allows the Administrator to update a distribution group’s name, description, or contact list.   
 Input: Group ID, updated group name, description, and/or contact list.   
 Output: Updated DistributionGroup object stored in the system.  
  
1.14 Distribution Group Deletion Function   
 Function ID: FR-14   
 Description: The system allows the Administrator to delete an existing distribution group from the system.   
 Input: Group ID selected from the system.   
 Output: The distribution group is removed from the system and associated Email Contact Distribution Group.  
  
1.15 Add Contact to Distribution Group Function   
 Function ID: FR-15   
 Description: The system allows the Administrator to add an existing contact to a distribution group.   
 Input: Contact ID and Distribution Group ID.   
 Output: Updated DistributionGroup object with the new contact added.  
  
1.16 Remove Contact from Distribution Group Function   
 Function ID: FR-16   
 Description: The system allows the Administrator to remove a contact from a distribution group.   
 Input: Contact ID and Distribution Group ID.   
 Output: Updated DistributionGroup object with the contact removed.  
  
1.17 Email Account Management Function   
 Function ID: FR-17   
 Description: The system allows the Administrator to manage the settings of an existing email account, including username, password, domain, and signature.   
 Input: Email Account ID and updated account settings.   
 Output: Updated EmailAccount object stored in the system.  
  
1.18 Email Account Update Function   
 Function ID: FR-18   
 Description: The system allows the Administrator to update the configuration of an email account.   
 Input: Email Account ID and updated configuration data.   
 Output: Updated EmailAccount object stored in the system.  
  
1.19 Email Account Deletion Function   
 Function ID: FR-19   
 Description: The system allows the Administrator to delete an email account from the system.   
 Input: Email Account ID.   
 Output: The email account is removed from the system, and a copy is archived if needed.  
  
1.20 Email Account Permission Management Function   
 Function ID: FR-20   
 Description: The system allows the Administrator to update the access permissions of an email account, including which distribution groups or users can interact with it.   
 Input: Email Account ID and updated permission settings.   
 Output: Updated permissions for the Email Account and updated Email Contact Distribution Group.  
  
1.21 Audit Record Viewing Function   
 Function ID: FR-21   
 Description: The system allows the Administrator to view an Audit Record to track system actions (e.g., email creation, deletion, archive).   
 Input: Audit Record ID or identifier selected from the system.   
 Output: Audit Record details displayed in a read-only format.  
  
1.22 Compliance Report Generation Function   
 Function ID: FR-22   
 Description: The system allows the Administrator to generate a compliance report by retrieving relevant data from the Email Archive, Audit Record, and Email Contact Distribution Group.   
 Input: Report criteria such as date range, Email Account, or group.   
 Output: A structured compliance report displayed to the Administrator for download or printing.  
  
1.23 Email Update Function   
 Function ID: FR-23   
 Description: The system allows the Administrator to update an existing email’s content or metadata.   
 Input: Email ID, updated subject, body, or recipient list.   
 Output: Updated Email object stored in the system and archived in the Email Archive.  
  
1.24 Email Archive Management Function   
 Function ID: FR-24   
 Description: The system allows the Administrator to manage archived emails, including tagging, categorizing, or moving them to subfolders.   
 Input: EmailArchiveRecord ID and management action (e.g., tag, move, delete).   
 Output: Updated EmailArchiveRecord and Audit Record documenting the action.  
  
1.25 Email Archive Deletion Function   
 Function ID: FR-25   
 Description: The system allows the Administrator to permanently delete an email from the Email Archive.   
 Input: EmailArchiveRecord ID selected from the Email Archive.   
 Output: The email is permanently removed from the Email Archive, and an Audit Record is generated.

# External Description

2. External Interfaces  
  
2.1 User Interface Output   
The system interacts with the Administrator through a user interface to perform the following actions:   
- Display screens for creating, updating, and deleting emails, contacts, and distribution groups.   
- Display read-only views of email content and metadata, contact details, and audit records.   
- Allow the Administrator to select recipients from the Email Contact Distribution Group when creating or sending emails.   
- Display a structured compliance report for download or printing.   
- Provide visual feedback for actions such as archiving, restoring, or deleting emails and contacts.   
- Enable the Administrator to manage email accounts, including updating usernames, passwords, domains, and signatures.   
- Allow navigation and interaction with the Email Archive, including tagging, categorizing, and moving archived emails to subfolders.   
  
The user interface should support intuitive controls and clear data representation to facilitate efficient system usage. It must be consistent in terminology and design, aligning with the functional requirements to ensure clarity and reduce confusion for the user.  
  
2.2 Hardware Interface Output   
There are no direct hardware interfaces required for this system. All operations are conducted through software and user interaction. However, the system must be compatible with standard computing hardware such as servers, workstations, and storage devices used to host the application and databases.   
  
The system may indirectly interact with hardware interfaces for tasks such as:   
- Email sending and receiving via network hardware (e.g., routers, switches).   
- Storing and retrieving emails and contacts from disk-based storage systems.   
  
These interactions are abstracted through software and communication interfaces and are not explicitly required for the system's core functionality.  
  
2.3 Software Interface Output   
The system interacts with the following software components and data sources:   
  
2.3.1 Email Archive   
- \*\*Definition\*\*: A repository where emails are stored after being archived by the system.   
- \*\*Role\*\*: Stores and manages historical email records, including metadata and audit trails.   
- \*\*Interaction Method\*\*:   
 - Input: Email object, EmailArchiveRecord, and management actions (e.g., tag, move, delete).   
 - Output: Archived Email object, updated EmailArchiveRecord, and Audit Record when applicable.   
- \*\*Description\*\*: The Email Archive is a critical data store for compliance and audit purposes. Emails are archived automatically upon deletion or manually via the Email Archiving Function (FR-06). The system allows the Administrator to manage these archived records, including tagging, categorizing, and recovery (FR-24, FR-25).   
  
2.3.2 Email Contact Distribution Group   
- \*\*Definition\*\*: A collection of contacts or sub-groups used to manage recipient lists for emails.   
- \*\*Role\*\*: Provides the structure for selecting recipients when emails are created or sent.   
- \*\*Interaction Method\*\*:   
 - Input: Contact IDs, distribution group names, descriptions, and configuration changes.   
 - Output: Updated distribution groups, contact associations, and Audit Records when changes are made.   
- \*\*Description\*\*: The Email Contact Distribution Group allows the Administrator to organize contacts into logical groups for efficient email distribution. It is used in the Email Creation Function (FR-01), Distribution Group Management Functions (FR-12 to FR-16), and Compliance Report Generation (FR-22).   
  
2.3.3 Email Account   
- \*\*Definition\*\*: A configured email account used for sending and receiving emails.   
- \*\*Role\*\*: Provides the credentials and settings for email communication.   
- \*\*Interaction Method\*\*:   
 - Input: Email Account ID, credentials (username, password), domain, signature, and configuration updates.   
 - Output: Updated EmailAccount object and Audit Record when changes are made.   
- \*\*Description\*\*: The Email Account is used to authenticate and send emails to recipients, as well as retrieve incoming emails. It is a core component of the Email Sending Function (FR-02), Email Receiving Function (FR-03), and Email Account Management Functions (FR-17 to FR-20).   
  
2.3.4 Audit Record   
- \*\*Definition\*\*: A log of all system actions, such as email creation, deletion, archiving, and updates.   
- \*\*Role\*\*: Tracks user activity and system changes for auditing and compliance purposes.   
- \*\*Interaction Method\*\*:   
 - Input: Email or contact actions (e.g., deletion, archiving).   
 - Output: An Audit Record is generated and stored in the system.   
- \*\*Description\*\*: The Audit Record is essential for system transparency and accountability. It is generated automatically when emails or contacts are deleted or archived (FR-05, FR-06, FR-25) and can be manually viewed by the Administrator (FR-21).   
  
2.3.5 Contact Database   
- \*\*Definition\*\*: A database or data store that contains all contact records.   
- \*\*Role\*\*: Stores and retrieves contact information for email distribution.   
- \*\*Interaction Method\*\*:   
 - Input: Contact details (name, email address, phone number, address) and actions (create, update, delete).   
 - Output: Contact object stored in the database and associated with the Email Contact Distribution Group.   
- \*\*Description\*\*: The system relies on the Contact Database to maintain up-to-date contact information. It is used in all Contact Management Functions (FR-08 to FR-11 and FR-15 to FR-16).   
  
2.4 Communication Interface Output   
The system communicates with external systems or services via the following communication interfaces:   
  
2.4.1 Email Server (SMTP/IMAP)   
- \*\*Definition\*\*: A third-party or internal email server that handles the sending and receiving of emails.   
- \*\*Role\*\*: Facilitates the delivery of outgoing emails and the retrieval of incoming emails.   
- \*\*Interaction Method\*\*:   
 - Input: Email content, recipient list, and authentication credentials from the Email Account.   
 - Output: Delivery confirmation for outgoing emails and incoming email data retrieved from the server.   
- \*\*Description\*\*: The system interacts with email servers using SMTP for sending and IMAP/POP3 for receiving emails. This is a core part of the Email Sending Function (FR-02) and Email Receiving Function (FR-03).   
  
2.4.2 Compliance Report Data Sources   
- \*\*Definition\*\*: A combination of the Email Archive, Audit Records, and Email Contact Distribution Group used to generate compliance reports.   
- \*\*Role\*\*: Provides structured data for regulatory or internal compliance audits.   
- \*\*Interaction Method\*\*:   
 - Input: Report criteria such as date ranges, specific Email Accounts, or groups.   
 - Output: A structured compliance report that can be downloaded or printed.   
- \*\*Description\*\*: The system pulls data from multiple sources to compile a compliance report. The Administrator can request reports based on specific time frames, email accounts, or distribution groups (FR-22).   
  
2.4.3 Email Notification Service (Optional)   
- \*\*Definition\*\*: An external service that can push notifications or updates to the Administrator.   
- \*\*Role\*\*: Notifies the Administrator of system events, such as new incoming emails or compliance report completion.   
- \*\*Interaction Method\*\*:   
 - Input: System events (e.g., new email received, compliance report ready).   
 - Output: Notification sent to the Administrator via email or in-app alerts.   
- \*\*Description\*\*: This interface is optional but can be integrated to enhance user experience by providing real-time updates. It is not explicitly required by the functional requirements but can be considered for system enhancement.   
  
2.4.4 Web-Based Communication (Optional)   
- \*\*Definition\*\*: The system may be accessed via a web browser or web application.   
- \*\*Role\*\*: Enables remote access to the system for managing emails, contacts, and distribution groups.   
- \*\*Interaction Method\*\*:   
 - Input: User login credentials and actions performed via the web interface.   
 - Output: Web-based display of system data and responses to user actions.   
- \*\*Description\*\*: If the system is deployed as a web application, it will support communication via HTTP/HTTPS protocols. This is optional but can be considered for scalability and accessibility.   
  
This section has identified all external data sources and interfaces that are referenced in the functional requirements. Each interface is clearly defined, with its role and interaction method described to ensure clarity for developers and stakeholders.

# Use Case

Use Case Name: Create Email   
Use Case ID: UC-01   
Actors: Administrator, Email Account   
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The Email Account is valid and associated with the Administrator.   
3. The system has access to the Email Archive and Audit Record modules for logging and storage.   
  
Postconditions:   
1. A new email is created and associated with the appropriate Email Contact Distribution Group.   
2. The email is saved to the Email Archive.   
3. An Audit Record is created documenting the email creation process.   
  
Main Flow:   
1. The Administrator selects the "Create Email" option from the system interface.   
2. The system prompts the Administrator to enter the email subject, body, and select recipients from the Email Contact Distribution Group.   
3. The Administrator enters the required information and confirms the recipients.   
4. The system validates the email content and recipient list.   
5. The system creates the email and associates it with the selected Email Contact Distribution Group.   
6. The system saves the email to the Email Archive.   
7. The system generates an Audit Record for the email creation event.   
8. The system confirms the successful creation of the email and displays a summary to the Administrator.   
  
Alternative Flow:   
1. If the email content is invalid (e.g., missing subject or body), the system displays an error message and prompts the Administrator to correct the information.   
2. If no recipients are selected, the system displays a warning and requires the Administrator to choose at least one recipient from the Email Contact Distribution Group.   
3. If the system fails to save the email to the Email Archive, the system displays an error message, and the Administrator is prompted to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was created but the audit process may be incomplete.  
  
Use Case Name: Send Email   
Use Case ID: UC-02   
Actors: Administrator, Email Account, Email Contact Distribution Group   
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The Email Account is valid and associated with the Administrator.   
3. An email has already been created using the "Create Email" use case.   
4. The system has access to the Email Archive and Audit Record modules for logging and storage.   
  
Postconditions:   
1. The email is successfully sent to the selected recipients in the Email Contact Distribution Group.   
2. A copy of the sent email is archived in the Email Archive.   
3. An Audit Record is created documenting the email sending process.   
  
Main Flow:   
1. The Administrator selects the "Send Email" option from the system interface.   
2. The system displays the email content and recipient list from the Email Contact Distribution Group.   
3. The Administrator reviews the email content and recipient list, and confirms the send action.   
4. The system validates the recipient list and email status (e.g., draft or ready to send).   
5. The system sends the email to the selected recipients using the associated Email Account.   
6. The system archives the sent email in the Email Archive.   
7. The system generates an Audit Record for the email sending event.   
8. The system confirms the successful sending of the email and displays a summary to the Administrator.   
  
Alternative Flow:   
1. If the recipient list is invalid or empty, the system displays an error message and prompts the Administrator to select at least one valid recipient.   
2. If the email is still in draft status, the system asks the Administrator if they want to finalize and send it or continue editing.   
3. If the system fails to send the email (e.g., due to network issues or invalid Email Account configuration), the system displays an error message and prompts the Administrator to retry the operation.   
4. If the system fails to archive the sent email, the system logs an internal error and notifies the Administrator that the email was sent but the archive process may be incomplete.   
5. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was sent but the audit process may be incomplete.  
  
Use Case Name: Receive Email   
Use Case ID: UC-03   
Actors: System, Email Account, Administrator   
Preconditions:   
1. The system is connected to the Email Account for receiving emails.   
2. The Administrator is authenticated and has access to the system.   
3. The system has access to the Email Archive and Audit Record modules for logging and storage.   
  
Postconditions:   
1. The received email is stored in the system and associated with the appropriate Email Contact Distribution Group.   
2. A copy of the received email is archived in the Email Archive.   
3. An Audit Record is created documenting the email receiving process.   
  
Main Flow:   
1. The system detects a new email received by the Email Account.   
2. The system retrieves the email content and identifies the sender from the Email Contact Distribution Group.   
3. The system stores the received email in the appropriate location.   
4. The system archives the email in the Email Archive.   
5. The system generates an Audit Record for the email receiving event.   
6. The system notifies the Administrator of the new email and provides a summary.   
  
Alternative Flow:   
1. If the system fails to retrieve the email (e.g., due to connection issues), it logs an error and prompts the Administrator to check the Email Account configuration.   
2. If the sender is not recognized in the Email Contact Distribution Group, the system flags the email for review and notifies the Administrator.   
3. If the system fails to save the email to the Email Archive, it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was received but the audit process may be incomplete.  
  
Use Case Name: View Email   
Use Case ID: UC-04   
Actors: Administrator, Email Archive   
Preconditions:   
1. The Administrator is authenticated and has access to the system.   
2. At least one email exists in the Email Archive.   
3. The system has access to the Email Archive module for retrieval.   
  
Postconditions:   
1. The Administrator can view the selected email's content and metadata.   
2. The system logs the viewing action in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "View Email" option from the system interface.   
2. The system displays a list of available emails from the Email Archive.   
3. The Administrator selects a specific email to view.   
4. The system retrieves the selected email's content and metadata from the Email Archive.   
5. The system presents the email to the Administrator in a readable format.   
6. The system generates an Audit Record for the email viewing event.   
  
Alternative Flow:   
1. If no emails are available in the Email Archive, the system displays a message indicating that there are no emails to view.   
2. If the selected email cannot be retrieved (e.g., due to file corruption or access issues), the system displays an error message and prompts the Administrator to try another email or contact support.   
3. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was viewed but the audit process may be incomplete.  
  
Use Case Name: Delete Email   
Use Case ID: UC-05   
Actors: Administrator, Email Archive, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the system.   
2. At least one email exists in the system that can be deleted.   
3. The system has access to the Email Archive and Audit Record modules for logging and storage.   
  
Postconditions:   
1. The selected email is deleted from the system.   
2. The deleted email is archived in the Email Archive.   
3. An Audit Record is created documenting the email deletion process.   
  
Main Flow:   
1. The Administrator selects the "Delete Email" option from the system interface.   
2. The system displays a list of emails that can be deleted.   
3. The Administrator selects the specific email to delete.   
4. The system confirms the deletion with the Administrator.   
5. The system deletes the email from the system.   
6. The system archives the deleted email in the Email Archive.   
7. The system generates an Audit Record for the email deletion event.   
8. The system confirms the successful deletion of the email and updates the email list.   
  
Alternative Flow:   
1. If the selected email cannot be deleted (e.g., due to permissions or system constraints), the system displays an error message and prompts the Administrator to choose another email.   
2. If the system fails to archive the deleted email, it logs an internal error and notifies the Administrator that the email was deleted but the archive process may be incomplete.   
3. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was deleted but the audit process may be incomplete.  
  
Use Case Name: Archive Email   
Use Case ID: UC-06   
Actors: Administrator, Email Archive, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the system.   
2. An email exists in the system that is eligible for archiving.   
3. The system has access to the Email Archive and Audit Record modules for logging and storage.   
  
Postconditions:   
1. The selected email is moved to the Email Archive.   
2. An Audit Record is created documenting the email archiving process.   
  
Main Flow:   
1. The Administrator selects the "Archive Email" option from the system interface.   
2. The system displays a list of emails available for archiving.   
3. The Administrator selects the email to be archived.   
4. The system confirms the archiving action with the Administrator.   
5. The system moves the selected email to the Email Archive.   
6. The system generates an Audit Record for the archiving event.   
7. The system confirms the successful archiving of the email and updates the email list.   
  
Alternative Flow:   
1. If no emails are available for archiving, the system displays a message indicating that there are no emails to archive.   
2. If the selected email cannot be archived (e.g., due to system constraints), the system displays an error message and prompts the Administrator to choose another email.   
3. If the system fails to save the email to the Email Archive, it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was archived but the audit process may be incomplete.  
  
Use Case Name: Recover Email   
Use Case ID: UC-07   
Actors: Administrator, Email Archive, Email Account   
Preconditions:   
1. The Administrator is authenticated and has access to the system.   
2. At least one email exists in the Email Archive that can be recovered.   
3. The system has access to the Email Archive and Audit Record modules for logging and storage.   
  
Postconditions:   
1. The selected email is recovered and restored to the system.   
2. The recovered email is associated with the appropriate Email Account.   
3. An Audit Record is created documenting the email recovery process.   
  
Main Flow:   
1. The Administrator selects the "Recover Email" option from the system interface.   
2. The system displays a list of emails available in the Email Archive for recovery.   
3. The Administrator selects the email to be recovered.   
4. The system retrieves the selected email from the Email Archive.   
5. The system confirms the recovery action with the Administrator.   
6. The system restores the email to the system and associates it with the relevant Email Account.   
7. The system generates an Audit Record for the recovery event.   
8. The system confirms the successful recovery of the email and updates the email list.   
  
Alternative Flow:   
1. If no emails are available in the Email Archive, the system displays a message indicating that there are no emails to recover.   
2. If the selected email cannot be recovered (e.g., due to system constraints or data corruption), the system displays an error message and prompts the Administrator to choose another email.   
3. If the system fails to restore the email to the system, it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was recovered but the audit process may be incomplete.  
  
Use Case Name: Create Contact   
Use Case ID: UC-08   
Actors: Administrator, Email Contact Distribution Group   
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The system is configured to allow contact creation.   
3. The system has access to the Email Archive and Audit Record modules for logging and storage.   
  
Postconditions:   
1. A new contact is successfully created and added to the Email Contact Distribution Group.   
2. The contact information is stored in the system.   
3. An Audit Record is created documenting the contact creation process.   
  
Main Flow:   
1. The Administrator selects the "Create Contact" option from the system interface.   
2. The system prompts the Administrator to enter the contact's details (e.g., name, email address, phone number).   
3. The Administrator enters the required information and submits the request.   
4. The system validates the contact details (e.g., checks for valid email format).   
5. The system adds the new contact to the Email Contact Distribution Group.   
6. The system generates an Audit Record for the contact creation event.   
7. The system confirms the successful creation of the contact and updates the contact list.   
  
Alternative Flow:   
1. If the contact details are invalid (e.g., missing required fields or incorrect email format), the system displays an error message and prompts the Administrator to correct the information.   
2. If the contact already exists in the Email Contact Distribution Group, the system displays a warning and asks the Administrator if they want to update the existing contact or cancel the creation.   
3. If the system fails to save the contact information, it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the contact was created but the audit process may be incomplete.  
  
Use Case Name: Update Contact   
Use Case ID: UC-09   
Actors: Administrator, Email Contact Distribution Group, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The contact to be updated already exists in the Email Contact Distribution Group.   
3. The system has access to the Audit Record module for logging the update process.   
  
Postconditions:   
1. The contact information is updated in the Email Contact Distribution Group.   
2. The system logs the update action in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "Update Contact" option from the system interface.   
2. The system displays a list of existing contacts from the Email Contact Distribution Group.   
3. The Administrator selects the contact they wish to update.   
4. The system retrieves the current contact details and displays them in an editable form.   
5. The Administrator modifies the necessary information (e.g., email address, phone number, name).   
6. The Administrator submits the updated contact information.   
7. The system validates the updated contact details (e.g., checks for valid email format).   
8. The system updates the contact information in the Email Contact Distribution Group.   
9. The system generates an Audit Record for the contact update event.   
10. The system confirms the successful update of the contact and updates the contact list.   
  
Alternative Flow:   
1. If the contact does not exist in the Email Contact Distribution Group, the system displays an error message and prompts the Administrator to select a valid contact.   
2. If the updated contact details are invalid (e.g., missing required fields or incorrect email format), the system displays an error message and prompts the Administrator to correct the information.   
3. If the system fails to update the contact in the Email Contact Distribution Group, it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the contact was updated but the audit process may be incomplete.  
  
Use Case Name: Delete Contact   
Use Case ID: UC-10   
Actors: Administrator, Email Contact Distribution Group, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The contact to be deleted already exists in the Email Contact Distribution Group.   
3. The system has access to the Audit Record module for logging the deletion process.   
  
Postconditions:   
1. The selected contact is deleted from the Email Contact Distribution Group.   
2. The system logs the deletion action in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "Delete Contact" option from the system interface.   
2. The system displays a list of existing contacts from the Email Contact Distribution Group.   
3. The Administrator selects the contact they wish to delete.   
4. The system confirms the deletion with the Administrator.   
5. The system removes the selected contact from the Email Contact Distribution Group.   
6. The system generates an Audit Record for the contact deletion event.   
7. The system confirms the successful deletion of the contact and updates the contact list.   
  
Alternative Flow:   
1. If the selected contact does not exist in the Email Contact Distribution Group, the system displays an error message and prompts the Administrator to select a valid contact.   
2. If the Administrator cancels the deletion during the confirmation step, the system returns to the main interface without making any changes.   
3. If the system fails to delete the contact (e.g., due to permissions or system constraints), it displays an error message and prompts the Administrator to choose another contact.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the contact was deleted but the audit process may be incomplete.  
  
Use Case Name: View Contact   
Use Case ID: UC-11   
Actors: Administrator, Email Contact Distribution Group   
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. At least one contact exists in the Email Contact Distribution Group.   
3. The system has access to the Audit Record module for logging the viewing action.   
  
Postconditions:   
1. The Administrator can view the selected contact's details (e.g., name, email, phone number).   
2. The system logs the viewing action in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "View Contact" option from the system interface.   
2. The system displays a list of contacts from the Email Contact Distribution Group.   
3. The Administrator selects a specific contact to view.   
4. The system retrieves and displays the contact's details in a read-only format.   
5. The system generates an Audit Record for the contact viewing event.   
6. The system confirms the successful retrieval of the contact information.   
  
Alternative Flow:   
1. If no contacts are available in the Email Contact Distribution Group, the system displays a message indicating that there are no contacts to view.   
2. If the selected contact cannot be retrieved (e.g., due to system constraints or data corruption), the system displays an error message and prompts the Administrator to choose another contact.   
3. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the contact was viewed but the audit process may be incomplete.  
  
Use Case Name: Create Distribution Group   
Use Case ID: UC-12   
Actors: Administrator, Email Contact Distribution Group, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The system is configured to allow the creation of distribution groups.   
3. The system has access to the Audit Record module for logging the creation process.   
  
Postconditions:   
1. A new distribution group is successfully created and saved in the Email Contact Distribution Group.   
2. The distribution group is associated with one or more contacts.   
3. An Audit Record is created documenting the distribution group creation process.   
  
Main Flow:   
1. The Administrator selects the "Create Distribution Group" option from the system interface.   
2. The system prompts the Administrator to enter the distribution group name and description.   
3. The Administrator enters the required information and selects contacts to add to the group.   
4. The system validates the group name and contact selections.   
5. The system creates the new distribution group and adds the selected contacts.   
6. The system generates an Audit Record for the distribution group creation event.   
7. The system confirms the successful creation of the distribution group and updates the group list.   
  
Alternative Flow:   
1. If the group name is missing or invalid, the system displays an error message and prompts the Administrator to provide a valid name.   
2. If no contacts are selected for the distribution group, the system displays a warning and requires the Administrator to choose at least one contact.   
3. If the system fails to save the distribution group, it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the group was created but the audit process may be incomplete.  
  
Use Case Name: Update Distribution Group   
Use Case ID: UC-13   
Actors: Administrator, Email Contact Distribution Group, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The distribution group to be updated already exists in the system.   
3. The system has access to the Audit Record module for logging the update process.   
  
Postconditions:   
1. The distribution group is updated with the new name, description, or contact list.   
2. The changes are saved in the Email Contact Distribution Group.   
3. An Audit Record is created documenting the distribution group update process.   
  
Main Flow:   
1. The Administrator selects the "Update Distribution Group" option from the system interface.   
2. The system displays a list of existing distribution groups for the Administrator to choose from.   
3. The Administrator selects the distribution group they wish to update.   
4. The system retrieves the current group details and displays them in an editable form.   
5. The Administrator modifies the group name, description, or adds/removes contacts as needed.   
6. The Administrator submits the updated information.   
7. The system validates the changes (e.g., checks for valid group name and contact selections).   
8. The system updates the distribution group in the Email Contact Distribution Group module.   
9. The system generates an Audit Record for the update event.   
10. The system confirms the successful update and displays the updated group information.   
  
Alternative Flow:   
1. If the selected distribution group does not exist, the system displays an error message and prompts the Administrator to select a valid group.   
2. If the updated group name is missing or invalid, the system displays an error message and prompts the Administrator to provide a valid name.   
3. If no changes are made to the group, the system displays a warning and asks the Administrator to confirm or cancel the update.   
4. If the system fails to save the updated group, it displays an error message and prompts the Administrator to retry the operation.   
5. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the group was updated but the audit process may be incomplete.  
  
Use Case Name: Delete Distribution Group   
Use Case ID: UC-14   
Actors: Administrator, Email Contact Distribution Group, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The distribution group to be deleted already exists in the system.   
3. The system has access to the Audit Record module for logging the deletion process.   
  
Postconditions:   
1. The selected distribution group is deleted from the Email Contact Distribution Group.   
2. An Audit Record is created documenting the distribution group deletion process.   
  
Main Flow:   
1. The Administrator selects the "Delete Distribution Group" option from the system interface.   
2. The system displays a list of existing distribution groups for the Administrator to choose from.   
3. The Administrator selects the distribution group they wish to delete.   
4. The system confirms the deletion with the Administrator.   
5. The system removes the selected distribution group from the Email Contact Distribution Group.   
6. The system generates an Audit Record for the deletion event.   
7. The system confirms the successful deletion of the distribution group and updates the group list.   
  
Alternative Flow:   
1. If the selected distribution group does not exist, the system displays an error message and prompts the Administrator to select a valid group.   
2. If the Administrator cancels the deletion during the confirmation step, the system returns to the main interface without making any changes.   
3. If the system fails to delete the distribution group (e.g., due to permissions or system constraints), it displays an error message and prompts the Administrator to choose another group.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the group was deleted but the audit process may be incomplete.  
  
Use Case Name: Add Contact to Distribution Group   
Use Case ID: UC-15   
Actors: Administrator, Email Contact Distribution Group, Email Account, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The contact to be added exists in the system.   
3. The target distribution group already exists in the Email Contact Distribution Group.   
4. The system has access to the Audit Record module for logging the addition process.   
  
Postconditions:   
1. The selected contact is successfully added to the target distribution group.   
2. The system logs the addition action in the Audit Record.   
3. The updated distribution group is saved in the Email Contact Distribution Group.   
  
Main Flow:   
1. The Administrator selects the "Add Contact to Distribution Group" option from the system interface.   
2. The system displays a list of contacts and a list of distribution groups.   
3. The Administrator selects a contact and a distribution group to add the contact to.   
4. The system confirms the addition with the Administrator.   
5. The system adds the selected contact to the distribution group.   
6. The system generates an Audit Record for the addition event.   
7. The system confirms the successful addition and updates the group and contact lists.   
  
Alternative Flow:   
1. If the selected contact does not exist, the system displays an error message and prompts the Administrator to choose a valid contact.   
2. If the selected distribution group does not exist, the system displays an error message and prompts the Administrator to choose a valid group.   
3. If the contact is already a member of the distribution group, the system displays a warning and asks the Administrator if they want to proceed or cancel.   
4. If the system fails to update the distribution group (e.g., due to system constraints), it displays an error message and prompts the Administrator to retry the operation.   
5. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the contact was added but the audit process may be incomplete.  
  
Use Case Name: Remove Contact from Distribution Group   
Use Case ID: UC-16   
Actors: Administrator, Email Contact Distribution Group, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Contact Distribution Group.   
2. The contact to be removed is a member of the selected distribution group.   
3. The system has access to the Audit Record module for logging the removal process.   
  
Postconditions:   
1. The selected contact is removed from the distribution group.   
2. The system logs the removal action in the Audit Record.   
3. The updated distribution group is saved in the Email Contact Distribution Group.   
  
Main Flow:   
1. The Administrator selects the "Remove Contact from Distribution Group" option from the system interface.   
2. The system displays a list of distribution groups for the Administrator to choose from.   
3. The Administrator selects a distribution group and views the list of contacts in that group.   
4. The Administrator selects the contact they wish to remove.   
5. The system confirms the removal action with the Administrator.   
6. The system removes the selected contact from the distribution group.   
7. The system generates an Audit Record for the removal event.   
8. The system confirms the successful removal and updates the group and contact lists.   
  
Alternative Flow:   
1. If the selected contact is not a member of the distribution group, the system displays an error message and prompts the Administrator to select a valid contact.   
2. If the selected distribution group does not exist, the system displays an error message and prompts the Administrator to choose a valid group.   
3. If the Administrator cancels the removal during the confirmation step, the system returns to the main interface without making any changes.   
4. If the system fails to update the distribution group (e.g., due to permissions or system constraints), it displays an error message and prompts the Administrator to retry the operation.   
5. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the contact was removed but the audit process may be incomplete.  
  
Use Case Name: Manage Email Account   
Use Case ID: UC-17   
Actors: Administrator, Email Account, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Account settings.   
2. The Email Account exists in the system and is associated with the Administrator.   
3. The system has access to the Audit Record module for logging the management process.   
  
Postconditions:   
1. The Email Account settings are successfully updated or modified.   
2. The system logs the management action in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "Manage Email Account" option from the system interface.   
2. The system displays the current Email Account details (e.g., username, password, server settings).   
3. The Administrator modifies the necessary information (e.g., password, email signature, permissions).   
4. The Administrator submits the updated Email Account information.   
5. The system validates the changes (e.g., checks for valid password format or server configuration).   
6. The system updates the Email Account settings in the system.   
7. The system generates an Audit Record for the management event.   
8. The system confirms the successful update of the Email Account and displays the updated information.   
  
Alternative Flow:   
1. If the Email Account does not exist, the system displays an error message and prompts the Administrator to select a valid account.   
2. If the updated Email Account information is invalid (e.g., password does not meet security requirements), the system displays an error message and prompts the Administrator to correct the information.   
3. If the system fails to update the Email Account (e.g., due to permissions or system constraints), it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the Email Account was updated but the audit process may be incomplete.  
  
Use Case Name: Update Email Account   
Use Case ID: UC-18   
Actors: Administrator, Email Account, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Account settings.   
2. The Email Account to be updated already exists in the system and is associated with the Administrator.   
3. The system has access to the Audit Record module for logging the update process.   
  
Postconditions:   
1. The Email Account settings are successfully updated (e.g., password, server settings, signature).   
2. The system logs the update action in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "Update Email Account" option from the system interface.   
2. The system displays the current Email Account details in an editable form.   
3. The Administrator modifies the necessary information (e.g., password, signature, server settings).   
4. The Administrator submits the updated information for review.   
5. The system validates the updated information (e.g., checks for valid password format or server configuration).   
6. The system updates the Email Account settings in the system.   
7. The system generates an Audit Record for the update event.   
8. The system confirms the successful update of the Email Account and displays the updated information.   
  
Alternative Flow:   
1. If the Email Account does not exist, the system displays an error message and prompts the Administrator to select a valid account.   
2. If the updated information is invalid (e.g., password does not meet security requirements), the system displays an error message and prompts the Administrator to correct the information.   
3. If the system fails to update the Email Account (e.g., due to permissions or system constraints), it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the Email Account was updated but the audit process may be incomplete.  
  
Use Case Name: Delete Email Account   
Use Case ID: UC-19   
Actors: Administrator, Email Account, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Account settings.   
2. The Email Account to be deleted already exists in the system and is associated with the Administrator.   
3. The system has access to the Audit Record module for logging the deletion process.   
  
Postconditions:   
1. The selected Email Account is deleted from the system.   
2. The deletion action is logged in the Audit Record.   
3. Any associated emails or settings are either archived or removed accordingly.   
  
Main Flow:   
1. The Administrator selects the "Delete Email Account" option from the system interface.   
2. The system displays a list of Email Accounts for the Administrator to choose from.   
3. The Administrator selects the Email Account they wish to delete.   
4. The system confirms the deletion with the Administrator.   
5. The system removes the selected Email Account from the system.   
6. The system generates an Audit Record for the deletion event.   
7. The system confirms the successful deletion of the Email Account and updates the account list.   
  
Alternative Flow:   
1. If the selected Email Account does not exist, the system displays an error message and prompts the Administrator to select a valid account.   
2. If the Administrator cancels the deletion during the confirmation step, the system returns to the main interface without making any changes.   
3. If the system fails to delete the Email Account (e.g., due to dependencies or system constraints), it displays an error message and prompts the Administrator to resolve the issue or choose another account.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the Email Account was deleted but the audit process may be incomplete.  
  
Use Case Name: Manage Email Account Permissions   
Use Case ID: UC-20   
Actors: Administrator, Email Account, Email Contact Distribution Group, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Account and Email Contact Distribution Group.   
2. The Email Account exists in the system and is associated with the Administrator.   
3. The system has access to the Audit Record module for logging the permission changes.   
  
Postconditions:   
1. The permissions of the Email Account are successfully updated or modified.   
2. The updated permissions are applied to the Email Contact Distribution Group.   
3. The system logs the permission changes in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "Manage Email Account Permissions" option from the system interface.   
2. The system displays a list of Email Accounts for the Administrator to choose from.   
3. The Administrator selects an Email Account and views its current permission settings.   
4. The Administrator modifies the permission settings (e.g., granting or revoking access to specific groups or users).   
5. The Administrator submits the updated permission settings.   
6. The system validates the permission changes (e.g., checks for conflicts or invalid configurations).   
7. The system updates the Email Account's permissions and applies the changes to the Email Contact Distribution Group.   
8. The system generates an Audit Record for the permission management event.   
9. The system confirms the successful update of the Email Account permissions and displays the updated settings.   
  
Alternative Flow:   
1. If the selected Email Account does not exist, the system displays an error message and prompts the Administrator to select a valid account.   
2. If the updated permissions are invalid (e.g., conflicting group assignments or missing required access levels), the system displays an error message and prompts the Administrator to correct the information.   
3. If the system fails to update the Email Account permissions (e.g., due to system constraints), it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the permissions were updated but the audit process may be incomplete.  
  
Use Case Name: View Audit Record   
Use Case ID: UC-21   
Actors: Administrator, Audit Record   
Preconditions:   
1. The Administrator is authenticated and has access to the Audit Record module.   
2. At least one Audit Record exists in the system.   
3. The system has access to the Audit Record module for retrieval.   
  
Postconditions:   
1. The Administrator can view the selected Audit Record's details (e.g., action performed, timestamp, user involved).   
2. The system confirms the successful retrieval of the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "View Audit Record" option from the system interface.   
2. The system displays a list of available Audit Records.   
3. The Administrator selects a specific Audit Record to view.   
4. The system retrieves the selected Audit Record's details from the Audit Record module.   
5. The system presents the Audit Record to the Administrator in a read-only format.   
6. The system confirms the successful retrieval of the Audit Record.   
  
Alternative Flow:   
1. If no Audit Records are available, the system displays a message indicating that there are no records to view.   
2. If the selected Audit Record cannot be retrieved (e.g., due to data corruption or access issues), the system displays an error message and prompts the Administrator to choose another record or contact support.  
  
Use Case Name: Generate Compliance Report   
Use Case ID: UC-22   
Actors: Administrator, Email Archive, Audit Record, Email Contact Distribution Group   
  
Preconditions:   
1. The Administrator is authenticated and has access to the compliance reporting feature.   
2. The system contains at least one email, contact, or distribution group that can be included in the compliance report.   
3. The system has access to the Email Archive, Audit Record, and Email Contact Distribution Group modules for data retrieval.   
  
Postconditions:   
1. A compliance report is generated and displayed to the Administrator.   
2. The report includes relevant data from the Email Archive, Audit Record, and Email Contact Distribution Group.   
3. The system logs the compliance report generation in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "Generate Compliance Report" option from the system interface.   
2. The system prompts the Administrator to select the scope of the report (e.g., date range, specific email account, distribution group, or contact).   
3. The Administrator selects the required criteria and confirms the report generation.   
4. The system retrieves relevant data from the Email Archive, Audit Record, and Email Contact Distribution Group based on the selected criteria.   
5. The system compiles the data into a structured compliance report.   
6. The system generates an Audit Record for the compliance report generation event.   
7. The system displays the compliance report to the Administrator in a readable format.   
8. The Administrator can download or print the report as needed.   
  
Alternative Flow:   
1. If no data is available based on the selected criteria, the system displays a message indicating that the report cannot be generated.   
2. If the selected criteria is invalid or incomplete, the system displays an error message and prompts the Administrator to provide valid inputs.   
3. If the system fails to retrieve data from the Email Archive or Audit Record, it displays an error message and prompts the Administrator to check the system configuration or retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the report was generated but the audit process may be incomplete.  
  
It seems there might be a misunderstanding, as the use case "Archive Email" (UC-06) has already been included in the provided list. If you'd like me to help with a different new use case or clarify something about the existing one, please provide additional details or specify the new functionality you'd like added.  
  
Use Case Name: Recover Email   
Use Case ID: UC-23   
Actors: Administrator, Email Archive, Email Account, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the system.   
2. The email to be recovered exists in the Email Archive.   
3. The system has access to the Email Archive and Audit Record modules for logging and retrieval.   
4. The system is configured to allow email recovery from the Email Archive.   
  
Postconditions:   
1. The selected email is successfully recovered and restored to the system.   
2. The recovered email is associated with the appropriate Email Account.   
3. An Audit Record is created documenting the email recovery process.   
  
Main Flow:   
1. The Administrator selects the "Recover Email" option from the system interface.   
2. The system displays a list of emails available in the Email Archive for recovery.   
3. The Administrator selects the email to be recovered.   
4. The system retrieves the selected email from the Email Archive.   
5. The system confirms the recovery action with the Administrator.   
6. The system restores the email to the system and associates it with the relevant Email Account.   
7. The system generates an Audit Record for the recovery event.   
8. The system confirms the successful recovery of the email and updates the email list.   
  
Alternative Flow:   
1. If no emails are available in the Email Archive, the system displays a message indicating that there are no emails to recover.   
2. If the selected email cannot be recovered (e.g., due to system constraints or data corruption), the system displays an error message and prompts the Administrator to choose another email.   
3. If the system fails to restore the email to the system, it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was recovered but the audit process may be incomplete.  
  
Use Case Name: Manage Email Archive   
Use Case ID: UC-24   
Actors: Administrator, Email Archive, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Archive module.   
2. The system contains at least one email stored in the Email Archive.   
3. The system has access to the Audit Record module for logging the management process.   
4. The system is configured to allow email archive management (e.g., organize, tag, or categorize emails).   
  
Postconditions:   
1. The selected email in the Email Archive is successfully managed (e.g., tagged, moved to a subfolder, or categorized).   
2. The system logs the management action in the Audit Record.   
3. The Email Archive is updated to reflect the changes in the email's status or metadata.   
  
Main Flow:   
1. The Administrator selects the "Manage Email Archive" option from the system interface.   
2. The system displays a list of emails currently stored in the Email Archive.   
3. The Administrator selects a specific email to manage and chooses an action (e.g., tag, categorize, move, or delete).   
4. The system prompts the Administrator for any additional information required to perform the action (e.g., tag name, category, or destination folder).   
5. The Administrator provides the necessary details and confirms the action.   
6. The system performs the selected management action on the email (e.g., updates tags, moves it to a new folder, or reclassifies it).   
7. The system generates an Audit Record for the email archive management event.   
8. The system confirms the successful management of the email and updates the Email Archive accordingly.   
  
Alternative Flow:   
1. If the selected email does not exist in the Email Archive, the system displays an error message and prompts the Administrator to select a valid email.   
2. If the provided management details are invalid (e.g., invalid tag or folder name), the system displays an error message and prompts the Administrator to correct the information.   
3. If the system fails to update the Email Archive (e.g., due to system constraints), it displays an error message and prompts the Administrator to retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email archive was modified but the audit process may be incomplete.  
  
Use Case Name: View Audit Record   
Use Case ID: UC-25   
Actors: Administrator, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Audit Record module.   
2. At least one Audit Record exists in the system.   
3. The system has access to the Audit Record module for retrieval.   
  
Postconditions:   
1. The Administrator can view the selected Audit Record's details (e.g., action performed, timestamp, user involved).   
2. The system confirms the successful retrieval of the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "View Audit Record" option from the system interface.   
2. The system displays a list of available Audit Records.   
3. The Administrator selects a specific Audit Record to view.   
4. The system retrieves the selected Audit Record's details from the Audit Record module.   
5. The system presents the Audit Record to the Administrator in a read-only format.   
6. The system confirms the successful retrieval of the Audit Record.   
  
Alternative Flow:   
1. If no Audit Records are available, the system displays a message indicating that there are no records to view.   
2. If the selected Audit Record cannot be retrieved (e.g., due to data corruption or access issues), the system displays an error message and prompts the Administrator to choose another record or contact support.  
  
Use Case Name: Generate Compliance Report   
Use Case ID: UC-23   
Actors: Administrator, Email Archive, Audit Record, Email Contact Distribution Group   
  
Preconditions:   
1. The Administrator is authenticated and has access to the compliance reporting feature.   
2. The system contains at least one email, contact, or distribution group that can be included in the compliance report.   
3. The system has access to the Email Archive, Audit Record, and Email Contact Distribution Group modules for data retrieval.   
  
Postconditions:   
1. A compliance report is generated and displayed to the Administrator.   
2. The report includes relevant data from the Email Archive, Audit Record, and Email Contact Distribution Group.   
3. The system logs the compliance report generation in the Audit Record.   
  
Main Flow:   
1. The Administrator selects the "Generate Compliance Report" option from the system interface.   
2. The system prompts the Administrator to select the scope of the report (e.g., date range, specific email account, distribution group, or contact).   
3. The Administrator selects the required criteria and confirms the report generation.   
4. The system retrieves relevant data from the Email Archive, Audit Record, and Email Contact Distribution Group based on the selected criteria.   
5. The system compiles the data into a structured compliance report.   
6. The system generates an Audit Record for the compliance report generation event.   
7. The system displays the compliance report to the Administrator in a readable format.   
8. The Administrator can download or print the report as needed.   
  
Alternative Flow:   
1. If no data is available based on the selected criteria, the system displays a message indicating that the report cannot be generated.   
2. If the selected criteria is invalid or incomplete, the system displays an error message and prompts the Administrator to provide valid inputs.   
3. If the system fails to retrieve data from the Email Archive or Audit Record, it displays an error message and prompts the Administrator to check the system configuration or retry the operation.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the report was generated but the audit process may be incomplete.  
  
Use Case Name: Update Email   
Use Case ID: UC-24   
Actors: Administrator, Email Archive, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the system.   
2. The email to be updated already exists in the system.   
3. The system has access to the Email Archive and Audit Record modules for logging and storage.   
4. The email is not currently being processed or locked by the system.   
  
Postconditions:   
1. The selected email is successfully updated with the new content or metadata.   
2. The updated email is saved in the system.   
3. A copy of the updated email is archived in the Email Archive.   
4. An Audit Record is created documenting the email update process.   
  
Main Flow:   
1. The Administrator selects the "Update Email" option from the system interface.   
2. The system displays a list of existing emails for the Administrator to choose from.   
3. The Administrator selects the email they wish to update.   
4. The system retrieves the email content and metadata and displays it in an editable form.   
5. The Administrator modifies the necessary information (e.g., subject, body, or recipient list).   
6. The Administrator submits the updated email information.   
7. The system validates the updated email content and metadata (e.g., checks for valid subject or body content).   
8. The system updates the email in the system.   
9. The system archives the updated email in the Email Archive.   
10. The system generates an Audit Record for the email update event.   
11. The system confirms the successful update of the email and displays the updated information to the Administrator.   
  
Alternative Flow:   
1. If the selected email does not exist, the system displays an error message and prompts the Administrator to select a valid email.   
2. If the updated email content is invalid (e.g., missing subject or body), the system displays an error message and prompts the Administrator to correct the information.   
3. If the system fails to save the updated email, it displays an error message and prompts the Administrator to retry the operation.   
4. If the system fails to archive the updated email, it logs an internal error and notifies the Administrator that the email was updated but the archive process may be incomplete.   
5. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was updated but the audit process may be incomplete.  
  
Use Case Name: Delete Email Archive   
Use Case ID: UC-25   
Actors: Administrator, Email Archive, Audit Record   
  
Preconditions:   
1. The Administrator is authenticated and has access to the Email Archive module.   
2. The Email Archive contains at least one email that can be deleted.   
3. The system is configured to allow deletion of archived emails.   
4. The system has access to the Audit Record module for logging the deletion process.   
  
Postconditions:   
1. The selected email is permanently deleted from the Email Archive.   
2. The system logs the deletion action in the Audit Record.   
3. The Email Archive is updated to reflect the removal of the email.   
  
Main Flow:   
1. The Administrator selects the "Delete Email Archive" option from the system interface.   
2. The system displays a list of emails currently stored in the Email Archive.   
3. The Administrator selects the specific email they wish to delete from the archive.   
4. The system confirms the deletion with the Administrator.   
5. The system permanently deletes the selected email from the Email Archive.   
6. The system generates an Audit Record for the deletion event.   
7. The system confirms the successful deletion of the email and updates the Email Archive accordingly.   
  
Alternative Flow:   
1. If the selected email does not exist in the Email Archive, the system displays an error message and prompts the Administrator to select a valid email.   
2. If the Administrator cancels the deletion during the confirmation step, the system returns to the main interface without making any changes.   
3. If the system fails to delete the email (e.g., due to permissions or system constraints), it displays an error message and prompts the Administrator to retry the operation or resolve the issue.   
4. If the Audit Record fails to be created, the system logs an internal error and notifies the Administrator that the email was deleted but the audit process may be incomplete.