项目文档

# Functional Requirement

1.1 Email Creation Function   
 Function ID: FR-01   
 Description: The system allows the Administrator to create a new Email using an Email Template and send it via a selected Email Account to a Distribution Group.   
 Input: Distribution Group, Email Template, customized email content, selected Email Account.   
 Output: A new Email with associated Email Account and Distribution Group, a Compliance Audit Record of the creation, and a success message to the Administrator.  
  
1.2 Email Sending Function   
 Function ID: FR-02   
 Description: The system allows the Administrator to send an Email that has been created and is associated with a valid Email Account and Distribution Group.   
 Input: Selected Email, associated Distribution Group, Email Account, Compliance Audit Record.   
 Output: The Email is sent to all recipients in the Distribution Group, archived, and the Compliance Audit Record is updated with the sending details.  
  
1.3 Email Receiving Function   
 Function ID: FR-03   
 Description: The system can detect, validate, and store incoming Emails via configured Email Accounts. It also archives the Email and updates the Compliance Audit Record.   
 Input: Incoming Email, Email Account.   
 Output: A new Email stored in the system, archived in the Email Archive, and a Compliance Audit Record updated with the receipt details. A notification is sent to the Administrator.  
  
1.4 Email Reading Function   
 Function ID: FR-04   
 Description: The system allows the Administrator to view the content of an Email stored in the Email Archive, along with its Compliance Audit Record.   
 Input: Selected Email from the Email Archive.   
 Output: Displayed Email content and Compliance Audit Record details. The system logs the view action.  
  
1.5 Email Deletion Function   
 Function ID: FR-05   
 Description: The system allows the Administrator to delete an Email from the Email Archive and update the Compliance Audit Record accordingly.   
 Input: Selected Email from the Email Archive, confirmation for deletion.   
 Output: The Email is removed from the system, and the Compliance Audit Record is updated with the deletion details. A confirmation message is displayed.  
  
1.6 Email Archiving Function   
 Function ID: FR-06   
 Description: The system allows the Administrator to manually archive an Email to the Email Archive and update the Compliance Audit Record with the archiving details.   
 Input: Selected Email, confirmation for archiving.   
 Output: The Email is moved to the Email Archive, and the Compliance Audit Record is updated with the archiving timestamp and details.  
  
1.7 Email Recovery Function   
 Function ID: FR-07   
 Description: The system allows the Administrator to recover an Email from the Email Archive and restore it to active email storage.   
 Input: Selected Email from the Email Archive, confirmation for recovery.   
 Output: The Email is restored to active storage, and the Compliance Audit Record is updated with the recovery details.  
  
1.8 Contact Creation Function   
 Function ID: FR-08   
 Description: The system allows the Administrator to create a new Contact and associate it with a Distribution Group.   
 Input: Contact name, email address, phone number, address, and associated Distribution Group.   
 Output: A new Contact stored in the system, associated with the correct Distribution Group, and a Compliance Audit Record updated with the creation details.  
  
1.9 Contact Update Function   
 Function ID: FR-09   
 Description: The system allows the Administrator to modify an existing Contact’s information and update its associated Distribution Group.   
 Input: Selected Contact, updated details (e.g., name, email, phone number), and updated Distribution Group.   
 Output: The Contact is updated in the system, associated with the correct Distribution Group, and the Compliance Audit Record is updated with the modification details.  
  
1.10 Contact Deletion Function   
 Function ID: FR-10   
 Description: The system allows the Administrator to delete an existing Contact and update the Compliance Audit Record accordingly.   
 Input: Selected Contact, confirmation for deletion.   
 Output: The Contact is removed from the system, the Compliance Audit Record is updated with the deletion details, and a confirmation message is displayed.  
  
1.11 Contact Viewing Function   
 Function ID: FR-11   
 Description: The system allows the Administrator to view the details of an existing Contact, including its associated Distribution Group and Compliance Audit Record.   
 Input: Selected Contact.   
 Output: Displayed Contact information, associated Distribution Group details, and Compliance Audit Record (if available). The view action is logged.  
  
1.12 Distribution Group Creation Function   
 Function ID: FR-12   
 Description: The system allows the Administrator to create a new Distribution Group and add one or more Contacts to it.   
 Input: Group name, description, and list of Contacts to include.   
 Output: A new Distribution Group stored in the system, with associated Contacts and a Compliance Audit Record updated with the creation details.  
  
1.13 Distribution Group Update Function   
 Function ID: FR-13   
 Description: The system allows the Administrator to update the name, description, and membership of an existing Distribution Group.   
 Input: Selected Distribution Group, updated name and description, modified list of Contacts.   
 Output: The updated Distribution Group is saved in the system, Compliance Audit Record is updated with the modification details.  
  
1.14 Distribution Group Deletion Function   
 Function ID: FR-14   
 Description: The system allows the Administrator to delete a Distribution Group and disassociate its Contacts.   
 Input: Selected Distribution Group, confirmation for deletion.   
 Output: The Distribution Group is removed from the system, associated Contacts are disassociated, and the Compliance Audit Record is updated with the deletion details.  
  
1.15 Distribution Group Viewing Function   
 Function ID: FR-15   
 Description: The system allows the Administrator to view the details of an existing Distribution Group, including its members and Compliance Audit Record.   
 Input: Selected Distribution Group.   
 Output: Displayed group name, description, associated Contacts, and Compliance Audit Record (if available). The view action is logged.  
  
1.16 Email Account Registration Function   
 Function ID: FR-16   
 Description: The system allows the Administrator to register a new Email Account, including email address, password, and server configuration.   
 Input: Email address, password, server configuration details.   
 Output: A new Email Account registered in the system, with a Compliance Audit Record updated with the registration details.  
  
1.17 Email Account Modification Function   
 Function ID: FR-17   
 Description: The system allows the Administrator to modify the details of an existing Email Account, such as password or server configuration.   
 Input: Selected Email Account, updated details (e.g., password, server configuration).   
 Output: The Email Account is updated in the system, and the Compliance Audit Record is updated with the modification details.  
  
1.18 Email Account Deletion Function   
 Function ID: FR-18   
 Description: The system allows the Administrator to delete an existing Email Account and update the Compliance Audit Record accordingly.   
 Input: Selected Email Account, confirmation for deletion.   
 Output: The Email Account is removed from the system, and the Compliance Audit Record is updated with the deletion details.  
  
1.19 Email Account Viewing Function   
 Function ID: FR-19   
 Description: The system allows the Administrator to view the details of an Email Account, including its server configuration and status.   
 Input: Selected Email Account.   
 Output: Displayed Email Account information, and Compliance Audit Record (if available). The view action is logged.  
  
1.20 Email Template Management Function   
 Function ID: FR-20   
 Description: The system allows the Administrator to create, update, or delete an Email Template.   
 Input: Selected action (create, update, delete), template name, subject, body content, and metadata (for create/update).   
 Output: The Email Template is created, updated, or deleted, and the Compliance Audit Record is updated accordingly.  
  
1.21 Email Template Creation Function   
 Function ID: FR-21   
 Description: The system allows the Administrator to create a new Email Template, including name, subject, body, and metadata.   
 Input: Template name, subject, body content, and metadata.   
 Output: A new Email Template stored in the system, with a Compliance Audit Record updated with the creation details.  
  
1.22 Email Template Update Function   
 Function ID: FR-22   
 Description: The system allows the Administrator to update an existing Email Template’s content or metadata.   
 Input: Selected Email Template, updated fields (e.g., name, subject, body content).   
 Output: The Email Template is updated in the system, and the Compliance Audit Record is updated with the modification details.  
  
1.23 Email Template Deletion Function   
 Function ID: FR-23   
 Description: The system allows the Administrator to delete an existing Email Template and update the Compliance Audit Record accordingly.   
 Input: Selected Email Template, confirmation for deletion.   
 Output: The Email Template is removed from the system, and the Compliance Audit Record is updated with the deletion details.  
  
1.24 Email Status Logging Function   
 Function ID: FR-24   
 Description: The system logs status changes of Emails (e.g., sent, received, read, deleted) in the Email Status Log.   
 Input: Email status change (e.g., "Sent", "Failed"), associated Email, timestamp, and description.   
 Output: A new or updated Email Status Log entry stored in the system, and the Compliance Audit Record updated with the action details.  
  
1.25 Email Status Log Management Function   
 Function ID: FR-25   
 Description: The system allows the Administrator to create, update, or delete an Email Status Log entry.   
 Input: Selected action (create, update, delete), Email, status, timestamp, and notes.   
 Output: The Email Status Log is created, updated, or deleted, and the Compliance Audit Record is updated accordingly.  
  
1.26 Compliance Audit Record Viewing Function   
 Function ID: FR-26   
 Description: The system allows the Administrator to view the details of a Compliance Audit Record, including the associated Email, Contact, or Distribution Group.   
 Input: Selected Compliance Audit Record.   
 Output: Displayed audit record details, including action type, timestamp, and related entities. The view action is logged.  
  
1.27 Compliance Audit Report Generation Function   
 Function ID: FR-27   
 Description: The system allows the Administrator to generate a Compliance Audit Report based on selected records and associated entities.   
 Input: Time range or specific Compliance Audit Records, selected report format (e.g., PDF, CSV).   
 Output: A generated Compliance Audit Report displayed to the Administrator, and the system logs the report generation action.  
  
1.28 Email Archive Record Management Function   
 Function ID: FR-28   
 Description: The system allows the Administrator to create, update, or delete an Email Archive Record, linking it to the Email and Compliance Audit Record.   
 Input: Selected action (create, update, delete), Email, archive date, recovery date, and status.   
 Output: The Email Archive Record is created, updated, or deleted, and the Compliance Audit Record is updated accordingly.  
  
1.29 Email Folder Management Function   
 Function ID: FR-29   
 Description: The system allows the Administrator to create, update, or delete an Email Folder to organize Emails.   
 Input: Selected action (create, update, delete), folder name, description, and parent folder (if applicable).   
 Output: The Email Folder is created, updated, or deleted, and the Compliance Audit Record is updated accordingly. Emails are reorganized if necessary.  
  
1.30 Email Update Function   
 Function ID: FR-30   
 Description: The system allows the Administrator to update an existing Email’s content, associated Email Account, or Distribution Group.   
 Input: Selected Email, updated content, Email Account, Distribution Group.   
 Output: The Email is updated in the system, and the Compliance Audit Record is updated with the modification details.  
  
1.31 Notification Management Function   
 Function ID: FR-31   
 Description: The system allows the Administrator to create, update, or delete a Notification, linking it to Email Accounts and Compliance Audit Records.   
 Input: Selected action (create, update, delete), notification title, message, target Email Account, and event trigger conditions.   
 Output: The Notification is created, updated, or deleted, and the Compliance Audit Record is updated accordingly.

# External Description

# 2. External Interfaces   
  
This section defines the external interfaces that the system interacts with, including user interfaces, hardware interfaces (if any), software interfaces (including databases and third-party tools), and communication interfaces. These interfaces are identified and described based on the inputs, outputs, and external data sources referenced in the functional requirements.   
  
## 2.1 User Interface Output   
  
The system interacts with the \*\*Administrator\*\* through a \*\*graphical user interface (GUI)\*\*. This interface allows the Administrator to perform various actions such as creating, sending, reading, updating, archiving, and deleting Emails, Contacts, Distribution Groups, Email Accounts, Email Templates, and Notifications. The interface also provides access to Compliance Audit Records and Email Archive Records.   
  
### 2.1.1 Email Management Interface   
- \*\*Description\*\*: A screen where the Administrator can create, update, or delete Emails.   
- \*\*Inputs\*\*:   
 - Distribution Group selection   
 - Email Template selection   
 - Customized email content   
 - Email Account selection   
- \*\*Outputs\*\*:   
 - Display of the created or modified Email   
 - Compliance Audit Record of the action   
 - Success or confirmation messages   
 - Email Status Log updates   
  
### 2.1.2 Contact Management Interface   
- \*\*Description\*\*: A screen for managing Contacts, including creating, updating, deleting, and viewing them.   
- \*\*Inputs\*\*:   
 - Contact name, email, phone, address   
 - Distribution Group association   
- \*\*Outputs\*\*:   
 - Display of Contact details   
 - Compliance Audit Record updates   
 - Confirmation messages   
  
### 2.1.3 Distribution Group Management Interface   
- \*\*Description\*\*: A screen for managing Distribution Groups, including creating, updating, deleting, and viewing groups and their members.   
- \*\*Inputs\*\*:   
 - Group name and description   
 - List of Contacts to add or remove   
- \*\*Outputs\*\*:   
 - Display of group details and members   
 - Compliance Audit Record updates   
  
### 2.1.4 Email Account Management Interface   
- \*\*Description\*\*: A screen for registering, modifying, or deleting Email Accounts.   
- \*\*Inputs\*\*:   
 - Email address, password, and server configuration   
- \*\*Outputs\*\*:   
 - Display of account details and server status   
 - Compliance Audit Record updates   
  
### 2.1.5 Email Template Management Interface   
- \*\*Description\*\*: A screen for creating, updating, or deleting Email Templates.   
- \*\*Inputs\*\*:   
 - Template name, subject, body, and metadata   
- \*\*Outputs\*\*:   
 - Display of updated or created templates   
 - Compliance Audit Record updates   
  
### 2.1.6 Compliance Audit Interface   
- \*\*Description\*\*: A screen for viewing Compliance Audit Records and generating Compliance Audit Reports.   
- \*\*Inputs\*\*:   
 - Selection of audit records or time range   
 - Report format (e.g., PDF, CSV)   
- \*\*Outputs\*\*:   
 - Display of audit details (action type, timestamp, related entities)   
 - Generated Compliance Audit Reports   
 - Logging of view actions   
  
### 2.1.7 Email Archive Management Interface   
- \*\*Description\*\*: A screen for viewing and managing archived Emails, including recovery and deletion of archive records.   
- \*\*Inputs\*\*:   
 - Selected Email for archiving or recovery   
 - Archive date, recovery date, and status   
- \*\*Outputs\*\*:   
 - Display of Email Archive Records   
 - Confirmation of archiving or recovery   
 - Compliance Audit Record updates   
  
### 2.1.8 Email Folder Management Interface   
- \*\*Description\*\*: A screen for managing Email Folders, including creating, updating, and deleting folders and reorganizing Emails.   
- \*\*Inputs\*\*:   
 - Folder name, description, and parent folder   
- \*\*Outputs\*\*:   
 - Updated folder structure   
 - Compliance Audit Record updates   
  
### 2.1.9 Notification Management Interface   
- \*\*Description\*\*: A screen for managing Notifications, including creating, updating, and deleting notification settings.   
- \*\*Inputs\*\*:   
 - Notification title, message, target Email Account   
 - Event trigger conditions   
- \*\*Outputs\*\*:   
 - Display of notification settings   
 - Compliance Audit Record updates   
  
---  
  
## 2.2 Hardware Interface Output   
  
No hardware interfaces are required for the system as described in the provided functional requirements. The system is expected to operate on standard server and desktop hardware without direct interaction with physical hardware devices.   
  
---  
  
## 2.3 Software Interface Output   
  
The system interacts with several \*\*software components\*\*, including \*\*databases\*\*, \*\*third-party tools\*\*, and \*\*internal modules\*\*. These are essential for data storage, retrieval, and processing.   
  
### 2.3.1 Email Archive Database   
- \*\*Description\*\*: A database that stores archived Email records, including metadata such as archive date, recovery date, and status.   
- \*\*Interaction Method\*\*:   
 - \*\*Create\*\*: When an Email is archived manually or after sending/receiving, the system inserts a new record into the Email Archive Database.   
 - \*\*Read\*\*: When an Email is viewed or recovered, the system retrieves the relevant archive record.   
 - \*\*Update\*\*: When an Email is recovered or marked as deleted, the system updates the archive record.   
 - \*\*Delete\*\*: When an Email Archive Record is deleted, the system removes it from the database.   
- \*\*Data Format\*\*: Structured data with fields such as `EmailID`, `ArchiveDate`, `RecoveryDate`, `Status`, and `ComplianceAuditID`.   
  
### 2.3.2 Compliance Audit Database   
- \*\*Description\*\*: A database that logs all system actions related to Emails, Contacts, Distribution Groups, Email Accounts, Templates, and Notifications.   
- \*\*Interaction Method\*\*:   
 - \*\*Create\*\*: When a new Email, Contact, Distribution Group, Email Account, Template, or Notification is created, the system inserts a new audit record.   
 - \*\*Update\*\*: When any entity is modified, the system updates the audit record with the modification details.   
 - \*\*Delete\*\*: When an entity is deleted, the system updates the audit record with the deletion details.   
- \*\*Data Format\*\*: Structured data with fields such as `ActionType`, `Timestamp`, `EntityID`, `EntityName`, and `Description`.   
  
### 2.3.3 Email Status Log Database   
- \*\*Description\*\*: A database that logs the status of Emails (e.g., sent, received, read, failed, deleted).   
- \*\*Interaction Method\*\*:   
 - \*\*Create/Update\*\*: When an Email status changes, the system inserts or updates a record in the Email Status Log Database.   
- \*\*Data Format\*\*: Structured data with fields such as `EmailID`, `Status`, `Timestamp`, and `Notes`.   
  
### 2.3.4 Email Account Configuration Module   
- \*\*Description\*\*: A module or database that stores configuration details of Email Accounts, including server settings (SMTP/IMAP), authentication credentials, and status (e.g., active, inactive).   
- \*\*Interaction Method\*\*:   
 - \*\*Create\*\*: When a new Email Account is registered, its details are stored in the configuration module.   
 - \*\*Read\*\*: When viewing or sending emails, the system retrieves the account’s configuration.   
 - \*\*Update/Delete\*\*: When an Email Account is modified or deleted, the system updates or removes the configuration accordingly.   
- \*\*Data Format\*\*: Structured data with fields such as `EmailID`, `ServerType`, `ServerAddress`, `Port`, `Username`, `Password`, `Status`.   
  
### 2.3.5 Email Template Storage Module   
- \*\*Description\*\*: A module or database for storing Email Templates, including the name, subject, body content, and metadata.   
- \*\*Interaction Method\*\*:   
 - \*\*Create\*\*: When a new Email Template is created, it is stored in this module.   
 - \*\*Read/Update/Delete\*\*: When templates are used, modified, or deleted, the system interacts with this module.   
- \*\*Data Format\*\*: Structured data with fields such as `TemplateName`, `Subject`, `BodyContent`, `Metadata`, `LastModified`.   
  
### 2.3.6 Contact Database   
- \*\*Description\*\*: A database that stores Contact information, including name, email, phone number, address, and association with Distribution Groups.   
- \*\*Interaction Method\*\*:   
 - \*\*Create\*\*: When a new Contact is added, its details are stored in the database.   
 - \*\*Read/Update/Delete\*\*: When viewing, modifying, or removing a Contact, the system retrieves or modifies the database.   
- \*\*Data Format\*\*: Structured data with fields such as `ContactID`, `Name`, `Email`, `Phone`, `Address`, `DistributionGroupID`.   
  
### 2.3.7 Distribution Group Database   
- \*\*Description\*\*: A database that stores Distribution Groups, including name, description, and list of associated Contacts.   
- \*\*Interaction Method\*\*:   
 - \*\*Create\*\*: When a new group is created, its details are stored in the database.   
 - \*\*Read/Update/Delete\*\*: When viewing, modifying, or deleting a group, the system interacts with the database.   
- \*\*Data Format\*\*: Structured data with fields such as `GroupID`, `GroupName`, `Description`, `ContactIDs`.   
  
---  
  
## 2.4 Communication Interface Output   
  
The system uses \*\*communication interfaces\*\* to interact with external services and to send and receive emails.   
  
### 2.4.1 Email Communication Interface   
- \*\*Description\*\*: The system uses this interface to send and receive emails via configured Email Accounts.   
- \*\*Protocols\*\*:   
 - \*\*SMTP (Simple Mail Transfer Protocol)\*\*: Used for sending emails.   
 - \*\*IMAP (Internet Message Access Protocol)\*\*: Used for receiving and retrieving emails.   
- \*\*Inputs\*\*:   
 - Email content (from Email Templates or customized input)   
 - Email Account credentials and server configuration   
 - Distribution Group of recipients   
- \*\*Outputs\*\*:   
 - Sent Emails to recipients in the Distribution Group   
 - Received Emails stored in the system   
 - Email Status Log updates (e.g., "Sent", "Failed")   
 - Compliance Audit Record updates   
  
### 2.4.2 Email Notification Interface   
- \*\*Description\*\*: The system sends notifications to the Administrator via the configured Email Accounts for events such as email receipt, deletion, or archive.   
- \*\*Inputs\*\*:   
 - Notification content (title, message)   
 - Target Email Account for sending the notification   
- \*\*Outputs\*\*:   
 - Email notification sent to the Administrator   
 - Compliance Audit Record of the notification action   
  
### 2.4.3 Email Archive Communication Interface   
- \*\*Description\*\*: The system communicates with an email archive system or external storage to archive and retrieve Emails.   
- \*\*Inputs\*\*:   
 - Email to be archived   
 - Archive date and status   
- \*\*Outputs\*\*:   
 - Archived Email stored in the system   
 - Archive record updated in the Email Archive Database   
 - Compliance Audit Record updates   
  
---  
  
This section has been carefully constructed to align with the functional requirements and ensure that all referenced data sources (e.g., Email Archive, Compliance Audit, Email Status Log, Contact Database, etc.) are clearly defined and categorized under the appropriate interface type. Developers can use this section to understand how the system interacts with external entities and how to structure the necessary integrations.

# Use Case

Use Case Name: Create Email   
Use Case ID: UC-01   
Actors: Administrator, Email Account   
Preconditions:   
1. The Administrator is logged into the system.   
2. The system has at least one Email Account configured.   
3. The Administrator has access to the Email Template and Compliance Audit Record features.   
  
Postconditions:   
1. A new Email is created and stored in the system.   
2. The Email is associated with the selected Email Account and Distribution Group.   
3. The Compliance Audit Record is updated with the creation details.   
  
Main Flow:   
1. The Administrator navigates to the "Create Email" interface.   
2. The Administrator selects a Distribution Group for the email recipients.   
3. The Administrator chooses an Email Template to use as a basis for the email.   
4. The Administrator customizes the email content as needed.   
5. The Administrator selects the appropriate Email Account to send the email from.   
6. The Administrator confirms the email details and clicks "Send".   
7. The system generates the email, attaches any required compliance information, and sends it using the selected Email Account.   
8. The system creates a new Compliance Audit Record for the email.   
9. The system displays a success message to the Administrator.   
  
Alternative Flow:   
1. If no Distribution Group is selected, the system displays an error message and prompts the Administrator to select one.   
2. If no Email Template is selected, the system allows the Administrator to manually compose the email content.   
3. If no Email Account is selected, the system displays an error message and prompts the Administrator to choose one.   
4. If the email content is not valid or incomplete, the system displays an error message and prompts the Administrator to correct it.   
5. If the email fails to send, the system logs the error and displays a failure message to the Administrator.  
  
Use Case Name: Send Email   
Use Case ID: UC-02   
Actors: Administrator, Email Account, Email Template, Distribution Group   
Preconditions:   
1. The Administrator is logged into the system.   
2. A new Email has been created and is ready for sending.   
3. The Email is associated with a valid Distribution Group and Email Account.   
4. The Compliance Audit Record has been created and linked to the Email.   
  
Postconditions:   
1. The Email is successfully sent to the recipients in the selected Distribution Group.   
2. The Compliance Audit Record is updated with the sending details.   
3. The system archives the sent Email for future reference.   
  
Main Flow:   
1. The Administrator selects the Email to be sent from the list of created Emails.   
2. The system confirms the associated Distribution Group and Email Account.   
3. The Administrator reviews the email content and confirms the send action.   
4. The system attaches the Compliance Audit Record and finalizes the email.   
5. The system sends the email using the selected Email Account.   
6. The system archives the sent Email.   
7. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the selected Email Account is not valid, the system displays an error and prompts the Administrator to select a valid one.   
2. If the Compliance Audit Record is missing or incomplete, the system prevents sending and prompts the Administrator to complete it.   
3. If the email fails to send, the system logs the failure and displays an error message to the Administrator.   
4. If the Administrator cancels the send action, the system returns to the email review interface without sending.  
  
Use Case Name: Receive Email   
Use Case ID: UC-03   
Actors: Administrator, Email Account, Email Archive, Compliance Audit Record   
Preconditions:   
1. The system is configured to monitor and receive emails via at least one Email Account.   
2. The Administrator has access to the email receiving functionality.   
3. The system is capable of archiving received emails and updating the Compliance Audit Record.   
  
Postconditions:   
1. A new email is received and stored in the system.   
2. The received Email is archived for future reference.   
3. The Compliance Audit Record is updated with the receipt details.   
  
Main Flow:   
1. The system detects an incoming email via the configured Email Account.   
2. The system verifies the email format and content for compliance.   
3. The system archives the received Email in the Email Archive.   
4. The system creates or updates a Compliance Audit Record with the receipt details.   
5. The system notifies the Administrator of the received email.   
6. The Administrator reviews the email and its audit record as needed.   
  
Alternative Flow:   
1. If the incoming email fails compliance checks, the system logs the issue and does not archive the email.   
2. If no valid Email Account is configured for receiving, the system logs the failure and does not process the email.   
3. If the system fails to archive the email, the Compliance Audit Record is not updated, and an error message is displayed to the Administrator.   
4. If the notification to the Administrator fails, the system logs the failure and retries at a later time.  
  
Use Case Name: Read Email   
Use Case ID: UC-04   
Actors: Administrator, Email Archive, Email   
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email exists in the Email Archive.   
3. The Administrator has access to the "Read Email" functionality.   
  
Postconditions:   
1. The Administrator can view the content of the selected Email.   
2. The Compliance Audit Record for the Email is accessed if needed.   
3. The system logs the read action for the Email.   
  
Main Flow:   
1. The Administrator navigates to the "Email Archive" interface.   
2. The Administrator selects an Email from the list to read.   
3. The system retrieves the Email and its associated Compliance Audit Record.   
4. The system displays the Email content and audit details to the Administrator.   
5. The system logs the read action in the Compliance Audit Record.   
  
Alternative Flow:   
1. If the selected Email is not found, the system displays an error message.   
2. If the Compliance Audit Record is missing, the system alerts the Administrator and displays only the email content.   
3. If the system fails to retrieve the Email, an error message is displayed, and the Administrator is prompted to try again.  
  
Use Case Name: Delete Email   
Use Case ID: UC-05   
Actors: Administrator, Email Archive, Email   
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email exists in the Email Archive.   
3. The Administrator has the necessary permissions to delete emails.   
  
Postconditions:   
1. The selected Email is removed from the system.   
2. The Compliance Audit Record for the deleted Email is updated to reflect the deletion.   
3. The system logs the deletion action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Archive" interface.   
2. The Administrator selects an Email to be deleted.   
3. The system confirms the selection and prompts the Administrator for confirmation.   
4. The Administrator confirms the deletion.   
5. The system removes the Email from the Email Archive.   
6. The system updates the Compliance Audit Record to indicate the deletion.   
7. The system logs the deletion action.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the selected Email is not found, the system displays an error message.   
2. If the Administrator cancels the deletion, the system returns to the Email Archive interface without making changes.   
3. If the deletion fails due to system constraints, the system displays an error message and logs the failure.  
  
Use Case Name: Archive Email   
Use Case ID: UC-06   
Actors: Administrator, Email, Email Archive, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email exists in the system and has been sent or received.   
3. The system has an Email Archive configured.   
4. The Compliance Audit Record for the Email is available.   
  
Postconditions:   
1. The selected Email is archived in the Email Archive.   
2. The Compliance Audit Record is updated with the archiving details.   
3. The system logs the archiving action.   
  
Main Flow:   
1. The Administrator navigates to the "Archive Email" interface.   
2. The Administrator selects an Email to be archived from the list of available emails.   
3. The system verifies that the Email has a valid Compliance Audit Record.   
4. The system moves the Email to the Email Archive.   
5. The system updates the Compliance Audit Record with the archiving timestamp and details.   
6. The system logs the archiving action.   
7. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the selected Email does not have a valid Compliance Audit Record, the system displays a warning and prompts the Administrator to review it before proceeding.   
2. If the Email is already archived, the system alerts the Administrator and does not perform any action.   
3. If the system fails to move the Email to the archive, an error message is displayed, and the action is logged.   
4. If the Administrator cancels the archiving action, the system returns to the email list without making changes.  
  
Use Case Name: Recover Email   
Use Case ID: UC-07   
Actors: Administrator, Email Archive, Email, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email exists in the Email Archive.   
3. The Administrator has the necessary permissions to recover emails.   
4. The system supports restoring emails from the archive to the active email storage.   
  
Postconditions:   
1. The selected Email is restored from the Email Archive to the active email storage.   
2. The Compliance Audit Record is updated to reflect the recovery action.   
3. The system logs the recovery action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Archive" interface.   
2. The Administrator selects an Email to be recovered.   
3. The system confirms the selection and prompts the Administrator for recovery confirmation.   
4. The Administrator confirms the recovery action.   
5. The system retrieves the selected Email from the archive.   
6. The system restores the Email to the active email storage.   
7. The system updates the Compliance Audit Record to indicate the recovery.   
8. The system logs the recovery action.   
9. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the selected Email is not found in the archive, the system displays an error message.   
2. If the Administrator cancels the recovery action, the system returns to the Email Archive interface without making changes.   
3. If the recovery fails due to system constraints, the system displays an error message and logs the failure.  
  
Use Case Name: Create Contact   
Use Case ID: UC-08   
Actors: Administrator   
Preconditions:   
1. The Administrator is logged into the system.   
2. The system allows the creation of new contacts.   
3. The Administrator has the necessary permissions to create contacts.   
  
Postconditions:   
1. A new Contact is created and stored in the system.   
2. The system logs the creation action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Create Contact" interface.   
2. The Administrator enters the contact details, including name, email address, and any relevant attributes.   
3. The Administrator selects the appropriate Distribution Group for the contact.   
4. The Administrator confirms the details and clicks "Save".   
5. The system validates the contact information and creates the Contact.   
6. The system logs the creation action in the Compliance Audit Record.   
7. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the contact details are incomplete or invalid, the system displays an error message and prompts the Administrator to correct them.   
2. If no Distribution Group is selected, the system displays a warning and allows the Administrator to assign one after saving.   
3. If the email address is already associated with an existing contact, the system alerts the Administrator and suggests reviewing the existing contact.   
4. If the Administrator cancels the operation, the system returns to the contact management interface without creating the contact.  
  
Use Case Name: Update Contact   
Use Case ID: UC-09   
Actors: Administrator, Contact, Distribution Group, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. A Contact already exists in the system.   
3. The Administrator has the necessary permissions to update contacts.   
4. The system supports updating Contact information and updating the Compliance Audit Record accordingly.   
  
Postconditions:   
1. The Contact's information is updated in the system.   
2. The updated Contact is associated with the correct Distribution Group.   
3. The Compliance Audit Record is updated to reflect the changes.   
4. The system logs the update action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Contact Management" interface.   
2. The Administrator selects an existing Contact to update.   
3. The system displays the current Contact details.   
4. The Administrator modifies the necessary fields (e.g., name, email address, attributes).   
5. The Administrator selects or updates the associated Distribution Group for the Contact.   
6. The Administrator confirms the changes and clicks "Update".   
7. The system validates the updated information.   
8. The system updates the Contact and logs the changes in the Compliance Audit Record.   
9. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the updated contact details are incomplete or invalid, the system displays an error message and prompts the Administrator to correct them.   
2. If no Distribution Group is selected, the system displays a warning and allows the Administrator to assign one after saving.   
3. If the updated email address is already associated with another existing Contact, the system alerts the Administrator and suggests reviewing the existing Contact.   
4. If the Administrator cancels the update operation, the system returns to the contact management interface without making changes.   
5. If the Compliance Audit Record update fails, the system logs the error and displays a warning message to the Administrator.  
  
Use Case Name: Delete Contact   
Use Case ID: UC-10   
Actors: Administrator, Contact, Distribution Group, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. A Contact exists in the system and is associated with a Distribution Group.   
3. The Administrator has the necessary permissions to delete contacts.   
4. The system supports updating the Compliance Audit Record when a Contact is deleted.   
  
Postconditions:   
1. The selected Contact is removed from the system.   
2. The Compliance Audit Record is updated with the deletion details.   
3. The system logs the deletion action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Contact Management" interface.   
2. The Administrator selects a Contact to be deleted.   
3. The system confirms the selection and prompts the Administrator for deletion confirmation.   
4. The Administrator confirms the deletion.   
5. The system removes the Contact from the system and updates the associated Distribution Group.   
6. The system updates the Compliance Audit Record to indicate the deletion.   
7. The system logs the deletion action.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the selected Contact is not found, the system displays an error message.   
2. If the Administrator cancels the deletion, the system returns to the Contact Management interface without making changes.   
3. If the deletion fails due to system constraints (e.g., Contact is linked to an active Email), the system displays an error message and logs the failure.  
  
Use Case Name: View Contact   
Use Case ID: UC-11   
Actors: Administrator, Contact, Distribution Group, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. At least one Contact exists in the system.   
3. The Administrator has the necessary permissions to view contacts.   
4. The system can retrieve Contact details and related information.   
  
Postconditions:   
1. The Administrator can view the details of the selected Contact.   
2. The associated Distribution Group information is displayed if applicable.   
3. The Compliance Audit Record for the Contact is accessed and displayed if available.   
4. The system logs the view action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Contact Management" interface.   
2. The Administrator selects a Contact from the list to view.   
3. The system retrieves the Contact details, including name, email address, and attributes.   
4. The system displays the Contact information to the Administrator.   
5. If the Contact is associated with a Distribution Group, the system shows the group details.   
6. The system retrieves and displays the Compliance Audit Record for the Contact, if available.   
7. The system logs the view action in the Compliance Audit Record.   
  
Alternative Flow:   
1. If the selected Contact is not found, the system displays an error message.   
2. If the Compliance Audit Record is missing, the system alerts the Administrator and displays only the Contact information.   
3. If the system fails to retrieve the Contact details, an error message is displayed, and the Administrator is prompted to try again.   
4. If the Administrator cancels the view action, the system returns to the Contact Management interface without displaying additional information.  
  
Use Case Name: Create Distribution Group   
Use Case ID: UC-12   
Actors: Administrator   
Preconditions:   
1. The Administrator is logged into the system.   
2. The system allows the creation of new Distribution Groups.   
3. The Administrator has the necessary permissions to create Distribution Groups.   
  
Postconditions:   
1. A new Distribution Group is created and stored in the system.   
2. The Compliance Audit Record is updated with the creation details.   
3. The system logs the creation action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Create Distribution Group" interface.   
2. The Administrator enters the name and description of the new Distribution Group.   
3. The Administrator adds one or more Contacts to the group.   
4. The Administrator confirms the details and clicks "Save".   
5. The system validates the group information and creates the Distribution Group.   
6. The system logs the creation action in the Compliance Audit Record.   
7. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the group name is missing or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If no Contacts are added to the group, the system displays a warning but allows the group to be created with no members.   
3. If the Administrator cancels the operation, the system returns to the Distribution Group management interface without making changes.   
4. If the system fails to save the Distribution Group due to constraints, an error message is displayed and the action is logged.  
  
Use Case Name: Update Distribution Group   
Use Case ID: UC-13   
Actors: Administrator, Distribution Group, Contact, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. A Distribution Group already exists in the system.   
3. The Administrator has the necessary permissions to update Distribution Groups.   
4. The system supports updating Distribution Group members and updating the Compliance Audit Record accordingly.   
  
Postconditions:   
1. The Distribution Group's information and membership are updated in the system.   
2. The Compliance Audit Record is updated to reflect the changes.   
3. The system logs the update action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Distribution Group Management" interface.   
2. The Administrator selects an existing Distribution Group to update.   
3. The system displays the current group name, description, and list of Contacts.   
4. The Administrator modifies the group name or description as needed.   
5. The Administrator adds or removes Contacts from the group.   
6. The Administrator confirms the changes and clicks "Update".   
7. The system validates the updated information and membership.   
8. The system updates the Distribution Group and logs the changes in the Compliance Audit Record.   
9. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the group name is missing or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If no Contacts are added after removal, the system displays a warning but allows the group to be updated with no members.   
3. If the Administrator cancels the update operation, the system returns to the Distribution Group management interface without making changes.   
4. If the system fails to update the Distribution Group due to constraints, an error message is displayed, and the action is logged.  
  
Use Case Name: Delete Distribution Group   
Use Case ID: UC-14   
Actors: Administrator, Distribution Group, Contact, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. A Distribution Group exists in the system.   
3. The Administrator has the necessary permissions to delete Distribution Groups.   
4. The system supports updating the Compliance Audit Record when a Distribution Group is deleted.   
  
Postconditions:   
1. The selected Distribution Group is removed from the system.   
2. All Contacts associated with the group are disassociated.   
3. The Compliance Audit Record is updated with the deletion details.   
4. The system logs the deletion action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Distribution Group Management" interface.   
2. The Administrator selects a Distribution Group to be deleted.   
3. The system confirms the selection and prompts the Administrator for deletion confirmation.   
4. The Administrator confirms the deletion.   
5. The system removes the Distribution Group and disassociates its Contacts.   
6. The system updates the Compliance Audit Record to indicate the deletion.   
7. The system logs the deletion action.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the selected Distribution Group is not found, the system displays an error message.   
2. If the Administrator cancels the deletion, the system returns to the Distribution Group management interface without making changes.   
3. If the deletion fails due to system constraints (e.g., the group is linked to an active Email), the system displays an error message and logs the failure.  
  
Use Case Name: View Distribution Group   
Use Case ID: UC-15   
Actors: Administrator, Distribution Group, Contact, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. At least one Distribution Group exists in the system.   
3. The Administrator has the necessary permissions to view Distribution Groups.   
4. The system can retrieve Distribution Group details and associated Contacts.   
  
Postconditions:   
1. The Administrator can view the details of the selected Distribution Group.   
2. The list of associated Contacts is displayed if applicable.   
3. The Compliance Audit Record for the Distribution Group is accessed and displayed if available.   
4. The system logs the view action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Distribution Group Management" interface.   
2. The Administrator selects a Distribution Group from the list to view.   
3. The system retrieves the Distribution Group details, including name, description, and associated Contacts.   
4. The system displays the Distribution Group information to the Administrator.   
5. If the Distribution Group has a Compliance Audit Record, the system shows the record details.   
6. The system logs the view action in the Compliance Audit Record.   
  
Alternative Flow:   
1. If the selected Distribution Group is not found, the system displays an error message.   
2. If the Compliance Audit Record is missing, the system alerts the Administrator and displays only the Distribution Group information.   
3. If the system fails to retrieve the Distribution Group details, an error message is displayed, and the Administrator is prompted to try again.   
4. If the Administrator cancels the view action, the system returns to the Distribution Group management interface without displaying additional information.  
  
Use Case Name: Register Email Account   
Use Case ID: UC-16   
Actors: Administrator, Email Account, Compliance Audit Record   
Preconditions:   
1. The Administrator is logged into the system.   
2. The system supports the registration of new Email Accounts.   
3. The Administrator has the necessary permissions to register an Email Account.   
4. The system is configured to validate the email account credentials and update the Compliance Audit Record.   
  
Postconditions:   
1. A new Email Account is registered and configured in the system.   
2. The Compliance Audit Record is updated with the registration details.   
3. The system logs the registration action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Register Email Account" interface.   
2. The Administrator enters the email account details, including email address, password, and server configuration.   
3. The Administrator confirms the details and clicks "Register".   
4. The system validates the email account credentials and configuration.   
5. The system registers the Email Account and saves it to the system.   
6. The system updates the Compliance Audit Record with the registration details.   
7. The system logs the registration action.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the email address is invalid or already registered, the system displays an error message and prompts the Administrator to correct it.   
2. If the password is incorrect or fails to authenticate with the email server, the system displays an error message and prompts the Administrator to re-enter the password.   
3. If the server configuration is invalid or incomplete, the system displays an error message and prompts the Administrator to correct it.   
4. If the Administrator cancels the registration, the system returns to the email account management interface without making changes.   
5. If the system fails to register the Email Account due to constraints, an error message is displayed, and the action is logged.  
  
Use Case Name: Modify Email Account   
Use Case ID: UC-17   
Actors: Administrator, Email Account, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email Account already exists in the system.   
3. The Administrator has the necessary permissions to modify Email Accounts.   
4. The system is capable of updating the Compliance Audit Record for the modification.   
  
Postconditions:   
1. The selected Email Account's information is updated in the system.   
2. The Compliance Audit Record is updated to reflect the modification.   
3. The system logs the modification action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Account Management" interface.   
2. The Administrator selects an existing Email Account to modify.   
3. The system displays the current Email Account details, including email address, password, and server configuration.   
4. The Administrator updates the necessary fields (e.g., password, server settings).   
5. The Administrator confirms the changes and clicks "Save".   
6. The system validates the updated information and modifies the Email Account.   
7. The system updates the Compliance Audit Record with the modification details.   
8. The system logs the modification action.   
9. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the updated email address is invalid or already in use, the system displays an error message and prompts the Administrator to correct it.   
2. If the password is incorrect or fails to authenticate with the email server, the system displays an error message and prompts the Administrator to re-enter the password.   
3. If the server configuration is invalid or incomplete, the system displays an error message and prompts the Administrator to correct it.   
4. If the Administrator cancels the modification, the system returns to the Email Account management interface without making changes.   
5. If the system fails to update the Email Account due to constraints, an error message is displayed, and the action is logged.  
  
Use Case Name: Delete Email Account   
Use Case ID: UC-18   
Actors: Administrator, Email Account, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email Account exists in the system.   
3. The Administrator has the necessary permissions to delete Email Accounts.   
4. The system supports updating the Compliance Audit Record when an Email Account is deleted.   
  
Postconditions:   
1. The selected Email Account is removed from the system.   
2. The Compliance Audit Record is updated with the deletion details.   
3. The system logs the deletion action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Account Management" interface.   
2. The Administrator selects an Email Account to be deleted.   
3. The system confirms the selection and prompts the Administrator for deletion confirmation.   
4. The Administrator confirms the deletion.   
5. The system removes the Email Account from the system.   
6. The system updates the Compliance Audit Record to indicate the deletion.   
7. The system logs the deletion action.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the selected Email Account is not found, the system displays an error message.   
2. If the Administrator cancels the deletion, the system returns to the Email Account management interface without making changes.   
3. If the deletion fails due to system constraints (e.g., the Email Account is associated with active Emails), the system displays an error message and logs the failure.  
  
Use Case Name: View Email Account Information   
Use Case ID: UC-19   
Actors: Administrator, Email Account, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email Account exists in the system.   
3. The Administrator has the necessary permissions to view Email Account information.   
4. The system can retrieve Email Account details and related Compliance Audit Records.   
  
Postconditions:   
1. The Administrator can view the details of the selected Email Account.   
2. The Compliance Audit Record for the Email Account is accessed and displayed if available.   
3. The system logs the view action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Account Management" interface.   
2. The Administrator selects an Email Account from the list to view.   
3. The system retrieves the Email Account details, including email address, server configuration, and status.   
4. The system displays the Email Account information to the Administrator.   
5. If the Email Account has a Compliance Audit Record, the system shows the record details.   
6. The system logs the view action in the Compliance Audit Record.   
  
Alternative Flow:   
1. If the selected Email Account is not found, the system displays an error message.   
2. If the Compliance Audit Record is missing, the system alerts the Administrator and displays only the Email Account information.   
3. If the system fails to retrieve the Email Account details, an error message is displayed, and the Administrator is prompted to try again.   
4. If the Administrator cancels the view action, the system returns to the Email Account management interface without displaying additional information.  
  
Use Case Name: Manage Email Templates   
Use Case ID: UC-20   
Actors: Administrator, Email Template, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. The system has an Email Template feature enabled.   
3. The Administrator has the necessary permissions to manage Email Templates.   
4. The system supports updating the Compliance Audit Record for template changes.   
  
Postconditions:   
1. The selected Email Template is either created, updated, or deleted in the system.   
2. The Compliance Audit Record is updated to reflect the management action.   
3. The system logs the management action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Template Management" interface.   
2. The Administrator selects an action: "Create", "Update", or "Delete".   
3. For "Create", the Administrator enters the template name, subject, body content, and other relevant details.   
4. For "Update", the Administrator selects an existing Email Template and modifies its content or metadata.   
5. For "Delete", the Administrator selects an existing Email Template and confirms the deletion.   
6. The system validates the input and performs the selected action on the Email Template.   
7. The system updates the Compliance Audit Record with the action details.   
8. The system logs the action and displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the template name is missing or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If the template content is incomplete or invalid, the system displays an error message and prevents the creation or update.   
3. If the Administrator cancels the action, the system returns to the Email Template management interface without making changes.   
4. If the selected Email Template does not exist, the system displays an error message.   
5. If the system fails to perform the requested action due to constraints, an error message is displayed, and the action is logged.  
  
Use Case Name: Create Email Template   
Use Case ID: UC-21   
Actors: Administrator, Email Template, Compliance Audit Record   
Preconditions:   
1. The Administrator is logged into the system.   
2. The system allows the creation of new Email Templates.   
3. The Administrator has the necessary permissions to manage Email Templates.   
4. The system is configured to update the Compliance Audit Record upon template creation.   
  
Postconditions:   
1. A new Email Template is created and stored in the system.   
2. The Compliance Audit Record is updated with the creation details.   
3. The system logs the creation action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Template Management" interface.   
2. The Administrator selects the "Create" option for Email Templates.   
3. The Administrator enters the template name, subject, body content, and any additional metadata.   
4. The Administrator confirms the details and clicks "Save".   
5. The system validates the template information and creates the Email Template.   
6. The system updates the Compliance Audit Record with the creation details.   
7. The system logs the action and displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the template name is missing or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If the template content is incomplete or invalid, the system prevents the creation and displays an error message.   
3. If the Administrator cancels the operation, the system returns to the Email Template management interface without creating the template.   
4. If the system fails to save the Email Template due to constraints, an error message is displayed, and the action is logged.  
  
Use Case Name: Update Email Template   
Use Case ID: UC-22   
Actors: Administrator, Email Template, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email Template already exists in the system.   
3. The Administrator has the necessary permissions to update Email Templates.   
4. The system is capable of updating the Compliance Audit Record for the template modification.   
  
Postconditions:   
1. The selected Email Template is updated in the system.   
2. The Compliance Audit Record is updated with the modification details.   
3. The system logs the update action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Template Management" interface.   
2. The Administrator selects an existing Email Template to update.   
3. The system displays the current template details, including name, subject, and body content.   
4. The Administrator modifies the necessary fields (e.g., name, subject, body content).   
5. The Administrator confirms the changes and clicks "Update".   
6. The system validates the updated information and modifies the Email Template.   
7. The system updates the Compliance Audit Record with the modification details.   
8. The system logs the update action.   
9. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the template name is missing or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If the template content is incomplete or invalid, the system prevents the update and displays an error message.   
3. If the Administrator cancels the update operation, the system returns to the Email Template management interface without making changes.   
4. If the system fails to update the Email Template due to constraints, an error message is displayed, and the action is logged.  
  
Use Case Name: Delete Email Template   
Use Case ID: UC-23   
Actors: Administrator, Email Template, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email Template exists in the system.   
3. The Administrator has the necessary permissions to delete Email Templates.   
4. The system supports updating the Compliance Audit Record when an Email Template is deleted.   
  
Postconditions:   
1. The selected Email Template is removed from the system.   
2. The Compliance Audit Record is updated to reflect the deletion.   
3. The system logs the deletion action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Template Management" interface.   
2. The Administrator selects an Email Template to be deleted.   
3. The system confirms the selection and prompts the Administrator for deletion confirmation.   
4. The Administrator confirms the deletion.   
5. The system removes the Email Template from the system.   
6. The system updates the Compliance Audit Record to indicate the deletion.   
7. The system logs the deletion action.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the selected Email Template is not found, the system displays an error message.   
2. If the Administrator cancels the deletion, the system returns to the Email Template management interface without making changes.   
3. If the deletion fails due to system constraints (e.g., the template is in use by an active Email), the system displays an error message and logs the failure.  
  
Use Case Name: View Compliance Audit Record   
Use Case ID: UC-24   
Actors: Administrator, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. A Compliance Audit Record exists in the system.   
3. The Administrator has the necessary permissions to view Compliance Audit Records.   
4. The system can retrieve Compliance Audit Record details and related information.   
  
Postconditions:   
1. The Administrator can view the details of the selected Compliance Audit Record.   
2. The associated Email, Contact, or Distribution Group information is displayed if applicable.   
3. The system logs the view action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Compliance Audit Record Management" interface.   
2. The Administrator selects a Compliance Audit Record from the list to view.   
3. The system retrieves the Compliance Audit Record details, including action type, timestamp, and related entities.   
4. The system displays the audit record information to the Administrator.   
5. If the audit record is associated with an Email, Contact, or Distribution Group, the system shows the relevant details.   
6. The system logs the view action in the Compliance Audit Record.   
  
Alternative Flow:   
1. If the selected Compliance Audit Record is not found, the system displays an error message.   
2. If the associated Email, Contact, or Distribution Group is missing, the system alerts the Administrator and displays only the audit record information.   
3. If the system fails to retrieve the Compliance Audit Record details, an error message is displayed, and the Administrator is prompted to try again.   
4. If the Administrator cancels the view action, the system returns to the Compliance Audit Record management interface without displaying additional information.  
  
Use Case Name: Generate Compliance Audit Report   
Use Case ID: UC-25   
Actors: Administrator, Compliance Audit Record, Email, Contact, Distribution Group, Email Account, Email Template   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. At least one Compliance Audit Record exists in the system.   
3. The Administrator has the necessary permissions to access and generate audit reports.   
4. The system supports generating reports based on Compliance Audit Records and associated entities.   
  
Postconditions:   
1. A Compliance Audit Report is generated and displayed to the Administrator.   
2. The report includes relevant details of Compliance Audit Records and associated entities (Email, Contact, Distribution Group, Email Account, Email Template).   
3. The system logs the report generation action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Compliance Audit Report" interface.   
2. The Administrator selects a time range or specific Compliance Audit Records to include in the report.   
3. The Administrator chooses the format of the report (e.g., PDF, CSV).   
4. The system retrieves the selected Compliance Audit Records and their associated entities.   
5. The system compiles the data into the requested report format.   
6. The system displays the generated Compliance Audit Report to the Administrator.   
7. The system logs the report generation action in the Compliance Audit system.   
  
Alternative Flow:   
1. If no Compliance Audit Records are selected or available, the system displays an error message and prompts the Administrator to select valid records.   
2. If the selected Compliance Audit Records cannot be retrieved, the system displays an error and logs the failure.   
3. If the report format is not supported, the system displays an error message and defaults to a standard format.   
4. If the Administrator cancels the report generation, the system returns to the Compliance Audit Report interface without generating the report.   
5. If the system fails to generate the report due to technical issues, an error message is displayed and the failure is logged.  
  
Use Case Name: Manage Email Archive Record   
Use Case ID: UC-26   
Actors: Administrator, Email Archive, Email Archive Record, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email Archive Record exists in the system or the system allows the creation of new Email Archive Records.   
3. The Administrator has the necessary permissions to manage Email Archive Records.   
4. The system is configured to link Email Archive Records with Compliance Audit Records.   
  
Postconditions:   
1. The selected Email Archive Record is either created, updated, or deleted in the system.   
2. The Compliance Audit Record is updated with the management action details.   
3. The system logs the management action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Archive Record Management" interface.   
2. The Administrator selects an action: "Create", "Update", or "Delete".   
3. For "Create", the Administrator enters metadata for the new Email Archive Record, such as the associated Email, archive date, and additional notes.   
4. For "Update", the Administrator selects an existing Email Archive Record and modifies its metadata or notes.   
5. For "Delete", the Administrator selects an existing Email Archive Record and confirms the deletion.   
6. The system validates the input and performs the selected action on the Email Archive Record.   
7. The system updates the Compliance Audit Record with the action details.   
8. The system logs the action and displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the required metadata for creating an Email Archive Record is missing or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If the selected Email Archive Record does not exist, the system displays an error message.   
3. If the update or deletion of an Email Archive Record fails due to system constraints, the system displays an error message and logs the failure.   
4. If the Administrator cancels the operation, the system returns to the Email Archive Record management interface without making changes.   
5. If the system fails to update the Compliance Audit Record, an error message is displayed, and the action is logged.  
  
Use Case Name: Manage Email Folder   
Use Case ID: UC-27   
Actors: Administrator, Email Folder, Email, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. The system supports the creation, update, deletion, and organization of Email Folders.   
3. The Administrator has the necessary permissions to manage Email Folders.   
4. The system is configured to update the Compliance Audit Record when an Email Folder is modified.   
  
Postconditions:   
1. The selected Email Folder is either created, updated, or deleted in the system.   
2. Emails associated with the folder are properly reorganized or reassigned if necessary.   
3. The Compliance Audit Record is updated with the management action details.   
4. The system logs the management action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Folder Management" interface.   
2. The Administrator selects an action: "Create", "Update", or "Delete".   
3. For "Create", the Administrator enters the folder name, description, and optionally assigns it a parent folder for hierarchical organization.   
4. For "Update", the Administrator selects an existing Email Folder and modifies its name, description, or parent folder.   
5. For "Delete", the Administrator selects an existing Email Folder and confirms the deletion.   
6. The system validates the input and performs the selected action on the Email Folder.   
7. If applicable, the system reassigns or reorganizes Emails that were in the updated or deleted folder.   
8. The system updates the Compliance Audit Record with the action details.   
9. The system logs the action and displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the folder name is missing or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If the selected Email Folder does not exist, the system displays an error message.   
3. If the deletion of an Email Folder fails due to system constraints (e.g., the folder contains active Emails and cannot be deleted without reassignment), the system displays an error message and logs the failure.   
4. If the Administrator cancels the operation, the system returns to the Email Folder management interface without making changes.   
5. If the system fails to update or link the Compliance Audit Record, an error message is displayed, and the action is logged.  
  
Use Case Name: Manage Notification   
Use Case ID: UC-28   
Actors: Administrator, Notification, Email Account, Email, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. The system supports the creation, modification, and deletion of Notifications.   
3. The Administrator has the necessary permissions to manage Notifications.   
4. The system is configured to link Notifications with Email Accounts and Compliance Audit Records.   
  
Postconditions:   
1. The selected Notification is either created, updated, or deleted in the system.   
2. The Notification is associated with the appropriate Email Account and Email (if applicable).   
3. The Compliance Audit Record is updated with the management action details.   
4. The system logs the management action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Notification Management" interface.   
2. The Administrator selects an action: "Create", "Update", or "Delete".   
3. For "Create", the Administrator enters the notification details, including title, message content, target Email Account, and conditions for triggering.   
4. The Administrator selects the associated Email or sets up the notification to monitor specific events (e.g., email sent, email received, audit record updated).   
5. The Administrator confirms the details and clicks "Save".   
6. The system validates the notification configuration and performs the selected action.   
7. The system updates the Compliance Audit Record to include the notification action and timestamp.   
8. The system logs the management action and displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the notification title or message content is missing or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If the selected Email Account is invalid or not configured, the system prevents the creation or update and displays an error message.   
3. If the notification is associated with an Email that does not exist, the system alerts the Administrator and prompts for a valid association.   
4. If the Administrator cancels the operation, the system returns to the Notification management interface without making changes.   
5. If the system fails to update the Compliance Audit Record, an error message is displayed, and the action is logged.  
  
Use Case Name: Manage Email Status Log   
Use Case ID: UC-29   
Actors: Administrator, Email Status Log, Email, Email Account, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email Status Log entry exists in the system or the system allows the creation of new Email Status Log entries.   
3. The Administrator has the necessary permissions to manage Email Status Logs.   
4. The system is configured to link Email Status Log entries with Emails, Email Accounts, and Compliance Audit Records.   
  
Postconditions:   
1. The selected Email Status Log entry is either created, updated, or deleted in the system.   
2. The Compliance Audit Record is updated to reflect the management action on the Email Status Log.   
3. The system logs the management action for audit purposes.   
4. The status of the associated Email is accurately reflected in the Email Status Log.   
  
Main Flow:   
1. The Administrator navigates to the "Email Status Log Management" interface.   
2. The Administrator selects an action: "Create", "Update", or "Delete".   
3. For "Create", the Administrator enters details for a new Email Status Log entry, such as associated Email, status (e.g., "Sent", "Failed", "Read"), timestamp, and any additional notes or error messages.   
4. For "Update", the Administrator selects an existing Email Status Log entry and modifies its status, timestamp, or notes.   
5. For "Delete", the Administrator selects an existing Email Status Log entry and confirms the deletion.   
6. The system validates the input and performs the selected action on the Email Status Log.   
7. The system updates the Compliance Audit Record to include the action performed on the Email Status Log.   
8. The system logs the management action and displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the required fields for creating an Email Status Log entry are missing or invalid, the system displays an error message and prompts the Administrator to correct them.   
2. If the selected Email Status Log entry does not exist, the system displays an error message.   
3. If the update or deletion of an Email Status Log entry fails due to system constraints (e.g., the log is linked to an active Email status change and cannot be modified or deleted), the system displays an error message and logs the failure.   
4. If the Administrator cancels the operation, the system returns to the Email Status Log management interface without making changes.   
5. If the system fails to update the Compliance Audit Record, an error message is displayed, and the action is logged.  
  
Use Case Name: Update Email   
Use Case ID: UC-30   
Actors: Administrator, Email, Email Account, Email Template, Distribution Group, Compliance Audit Record   
  
Preconditions:   
1. The Administrator is logged into the system.   
2. An Email exists in the system and is not currently being sent or processed.   
3. The Administrator has the necessary permissions to update Emails.   
4. The system supports updating Email content, associated Email Account, and Distribution Group, and updating the Compliance Audit Record accordingly.   
  
Postconditions:   
1. The selected Email is updated in the system with the new content, Email Account, or Distribution Group.   
2. The Compliance Audit Record is updated to reflect the changes made to the Email.   
3. The system logs the update action for audit purposes.   
  
Main Flow:   
1. The Administrator navigates to the "Email Management" interface.   
2. The Administrator selects an existing Email to update.   
3. The system displays the current Email details, including content, associated Email Account, and Distribution Group.   
4. The Administrator modifies the necessary fields (e.g., content, Email Account, Distribution Group) as needed.   
5. If changes to the content are made, the Administrator can choose to use an updated Email Template or manually edit the content.   
6. The Administrator confirms the changes and clicks "Update".   
7. The system validates the updated information and modifies the Email accordingly.   
8. The system updates the Compliance Audit Record with the modification details and timestamp.   
9. The system logs the update action.   
10. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the updated email content is incomplete or invalid, the system displays an error message and prompts the Administrator to correct it.   
2. If the selected Email Account is invalid or not configured, the system prevents the update and displays an error message.   
3. If the selected Distribution Group is invalid or not configured, the system displays a warning and prompts the Administrator to select a valid group.   
4. If the Compliance Audit Record update fails, the system logs the error and displays a warning message to the Administrator.   
5. If the Administrator cancels the update operation, the system returns to the Email management interface without making changes.   
6. If the system fails to update the Email due to constraints (e.g., email is in the process of being sent), an error message is displayed, and the action is logged.