项目文档

# Functional Requirement

1.1 Email Creation Function   
Function ID: FR-01   
Description: Administrators can create new emails by selecting a recipient Contact, entering subject and content, and associating the email with a valid Account.   
Input: Recipient Contact details, email subject, email content, and associated Account ID.   
Output: A new Email entity with the status "Draft" or "Sent", stored in the Email Archive.   
  
1.2 Email Sending Function   
Function ID: FR-02   
Description: Administrators can send a selected email to the associated Contact. The system updates the email status and logs the sending action.   
Input: Selected Email ID, recipient Contact details, and associated Account ID.   
Output: The Email status is updated to "Sent", and a record is added to the Email Log.   
  
1.3 Email Receiving Function   
Function ID: FR-03   
Description: The system automatically detects and stores incoming emails in the Email Archive, associating them with the appropriate Contact and Account.   
Input: Incoming email data (sender, content, timestamp, etc.).   
Output: A new Email entity with the status "Received", stored in the Email Archive and associated with a Contact and Account.   
  
1.4 Email Reading Function   
Function ID: FR-04   
Description: Administrators can view the content of a selected email along with its associated Contact and Account details. The system logs the read action and updates the email's read status.   
Input: Selected Email ID.   
Output: Email content and metadata displayed to the Administrator; the Email status is updated to "Read", and a read log entry is added.   
  
1.5 Email Deletion Function   
Function ID: FR-05   
Description: Administrators can delete an email from the system. The system verifies the selection and logs the deletion action.   
Input: Selected Email ID.   
Output: The Email is removed from the system; a deletion log entry is added to the Email Log.   
  
1.6 Email Archiving Function   
Function ID: FR-06   
Description: Administrators can archive an email to ensure long-term storage and compliance. The system updates the email status and logs the archiving action.   
Input: Selected Email ID and archiving reason (optional).   
Output: The Email status is updated to "Archived", and a corresponding Archive Record is created in the Email Archive.   
  
1.7 Email Recovery Function   
Function ID: FR-07   
Description: Administrators can recover an archived email and return it to the inbox or sent items. The system updates the email status and logs the recovery action.   
Input: Selected Email ID from the Email Archive.   
Output: The Email is moved back to its original location with status "Recovered", and a recovery log entry is added.   
  
1.8 Email Formatting Function   
Function ID: FR-08   
Description: Administrators can apply formatting rules (font style, size, color, layout) to an email using a Format Template.   
Input: Selected Email ID and formatting rules from a Format Template.   
Output: The Email is updated with the applied formatting, and the formatting changes are stored in the Email Archive.   
  
1.9 Contact Creation Function   
Function ID: FR-09   
Description: Administrators can create new Contacts and associate them with a valid Account.   
Input: Contact name, email address, phone number, address, and associated Account ID.   
Output: A new Contact entity stored in the system and linked to a valid Account.   
  
1.10 Contact Update Function   
Function ID: FR-10   
Description: Administrators can modify the details of an existing Contact, and the changes are logged.   
Input: Selected Contact ID and updated Contact details.   
Output: The Contact entity is updated in the system, and an update log entry is added.   
  
1.11 Contact Deletion Function   
Function ID: FR-11   
Description: Administrators can delete a Contact from the system. The system updates related Email records and logs the deletion action.   
Input: Selected Contact ID.   
Output: The Contact is removed from the system; related Email records are updated, and a deletion log entry is added.   
  
1.12 Contact Viewing Function   
Function ID: FR-12   
Description: Administrators can view the details of an existing Contact, including their associated Account.   
Input: Selected Contact ID.   
Output: Contact details displayed to the Administrator, and a view log entry is added.   
  
1.13 Account Management Function   
Function ID: FR-13   
Description: Administrators can create, update, or delete an Account. The system ensures all associated Emails and Contacts are updated accordingly.   
Input: Account details for creation, update, or deletion.   
Output: Account entity is created, updated, or deleted in the system; related entities are adjusted, and the action is logged.   
  
1.14 Account Update Function   
Function ID: FR-14   
Description: Administrators can update an existing Account's information, and the system logs the update and reflects changes in related entities.   
Input: Selected Account ID and updated Account details.   
Output: Account entity is updated in the system; related Emails and Contacts are updated as necessary, and an update log entry is added.   
  
1.15 Account Deletion Function   
Function ID: FR-15   
Description: Administrators can delete an Account. The system verifies for active dependencies and updates or disassociates related Contacts and Emails.   
Input: Selected Account ID.   
Output: The Account is deleted from the system; related Contacts and Emails are updated or disassociated, and a deletion log entry is added.   
  
1.16 Account Viewing Function   
Function ID: FR-16   
Description: Administrators can view the details of an Account and its associated Contacts.   
Input: Selected Account ID.   
Output: Account details and associated Contacts are displayed to the Administrator, and a view log entry is added.   
  
1.17 Archive Record Management Function   
Function ID: FR-17   
Description: Administrators can create, update, or delete Archive Records for archived Emails. The system logs all actions and updates the Email Archive accordingly.   
Input: Archive Record details for creation, update, or deletion.   
Output: Archive Record is created, updated, or deleted in the system; the Email Archive is updated if necessary, and the action is logged.   
  
1.18 Compliance Audit Function   
Function ID: FR-18   
Description: Administrators can perform a compliance audit to check emails against data privacy and content policies. The system flags non-compliant emails and generates a compliance report.   
Input: Audit criteria (time range, filters, etc.).   
Output: Compliance audit results displayed to the Administrator, including flagged emails; a Compliance Log is updated with audit details.   
  
1.19 Archive Log Viewing Function   
Function ID: FR-19   
Description: Administrators can view logs of archiving and recovery actions. The system supports filtering by time range and other audit criteria.   
Input: Time range or filter criteria for archive logs.   
Output: Archive logs displayed to the Administrator, including email details, action timestamps, and associated entities; the view is logged.   
  
1.20 Administrator Log Viewing Function   
Function ID: FR-20   
Description: Administrators can view logs of their own actions and other administrators' actions for auditing and troubleshooting.   
Input: Time range or filter criteria for administrator logs.   
Output: Administrator logs displayed to the user, including action details and timestamps; the viewing action is logged.   
  
1.21 Format Template Management Function   
Function ID: FR-21   
Description: Administrators can create, update, or delete Format Templates that define formatting rules for Emails.   
Input: Format Template details for creation, update, or deletion.   
Output: Format Template is created, updated, or deleted in the system; the formatting rules are applied to associated Emails, and the action is logged.   
  
1.22 Administrator Creation Function   
Function ID: FR-22   
Description: Administrators can create new Administrator accounts and assign them to valid Accounts.   
Input: New Administrator details (name, username, password) and associated Account ID.   
Output: A new Administrator is created in the system and linked to an Account; the action is logged.   
  
1.23 Administrator Permission Assignment Function   
Function ID: FR-23   
Description: Administrators can assign administrative permissions to other users within the system.   
Input: Target user ID and the Account for which permissions are being assigned.   
Output: The user is granted administrative rights for the selected Account; the action is logged.   
  
1.24 Administrator Removal Function   
Function ID: FR-24   
Description: Administrators can remove other administrators from the system. The system verifies if there are other administrators for the Account and updates permissions accordingly.   
Input: Target Administrator ID.   
Output: The Administrator is removed from the system; the associated Account is updated, and the action is logged.   
  
1.25 Compliance Log Management Function   
Function ID: FR-25   
Description: Administrators can view, update, or delete Compliance Log entries that track audit results for Emails.   
Input: Compliance Log action (view, update, or delete) and relevant Compliance Log ID.   
Output: Compliance Log is updated or removed as per the action; the action is logged for traceability.

# External Description

# \*\*Chapter 2: External Interfaces\*\*   
  
This chapter defines the external interfaces of the system, including user interfaces, hardware interfaces, software interfaces, and communication interfaces. These interfaces are essential for the system to interact with external entities such as users, hardware components, external software systems, and communication protocols. The description of each interface includes its role, definition, and interaction method with the system.   
  
---  
  
## \*\*2.1 User Interface Output\*\*   
  
The system provides a set of user interfaces for administrators to manage emails, contacts, accounts, format templates, and compliance logs. These interfaces are designed for ease of use and efficient interaction with the system.   
  
### \*\*2.1.1 Email Management Interface\*\*   
\*\*Definition:\*\* A graphical interface for creating, sending, reading, deleting, archiving, and recovering emails.   
\*\*Role:\*\* Allows administrators to compose and manage emails, view their status and content, and perform related actions.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Recipient Contact details   
 - Email subject and content   
 - Email ID for sending, reading, deleting, archiving, or recovering   
 - Formatting rules from a selected Format Template   
- \*\*Outputs:\*\*   
 - Display of email content and metadata   
 - Status updates (e.g., "Draft", "Sent", "Read", "Archived", "Recovered")   
 - Confirmation messages for sending, deleting, or archiving actions   
 - Logging of user actions (e.g., sending, reading, deleting)   
  
### \*\*2.1.2 Contact Management Interface\*\*   
\*\*Definition:\*\* A graphical interface for creating, updating, deleting, and viewing contacts.   
\*\*Role:\*\* Enables administrators to manage contact records associated with accounts.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Contact name, email address, phone number, and address   
 - Contact ID for updating or deleting   
- \*\*Outputs:\*\*   
 - Display of contact details and associated account   
 - Confirmation of contact creation, update, or deletion   
 - Logging of user actions   
  
### \*\*2.1.3 Account Management Interface\*\*   
\*\*Definition:\*\* A graphical interface for creating, updating, deleting, and viewing account records.   
\*\*Role:\*\* Provides a central point for administrators to manage account-related data and associated contacts and emails.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Account details for creation or update   
 - Account ID for deletion or viewing   
- \*\*Outputs:\*\*   
 - Display of account information and associated contacts   
 - Confirmation of account creation, update, or deletion   
 - Logging of user actions   
  
### \*\*2.1.4 Format Template Management Interface\*\*   
\*\*Definition:\*\* A graphical interface for managing formatting rules applied to emails.   
\*\*Role:\*\* Allows administrators to define, update, or delete format templates for consistent email formatting.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Format template details (font style, size, color, layout)   
 - Template ID for updating or deleting   
- \*\*Outputs:\*\*   
 - Display of format template details   
 - Confirmation of template creation, update, or deletion   
 - Logging of user actions   
  
### \*\*2.1.5 Compliance Audit Interface\*\*   
\*\*Definition:\*\* A graphical interface for performing compliance audits on emails.   
\*\*Role:\*\* Enables administrators to review emails for compliance with data privacy and content policies.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Audit criteria (e.g., time range, filters)   
- \*\*Outputs:\*\*   
 - Display of audit results, including flagged emails   
 - Generation of compliance audit reports   
 - Logging of audit actions   
  
### \*\*2.1.6 Administrator Management Interface\*\*   
\*\*Definition:\*\* A graphical interface for managing administrator accounts and permissions.   
\*\*Role:\*\* Provides tools for creating new administrators, assigning or removing permissions, and viewing logs of administrative actions.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Administrator details (name, username, password)   
 - Target user or administrator ID for permission assignment or removal   
- \*\*Outputs:\*\*   
 - Display of administrator account details and permissions   
 - Confirmation of administrator creation, permission assignment, or removal   
 - Logging of administrative actions   
  
---  
  
## \*\*2.2 Hardware Interface Output\*\*   
  
There are no direct hardware interfaces required for this system, as it operates primarily through software and network-based communication. The system is expected to run on standard server hardware and desktop/laptop devices, but no specialized hardware is required for its core functionality.   
  
---  
  
## \*\*2.3 Software Interface Output\*\*   
  
The system interacts with external software components, particularly databases and logging systems, to store and retrieve data efficiently.   
  
### \*\*2.3.1 Email Archive Database\*\*   
\*\*Definition:\*\* A persistent storage system for email entities, including their content, metadata, status, and associated contacts and accounts.   
\*\*Role:\*\* Stores all created, sent, received, read, archived, and recovered emails.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Email entities with statuses such as "Draft", "Sent", "Read", "Archived", or "Recovered"   
 - Archive records for long-term compliance storage   
- \*\*Outputs:\*\*   
 - Retrieval of email entities for viewing, updating, or deleting   
 - Storage of email entities with updated status or formatting   
 - Creation of archive records for compliance   
  
### \*\*2.3.2 Email Log Database\*\*   
\*\*Definition:\*\* A database that records all email-related actions, including sending, reading, deleting, and archiving.   
\*\*Role:\*\* Maintains a traceable history of all email operations for auditing and compliance.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Email action details (e.g., "Sent", "Read", "Deleted", "Archived", "Recovered")   
 - Timestamps and associated entity IDs (Email ID, Contact ID, Account ID)   
- \*\*Outputs:\*\*   
 - Storage of log entries   
 - Retrieval of log data for viewing or audit purposes   
  
### \*\*2.3.3 Compliance Log Database\*\*   
\*\*Definition:\*\* A database that stores compliance audit results and actions taken on emails.   
\*\*Role:\*\* Ensures traceability and compliance tracking for all email content.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Compliance audit details (e.g., flagged emails, audit timestamps, criteria)   
 - Log entries for viewing, updating, or deleting   
- \*\*Outputs:\*\*   
 - Storage of compliance audit results   
 - Retrieval of log data for viewing or updating   
  
### \*\*2.3.4 Format Template Database\*\*   
\*\*Definition:\*\* A database storing formatting rules and templates used to apply consistent styles to emails.   
\*\*Role:\*\* Stores and retrieves formatting configurations for email creation and modification.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Format template details (font style, size, color, layout)   
 - Template ID for retrieval or deletion   
- \*\*Outputs:\*\*   
 - Retrieval of formatting rules for applying to emails   
 - Storage of new or updated format templates   
  
---  
  
## \*\*2.4 Communication Interface Output\*\*   
  
The system communicates with external entities through email protocols and network-based interactions.   
  
### \*\*2.4.1 Email Communication Interface\*\*   
\*\*Definition:\*\* A communication interface for sending and receiving emails via standard email protocols (e.g., SMTP, POP3, IMAP).   
\*\*Role:\*\* Enables the system to send outgoing emails to recipients and receive incoming emails from external sources.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - Email content and recipient details for sending   
 - Incoming email data (sender, content, timestamp) for receiving   
- \*\*Outputs:\*\*   
 - Sent emails to the recipient’s email server   
 - Stored incoming emails in the Email Archive with appropriate associations   
 - Logging of sending and receiving actions   
  
### \*\*2.4.2 Web Communication Interface\*\*   
\*\*Definition:\*\* A communication interface for administrators to access the system via a web browser.   
\*\*Role:\*\* Provides a secure and accessible way to interact with the system using HTTP/HTTPS protocols.   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - User login credentials   
 - Input data from web-based forms and interfaces (e.g., email content, contact details)   
- \*\*Outputs:\*\*   
 - Rendered web pages and interface elements   
 - Real-time updates and responses to user actions   
 - Logging of all web-based interactions   
  
### \*\*2.4.3 API Communication Interface (Optional)\*\*   
\*\*Definition:\*\* A potential software interface for external systems to interact with the email management system using defined API endpoints.   
\*\*Role:\*\* Allows for integration with third-party systems (e.g., CRM tools, enterprise email servers).   
\*\*Interaction Method:\*\*   
- \*\*Inputs:\*\*   
 - JSON/XML payloads containing email, contact, or account data   
 - API requests for creating, updating, or retrieving data   
- \*\*Outputs:\*\*   
 - Structured responses in JSON/XML format   
 - Status codes indicating success or failure of API requests   
 - Logging of API-based actions   
  
---  
  
## \*\*Summary of External Interfaces\*\*   
  
| Interface Type | Interface Name | Description |  
|-----------------------------|----------------------------------|-----------------------------------------------------------------------------|  
| User Interface | Email Management Interface | Manages creation, sending, reading, deleting, archiving, and recovery of emails |  
| User Interface | Contact Management Interface | Manages contact records and their associations to accounts |  
| User Interface | Account Management Interface | Manages account creation, updates, deletions, and associated entities |  
| User Interface | Format Template Management Interface | Manages formatting templates for emails |  
| User Interface | Compliance Audit Interface | Performs and displays compliance audits on emails |  
| User Interface | Administrator Management Interface | Manages administrator accounts and permissions |  
| Software Interface | Email Archive Database | Stores and retrieves email entities and their metadata |  
| Software Interface | Email Log Database | Logs all email-related actions for auditability |  
| Software Interface | Compliance Log Database | Logs compliance audit results for traceability |  
| Software Interface | Format Template Database | Stores formatting rules for email templates |  
| Communication Interface | Email Communication Interface | Handles sending and receiving of emails via external email servers |  
| Communication Interface | Web Communication Interface | Provides access to the system through web browsers |  
| Communication Interface | API Communication Interface | Allows external systems to interact with the system through API endpoints |  
  
---  
  
This section ensures that all external data sources referenced in the functional requirements are clearly defined and categorized. Developers can refer to these interfaces to understand how the system interacts with the outside world and how to implement these interactions consistently and accurately.

# Use Case

Use Case Name: Create Email   
Use Case ID: UC-01   
Actors: Administrator, Email Archive, Email, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the email creation interface. The system must have an active Email Archive and valid Contact and Account information available.   
Postconditions: A new email is successfully created and stored in the Email Archive. The email is associated with the appropriate Contact and Account.   
Main Flow:   
1. The Administrator navigates to the email creation interface.   
2. The Administrator selects the recipient Contact from the Contact list.   
3. The Administrator enters the email subject and content.   
4. The Administrator selects the associated Account for the email.   
5. The Administrator clicks the "Create Email" button.   
6. The system validates the input information.   
7. The system creates the new email and stores it in the Email Archive.   
8. The system displays a confirmation message indicating the email was created successfully.   
  
Alternative Flow:   
1. If the Administrator does not select a valid Contact, the system displays an error message and prompts the Administrator to choose a valid Contact.   
2. If the email subject or content is missing, the system displays an error message and prompts the Administrator to fill in the required information.   
3. If the selected Account is invalid, the system displays an error message and prompts the Administrator to choose a valid Account.  
  
Use Case Name: Send Email   
Use Case ID: UC-02   
Actors: Administrator, Email Archive, Email, Contact, Account   
Preconditions: The Administrator has created an Email and it is stored in the Email Archive. The Administrator is authenticated and has access to the email sending interface. The system must have valid Contact and Account information associated with the Email.   
Postconditions: The selected email is successfully sent to the specified Contact. A record of the sent email is updated in the Email Archive.   
Main Flow:   
1. The Administrator navigates to the email sending interface.   
2. The Administrator selects an email from the Email Archive.   
3. The Administrator confirms the recipient Contact associated with the email.   
4. The Administrator initiates the sending process by clicking the "Send Email" button.   
5. The system validates the email and recipient details.   
6. The system sends the email to the specified Contact.   
7. The system updates the status of the email in the Email Archive to "Sent".   
8. The system displays a confirmation message indicating the email was sent successfully.   
  
Alternative Flow:   
1. If the selected email is not valid, the system displays an error message and prompts the Administrator to select a valid email.   
2. If the recipient Contact is not associated with the email, the system displays an error message and prompts the Administrator to assign a valid Contact.   
3. If the sending process fails due to system errors, the system displays an error message and retains the email in the "Draft" status in the Email Archive.  
  
Use Case Name: Receive Email   
Use Case ID: UC-03   
Actors: Administrator, Email Archive, Email, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the email receiving interface. The system must have an active Email Archive and valid Contact and Account information. An incoming email must be detected by the system.   
Postconditions: The incoming email is successfully received and stored in the Email Archive. The email is associated with the appropriate Contact and Account.   
Main Flow:   
1. The system detects an incoming email.   
2. The system identifies the recipient Contact based on the email address.   
3. The system associates the email with the relevant Account.   
4. The system stores the email in the Email Archive.   
5. The Administrator is notified of the received email.   
6. The system displays the email in the Administrator's inbox.   
7. The system updates the Email Archive with the status "Received".   
8. The system logs the receipt of the email.   
  
Alternative Flow:   
1. If the recipient Contact cannot be identified, the system displays an error message and stores the email in the Email Archive with an "Unassigned" status.   
2. If the associated Account is invalid, the system displays an error message and prompts the Administrator to assign a valid Account manually.   
3. If the system fails to store the email, the system displays an error message and retains the email in a temporary buffer for manual intervention.  
  
Use Case Name: Read Email   
Use Case ID: UC-04   
Actors: Administrator, Email Archive, Email, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the email reading interface. The system must have an active Email Archive containing emails. The selected email must be associated with a valid Contact and Account.   
Postconditions: The Administrator successfully views the selected email's content. The email's "Read" status is updated in the Email Archive.   
Main Flow:   
1. The Administrator navigates to the email reading interface.   
2. The Administrator selects an email from the Email Archive.   
3. The system retrieves the email details from the Email Archive.   
4. The system displays the email's subject, content, recipient Contact, and associated Account.   
5. The Administrator reviews the email information.   
6. The system updates the email status to "Read" in the Email Archive.   
7. The system logs the read action.   
  
Alternative Flow:   
1. If the selected email is not valid, the system displays an error message and prompts the Administrator to select a valid email.   
2. If the associated Contact or Account is missing, the system displays an error message and prompts the Administrator to assign a valid Contact and Account manually.   
3. If the system fails to retrieve the email, the system displays an error message and retains the email status as "Unread".  
  
Use Case Name: Delete Email   
Use Case ID: UC-05   
Actors: Administrator, Email Archive, Email   
Preconditions: The Administrator is authenticated and has access to the email deletion interface. The system must have an active Email Archive containing emails. The Administrator must select a valid email for deletion.   
Postconditions: The selected email is successfully deleted from the Email Archive. The deletion is logged in the system.   
Main Flow:   
1. The Administrator navigates to the email deletion interface.   
2. The Administrator selects the email to be deleted from the Email Archive.   
3. The system confirms the selected email details to the Administrator.   
4. The Administrator clicks the "Delete Email" button.   
5. The system validates the email selection.   
6. The system deletes the selected email from the Email Archive.   
7. The system displays a confirmation message indicating the email was deleted successfully.   
8. The system logs the deletion action.   
  
Alternative Flow:   
1. If the selected email is not valid, the system displays an error message and prompts the Administrator to select a valid email.   
2. If the system fails to delete the email, the system displays an error message and retains the email in the Email Archive.   
3. If the Administrator cancels the deletion, the system returns to the email list without making any changes.  
  
Use Case Name: Archive Email   
Use Case ID: UC-06   
Actors: Administrator, Email, Email Archive, Account, Contact   
Preconditions: The Administrator is authenticated and has access to the email archiving interface. The system must have an active Email Archive and a valid Email that is either "Sent" or "Received". The email must be associated with a valid Contact and Account.   
Postconditions: The selected email is moved to the Email Archive. The email's status is updated to "Archived". The deletion or movement from the inbox or sent items is logged.   
Main Flow:   
1. The Administrator navigates to the email archiving interface.   
2. The Administrator selects an email from the inbox or sent items.   
3. The system confirms the email details and its association with Contact and Account.   
4. The Administrator clicks the "Archive Email" button.   
5. The system validates the email and archiving permissions.   
6. The system moves the selected email to the Email Archive.   
7. The system updates the email status to "Archived".   
8. The system displays a confirmation message indicating the email was archived successfully.   
  
Alternative Flow:   
1. If the selected email is not valid, the system displays an error message and prompts the Administrator to select a valid email.   
2. If the email is not associated with a valid Contact or Account, the system displays an error message and prompts the Administrator to assign or verify the details.   
3. If the system fails to move the email to the archive, the system displays an error message and retains the email in its original location.  
  
Use Case Name: Recover Email   
Use Case ID: UC-07   
Actors: Administrator, Email Archive, Email, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the email recovery interface. The system must have an active Email Archive containing emails with an "Archived" status. The Administrator must select a valid archived email for recovery.   
Postconditions: The selected email is successfully recovered from the Email Archive. The email's status is updated to "Recovered" or moved back to the inbox/sent items. The recovery action is logged in the system.   
Main Flow:   
1. The Administrator navigates to the email recovery interface.   
2. The Administrator selects an email from the Email Archive with an "Archived" status.   
3. The system confirms the email details and its association with Contact and Account.   
4. The Administrator clicks the "Recover Email" button.   
5. The system validates the email and recovery permissions.   
6. The system moves the selected email back to the inbox or sent items based on its original status.   
7. The system updates the email status to "Recovered".   
8. The system displays a confirmation message indicating the email was recovered successfully.   
  
Alternative Flow:   
1. If the selected email is not valid, the system displays an error message and prompts the Administrator to select a valid email.   
2. If the email is not in the "Archived" status, the system displays an error message and prompts the Administrator to choose an archived email.   
3. If the system fails to recover the email, the system displays an error message and retains the email in the Email Archive.  
  
Use Case Name: Format Email   
Use Case ID: UC-08   
Actors: Administrator, Email, Email Archive, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the email formatting interface. An email must be selected from the Email Archive or created in the system. The email must be associated with a valid Contact and Account.   
Postconditions: The selected email is formatted according to the specified preferences. The formatting details are saved in the Email Archive. The email is ready for sending or further editing.   
Main Flow:   
1. The Administrator navigates to the email formatting interface.   
2. The Administrator selects an email from the Email Archive or creates a new one.   
3. The system displays the email's subject and content for formatting.   
4. The Administrator applies formatting options such as font style, size, color, and layout.   
5. The Administrator clicks the "Apply Format" button.   
6. The system validates the formatting changes.   
7. The system updates the email in the Email Archive with the new formatting.   
8. The system displays a confirmation message indicating the email was formatted successfully.   
  
Alternative Flow:   
1. If the selected email is not valid, the system displays an error message and prompts the Administrator to select a valid email.   
2. If no formatting changes are applied, the system displays a warning message and allows the Administrator to confirm or cancel.   
3. If the system fails to apply the formatting, the system displays an error message and retains the email in its original format.  
  
Use Case Name: Create Contact   
Use Case ID: UC-09   
Actors: Administrator, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the contact creation interface. The system must have a valid Account associated with the new Contact.   
Postconditions: A new Contact is successfully created and stored in the system. The Contact is associated with a valid Account.   
Main Flow:   
1. The Administrator navigates to the contact creation interface.   
2. The Administrator enters the Contact's details, including name, email address, phone number, and role.   
3. The Administrator selects or enters the associated Account for the Contact.   
4. The Administrator clicks the "Create Contact" button.   
5. The system validates the input information.   
6. The system creates the new Contact and stores it in the system.   
7. The system displays a confirmation message indicating the Contact was created successfully.   
  
Alternative Flow:   
1. If the Administrator does not enter a valid name or email address, the system displays an error message and prompts the Administrator to fill in the required information.   
2. If the selected Account is invalid, the system displays an error message and prompts the Administrator to choose a valid Account.   
3. If the system fails to create the Contact, the system displays an error message and retains the Contact in a draft state for manual correction.  
  
Use Case Name: Update Contact   
Use Case ID: UC-10   
Actors: Administrator, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the contact update interface. A valid Contact must already exist in the system. The Contact must be associated with a valid Account.   
Postconditions: The selected Contact's information is successfully updated in the system. The updated Contact details are associated with the same Account. The change is logged in the system.   
Main Flow:   
1. The Administrator navigates to the contact update interface.   
2. The Administrator selects an existing Contact from the Contact list.   
3. The system displays the Contact's current details.   
4. The Administrator modifies the Contact's information as needed (e.g., name, email address, phone number, role).   
5. The Administrator clicks the "Update Contact" button.   
6. The system validates the updated information.   
7. The system updates the Contact details in the system.   
8. The system displays a confirmation message indicating the Contact was updated successfully.   
  
Alternative Flow:   
1. If the Administrator does not enter a valid name or email address, the system displays an error message and prompts the Administrator to correct the information.   
2. If the associated Account is invalid or removed, the system displays an error message and prompts the Administrator to assign a valid Account.   
3. If the system fails to update the Contact, the system displays an error message and retains the previous Contact information.  
  
Use Case Name: Delete Contact   
Use Case ID: UC-11   
Actors: Administrator, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the contact deletion interface. A valid Contact must exist in the system and be associated with a valid Account.   
Postconditions: The selected Contact is successfully deleted from the system. The deletion is logged in the system. Any associated emails or records are updated to reflect the deletion or disassociation.   
Main Flow:   
1. The Administrator navigates to the contact deletion interface.   
2. The Administrator selects the Contact to be deleted from the Contact list.   
3. The system confirms the Contact's details and its association with the Account.   
4. The Administrator clicks the "Delete Contact" button.   
5. The system validates the Contact and deletion permissions.   
6. The system deletes the Contact from the system.   
7. The system updates any related records (e.g., emails) to reflect the deletion or remove references to the Contact.   
8. The system displays a confirmation message indicating the Contact was deleted successfully.   
  
Alternative Flow:   
1. If the selected Contact is not valid, the system displays an error message and prompts the Administrator to select a valid Contact.   
2. If the Contact is associated with critical emails or records, the system displays a warning message and asks the Administrator to confirm the deletion.   
3. If the system fails to delete the Contact, the system displays an error message and retains the Contact in the system.  
  
Use Case Name: View Contact   
Use Case ID: UC-12   
Actors: Administrator, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the contact viewing interface. A valid Contact must exist in the system and be associated with a valid Account.   
Postconditions: The Administrator successfully views the selected Contact's information. The system logs the view action.   
Main Flow:   
1. The Administrator navigates to the contact viewing interface.   
2. The Administrator selects a Contact from the Contact list.   
3. The system retrieves the Contact's details from the system.   
4. The system displays the Contact's name, email address, phone number, role, and associated Account.   
5. The Administrator reviews the Contact information.   
6. The system logs the view action.   
  
Alternative Flow:   
1. If the selected Contact is not valid, the system displays an error message and prompts the Administrator to select a valid Contact.   
2. If the associated Account is missing or invalid, the system displays an error message and prompts the Administrator to verify or assign a valid Account.   
3. If the system fails to retrieve the Contact details, the system displays an error message and retains the Contact in the list.  
  
Use Case Name: Manage Account   
Use Case ID: UC-13   
Actors: Administrator, Account   
Preconditions: The Administrator is authenticated and has access to the account management interface. A valid Account must exist in the system or be newly created.   
Postconditions: The selected Account is successfully created, updated, or deleted. The system logs the action and updates related data entities accordingly.   
  
Main Flow:   
1. The Administrator navigates to the account management interface.   
2. The Administrator selects an action: "Create Account", "Update Account", or "Delete Account".   
3. If creating an account, the Administrator enters the Account details (e.g., name, type, status).   
4. If updating an account, the Administrator selects an existing Account and modifies its details.   
5. If deleting an account, the Administrator selects an existing Account and confirms the deletion.   
6. The system validates the input or selection.   
7. The system performs the selected action on the Account (create, update, or delete).   
8. The system displays a confirmation message indicating the action was completed successfully.   
  
Alternative Flow:   
1. If the input for creating or updating an account is incomplete or invalid, the system displays an error message and prompts the Administrator to correct the information.   
2. If the selected account for updating or deleting is invalid, the system displays an error message and prompts the Administrator to select a valid account.   
3. If the Administrator cancels the action during the confirmation step, the system returns to the account list without making any changes.   
4. If the system fails to perform the action, an error message is displayed, and the Account remains in its previous state.  
  
Use Case Name: Update Account   
Use Case ID: UC-14   
Actors: Administrator, Account   
Preconditions: The Administrator is authenticated and has access to the account update interface. A valid Account must already exist in the system and be selected for modification.   
Postconditions: The selected Account's information is successfully updated in the system. The system logs the update action and reflects the changes in related data entities (e.g., Email, Contact).   
  
Main Flow:   
1. The Administrator navigates to the account update interface.   
2. The Administrator selects an existing Account from the Account list.   
3. The system displays the Account's current details (e.g., name, type, status).   
4. The Administrator modifies the Account's information as needed.   
5. The Administrator clicks the "Update Account" button.   
6. The system validates the updated information.   
7. The system updates the Account details in the system.   
8. The system displays a confirmation message indicating the Account was updated successfully.   
  
Alternative Flow:   
1. If the Administrator does not enter valid or complete information, the system displays an error message and prompts the Administrator to correct the details.   
2. If the selected Account is invalid or does not exist, the system displays an error message and prompts the Administrator to choose a valid Account.   
3. If the system fails to update the Account, the system displays an error message and retains the previous Account information.  
  
Use Case Name: Delete Account   
Use Case ID: UC-15   
Actors: Administrator, Account, Contact, Email Archive   
Preconditions: The Administrator is authenticated and has access to the account deletion interface. A valid Account must exist in the system. The Account must not have any active dependencies or critical data that would prevent deletion.   
Postconditions: The selected Account is successfully deleted from the system. All associated Contacts and Emails are either disassociated or updated to reflect the deletion. The system logs the deletion action.   
  
Main Flow:   
1. The Administrator navigates to the account deletion interface.   
2. The Administrator selects an existing Account from the Account list.   
3. The system confirms the Account's details and its associated Contacts and Emails.   
4. The Administrator clicks the "Delete Account" button.   
5. The system validates the Account and checks for any active dependencies.   
6. The system deletes the Account from the system.   
7. The system updates or disassociates all related Contacts and Emails.   
8. The system displays a confirmation message indicating the Account was deleted successfully.   
  
Alternative Flow:   
1. If the selected Account is invalid or does not exist, the system displays an error message and prompts the Administrator to select a valid Account.   
2. If the Account has active dependencies (e.g., associated emails or contacts), the system displays a warning message and asks the Administrator to confirm the deletion or resolve the dependencies.   
3. If the system fails to delete the Account, an error message is displayed, and the Account remains in the system for manual correction.  
  
Use Case Name: View Account Information   
Use Case ID: UC-16   
Actors: Administrator, Account   
Preconditions: The Administrator is authenticated and has access to the account information viewing interface. A valid Account must exist in the system and be selected for viewing.   
Postconditions: The Administrator successfully views the selected Account's information. The system logs the view action.   
  
Main Flow:   
1. The Administrator navigates to the account information viewing interface.   
2. The Administrator selects an Account from the Account list.   
3. The system retrieves the Account's details (e.g., name, type, status, and associated Contacts).   
4. The system displays the Account's information to the Administrator.   
5. The Administrator reviews the displayed information.   
6. The system logs the view action.   
  
Alternative Flow:   
1. If the selected Account is not valid, the system displays an error message and prompts the Administrator to select a valid Account.   
2. If the system fails to retrieve the Account information, the system displays an error message and retains the Account in the list.  
  
Use Case Name: Manage Email Archive   
Use Case ID: UC-06   
Actors: Administrator, Email Archive, Email, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the email archiving interface. The system must have an active Email Archive and a valid Email that is either "Sent" or "Received". The Email must be associated with a valid Contact and Account.   
Postconditions: The selected Email is moved to the Email Archive. The Email's status is updated to "Archived". The system logs the archiving action.   
  
Main Flow:   
1. The Administrator navigates to the email archiving interface.   
2. The Administrator selects an Email from the inbox or sent items.   
3. The system confirms the Email details and its association with Contact and Account.   
4. The Administrator clicks the "Archive Email" button.   
5. The system validates the Email and archiving permissions.   
6. The system moves the selected Email to the Email Archive.   
7. The system updates the Email status to "Archived".   
8. The system displays a confirmation message indicating the Email was archived successfully.   
  
Alternative Flow:   
1. If the selected Email is not valid, the system displays an error message and prompts the Administrator to select a valid Email.   
2. If the Email is not associated with a valid Contact or Account, the system displays an error message and prompts the Administrator to assign or verify the details.   
3. If the system fails to move the Email to the archive, the system displays an error message and retains the Email in its original location.  
  
Use Case Name: View Archive Logs   
Use Case ID: UC-17   
Actors: Administrator, Email Archive, Email, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the archive log viewing interface. The system must have an active Email Archive containing archived Emails.   
Postconditions: The Administrator successfully views the archive logs. The system logs the viewing action.   
  
Main Flow:   
1. The Administrator navigates to the archive log viewing interface.   
2. The Administrator selects a specific time range or filter for the logs.   
3. The system retrieves the relevant archive logs from the Email Archive.   
4. The system displays the logs, including details such as email subject, recipient Contact, associated Account, and the archiving timestamp.   
5. The Administrator reviews the archive logs.   
6. The system logs the viewing action.   
  
Alternative Flow:   
1. If the selected time range or filter is invalid, the system displays an error message and prompts the Administrator to adjust the parameters.   
2. If no archive logs match the criteria, the system displays a message indicating no logs were found.   
3. If the system fails to retrieve the logs, an error message is displayed, and the Administrator is redirected to the Email Archive for manual review.  
  
Use Case Name: Perform Compliance Audit   
Use Case ID: UC-18   
Actors: Administrator, Email Archive, Email, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the compliance audit interface. The system must have an active Email Archive containing emails, and valid Contact and Account information must be available for review.   
Postconditions: The compliance audit is successfully performed. Any non-compliant emails are flagged or reported. The system logs the audit action and provides a summary of the audit results.   
  
Main Flow:   
1. The Administrator navigates to the compliance audit interface.   
2. The Administrator selects a specific time range or filter for the audit.   
3. The system retrieves all relevant emails from the Email Archive based on the selected criteria.   
4. The system cross-checks each email against compliance rules (e.g., data privacy, content policies).   
5. The system identifies and flags any non-compliant emails.   
6. The system compiles an audit report summarizing the findings, including flagged emails, associated Contacts, and Accounts.   
7. The system displays the audit report to the Administrator.   
8. The system logs the compliance audit action.   
  
Alternative Flow:   
1. If the selected time range or filter is invalid, the system displays an error message and prompts the Administrator to adjust the parameters.   
2. If no emails match the audit criteria, the system displays a message indicating no emails were found for the audit.   
3. If the system fails to retrieve or process the emails, an error message is displayed, and the Administrator is redirected to the Email Archive for manual review.  
  
Use Case Name: Create Administrator   
Use Case ID: UC-19   
Actors: System, Administrator   
Preconditions: The system is operational and accessible. The Administrator has the necessary permissions to create a new Administrator. The system must have valid Account information for the new Administrator.   
Postconditions: A new Administrator is successfully created and stored in the system. The new Administrator is associated with a valid Account. The system logs the creation action.   
  
Main Flow:   
1. The system displays the Administrator creation interface.   
2. The Administrator enters the new Administrator's details, including name, username, and password.   
3. The Administrator selects or assigns an Account for the new Administrator.   
4. The Administrator clicks the "Create Administrator" button.   
5. The system validates the input information, ensuring the username is unique and the password meets security requirements.   
6. The system creates the new Administrator and stores it in the system.   
7. The system assigns the new Administrator to the selected Account.   
8. The system displays a confirmation message indicating the Administrator was created successfully.   
  
Alternative Flow:   
1. If the username is not unique, the system displays an error message and prompts the Administrator to choose a different username.   
2. If the password does not meet security requirements, the system displays an error message and prompts the Administrator to enter a valid password.   
3. If the selected Account is invalid, the system displays an error message and prompts the Administrator to choose a valid Account.   
4. If the system fails to create the Administrator, an error message is displayed, and the new Administrator remains in a draft state for manual correction.  
  
Use Case Name: Assign Administrator Permissions   
Use Case ID: UC-20   
Actors: Administrator, System, Account   
Preconditions: The Administrator is authenticated and has access to the permission assignment interface. A valid Account must exist in the system. The target user must be registered in the system and eligible for administrator permissions.   
Postconditions: The target user is successfully assigned administrator permissions for the selected Account. The system logs the permission assignment action.   
  
Main Flow:   
1. The Administrator navigates to the permission assignment interface.   
2. The Administrator selects an existing user from the system for permission assignment.   
3. The Administrator selects the Account to which the user will be assigned administrator permissions.   
4. The Administrator clicks the "Assign Permissions" button.   
5. The system validates the selected user and Account.   
6. The system assigns administrator permissions to the user for the selected Account.   
7. The system displays a confirmation message indicating the permissions were assigned successfully.   
8. The system logs the permission assignment action.   
  
Alternative Flow:   
1. If the selected user is not valid or not registered, the system displays an error message and prompts the Administrator to select a valid user.   
2. If the selected Account is invalid, the system displays an error message and prompts the Administrator to choose a valid Account.   
3. If the system fails to assign the permissions, an error message is displayed, and the permissions remain unchanged.  
  
Use Case Name: Remove Administrator   
Use Case ID: UC-21   
Actors: Administrator, System, Account   
Preconditions: The Administrator is authenticated and has access to the administrator removal interface. The target Administrator must be registered in the system and associated with a valid Account.   
Postconditions: The target Administrator is successfully removed from the system. The system logs the removal action and updates the Account to reflect the change in administrator status.   
  
Main Flow:   
1. The Administrator navigates to the administrator removal interface.   
2. The Administrator selects a target Administrator from the list of registered users.   
3. The system confirms the target Administrator’s details and their association with an Account.   
4. The Administrator clicks the "Remove Administrator" button.   
5. The system validates the target Administrator and removal permissions.   
6. The system removes the Administrator from the system.   
7. The system updates the Account to remove the Administrator’s access rights.   
8. The system displays a confirmation message indicating the Administrator was removed successfully.   
  
Alternative Flow:   
1. If the selected Administrator is not valid or not registered, the system displays an error message and prompts the Administrator to choose a valid user.   
2. If the target Administrator is the only one with administrative rights for the Account, the system displays a warning message and requires the Administrator to assign new administrative rights before proceeding.   
3. If the system fails to remove the Administrator, an error message is displayed, and the Administrator remains in the system for manual correction.  
  
Use Case Name: View Administrator Logs   
Use Case ID: UC-22   
Actors: Administrator, System   
Preconditions: The Administrator is authenticated and has access to the administrator log viewing interface. The system must have an active log database containing records of administrator actions.   
Postconditions: The Administrator successfully views the logs of administrative actions. The system logs the viewing action.   
  
Main Flow:   
1. The Administrator navigates to the administrator log viewing interface.   
2. The Administrator selects a specific time range or filter for the logs.   
3. The system retrieves the relevant administrator logs from the log database.   
4. The system displays the logs, including details such as action performed, timestamp, and affected entities (e.g., Account, Email, Contact).   
5. The Administrator reviews the logs for auditing or troubleshooting purposes.   
6. The system logs the viewing action for traceability.   
  
Alternative Flow:   
1. If the selected time range or filter is invalid, the system displays an error message and prompts the Administrator to adjust the parameters.   
2. If no administrator logs match the criteria, the system displays a message indicating no logs were found.   
3. If the system fails to retrieve the logs, an error message is displayed, and the Administrator is redirected to the log database for manual review.  
  
Use Case Name: Manage Format Template   
Use Case ID: UC-23   
Actors: Administrator, Format Template, Email   
Preconditions: The Administrator is authenticated and has access to the format template management interface. The system must have an active Format Template module. The Administrator must select an action: "Create Format Template", "Update Format Template", or "Delete Format Template".   
Postconditions: The selected Format Template is successfully created, updated, or deleted in the system. The system logs the action, and changes are reflected in the Email formatting process.   
  
Main Flow:   
1. The Administrator navigates to the format template management interface.   
2. The Administrator selects an action: "Create Format Template", "Update Format Template", or "Delete Format Template".   
3. If creating a template, the Administrator defines the template name and applies formatting rules (e.g., font style, size, color, layout).   
4. If updating a template, the Administrator selects an existing Format Template and modifies its formatting rules.   
5. If deleting a template, the Administrator selects an existing Format Template and confirms the deletion.   
6. The system validates the template name and formatting rules.   
7. The system performs the selected action (create, update, or delete) on the Format Template.   
8. The system displays a confirmation message indicating the action was completed successfully.   
9. The system logs the action for traceability and compliance purposes.   
  
Alternative Flow:   
1. If the template name is not unique, the system displays an error message and prompts the Administrator to choose a different name.   
2. If the formatting rules are incomplete or invalid, the system displays an error message and prompts the Administrator to correct the rules.   
3. If the selected Format Template for updating or deleting is invalid, the system displays an error message and prompts the Administrator to choose a valid template.   
4. If the system fails to perform the selected action, an error message is displayed, and the Format Template remains in its previous state.   
5. If the Administrator cancels the action during the confirmation step, the system returns to the format template list without making any changes.  
  
Use Case Name: Manage Archive Record   
Use Case ID: UC-24   
Actors: Administrator, Email Archive, Archive Record, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the archive record management interface. The system must have an active Email Archive containing Archive Records. The Administrator must select an action: "Create Archive Record", "Update Archive Record", or "Delete Archive Record".   
Postconditions: The selected Archive Record is successfully created, updated, or deleted in the system. The system logs the action, and the Email Archive is updated accordingly to reflect the changes in record management.   
  
Main Flow:   
1. The Administrator navigates to the archive record management interface.   
2. The Administrator selects an action: "Create Archive Record", "Update Archive Record", or "Delete Archive Record".   
3. If creating an archive record, the Administrator enters the record details (e.g., email reference, archiving date, reason for archiving).   
4. If updating an archive record, the Administrator selects an existing Archive Record and modifies its details.   
5. If deleting an archive record, the Administrator selects an existing Archive Record and confirms the deletion.   
6. The system validates the input or selection for consistency and correctness.   
7. The system performs the selected action (create, update, or delete) on the Archive Record.   
8. The system displays a confirmation message indicating the action was completed successfully.   
9. The system updates the Email Archive with the changes, if applicable.   
10. The system logs the action for traceability and compliance purposes.   
  
Alternative Flow:   
1. If the input for creating or updating an archive record is incomplete or invalid, the system displays an error message and prompts the Administrator to correct the information.   
2. If the selected Archive Record for updating or deleting is invalid, the system displays an error message and prompts the Administrator to choose a valid record.   
3. If the system fails to perform the selected action, an error message is displayed, and the Archive Record remains in its previous state.   
4. If the Administrator cancels the action during the confirmation step, the system returns to the archive record list without making any changes.   
5. If the associated Email or Contact for the Archive Record is missing or invalid, the system displays an error message and prompts the Administrator to verify or assign the correct associations.  
  
Use Case Name: Manage Compliance Log   
Use Case ID: UC-25   
Actors: Administrator, Compliance Log, Email Archive, Email, Contact, Account   
Preconditions: The Administrator is authenticated and has access to the compliance log management interface. The system must have an active Compliance Log and Email Archive containing records for compliance tracking. The Administrator must select an action: "View Compliance Log", "Update Compliance Log", or "Delete Compliance Log".   
Postconditions: The selected Compliance Log is successfully viewed, updated, or deleted in the system. The system logs the action, and changes are reflected in the compliance tracking process.   
  
Main Flow:   
1. The Administrator navigates to the compliance log management interface.   
2. The Administrator selects an action: "View Compliance Log", "Update Compliance Log", or "Delete Compliance Log".   
3. If viewing a compliance log, the Administrator selects a Compliance Log entry, and the system retrieves and displays its details (e.g., audit timestamp, email reference, compliance status, and any flagged issues).   
4. If updating a compliance log, the Administrator selects an existing Compliance Log entry and modifies its status or adds notes for clarification.   
5. If deleting a compliance log, the Administrator selects an existing Compliance Log entry and confirms the deletion.   
6. The system validates the action and input for correctness and consistency.   
7. The system performs the selected action (view, update, or delete) on the Compliance Log.   
8. The system displays a confirmation message indicating the action was completed successfully.   
9. The system logs the action for traceability and audit purposes.   
  
Alternative Flow:   
1. If the selected Compliance Log entry is invalid or does not exist, the system displays an error message and prompts the Administrator to select a valid Compliance Log.   
2. If the Administrator attempts to update a Compliance Log entry with incomplete or incorrect information, the system displays an error message and prompts the Administrator to correct the data.   
3. If the system fails to perform the selected action, an error message is displayed, and the Compliance Log remains in its previous state.   
4. If the Administrator cancels the action during the confirmation step, the system returns to the compliance log list without making any changes.   
5. If the associated Email Archive record or Email is missing or invalid, the system displays an error message and prompts the Administrator to verify or assign the correct associations.