

-

From: [REDACTED]
Sent: Friday, November 04, 2005 4:21 PM
To: [REDACTED]
Subject: Email Archive Process.ppt
Attachments: Email Archive Process.ppt

What are/is the new issue with ECRMS?

HOGR6OA-022296

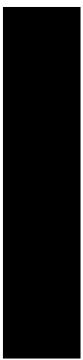
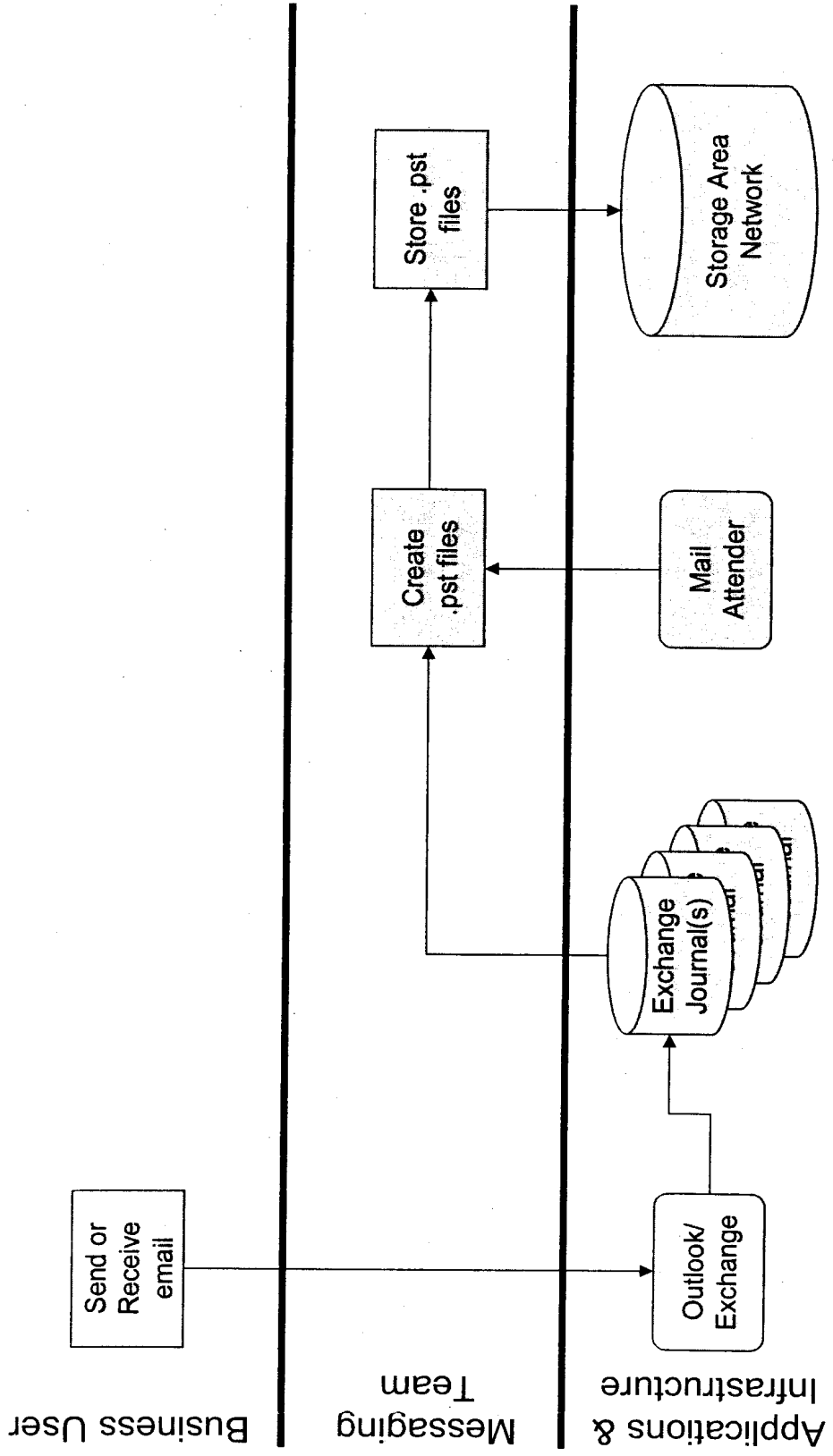
Email Archive Process Risk Mitigation

Discussion Document

October 25, 2005

HOGR60A-022297

There is operational risk in current email storage management processes.



Lost or misplaced email archives may result in an inability to meet statutory requirements.

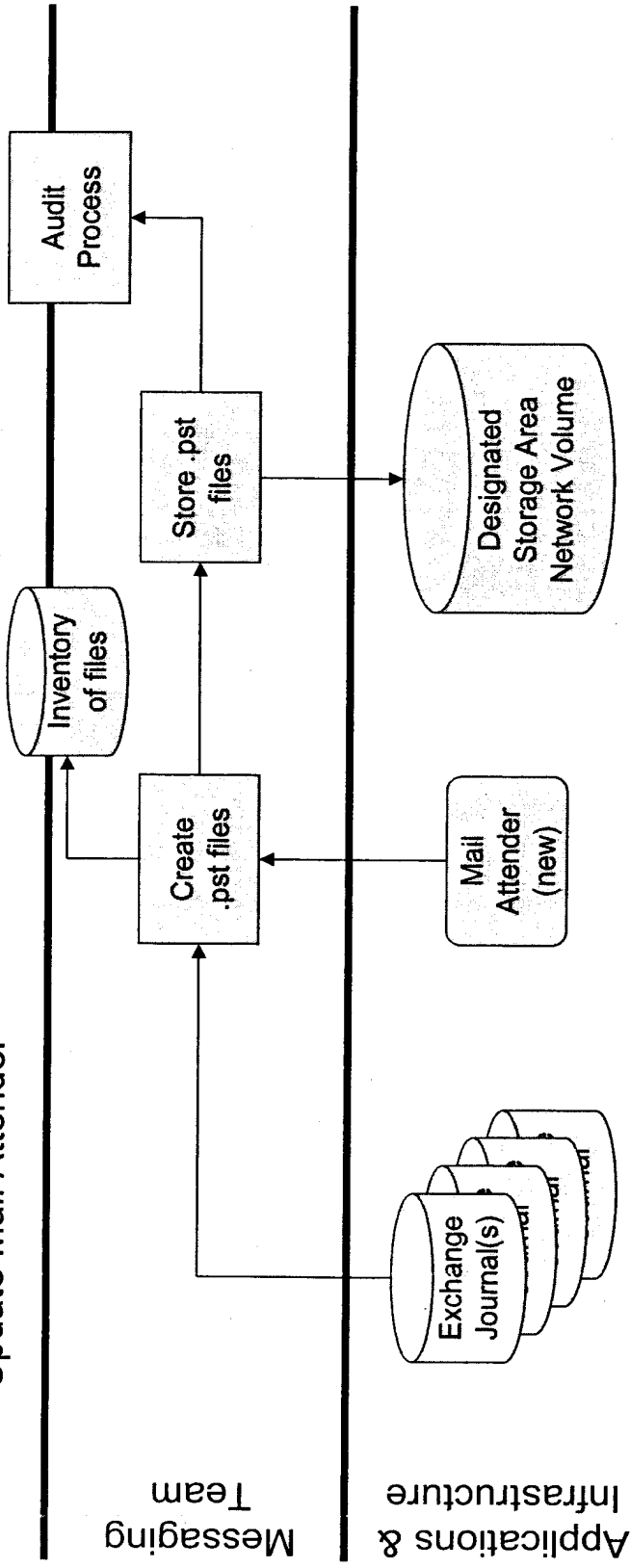
- The email archive process depends on manual operations and monitoring.
 - Institutional knowledge is held by a single administrator
 - The administrator must launch each process and monitor to completion
- Standard operating procedures for email management do not exist
- Automated tools that support the email archive process are not robust
 - The current version of Mail Attender is prone to failure
 - Naming requirements are not fully supported
- Archive process are not monitored with system management tools
 - System management tools can be used to alert when a process fails
 - Completeness of the archive process can be monitored as well
- There is no “dedicated” archive location. Emails have been stored in various locations
 - Storage locations are created whenever there is available space, at the direction of the operator
 - Searches of email in response to statutory requirements may not be complete, creating legal and political risk

This risk can be mitigated.

- Implement interim procedures
 - Daily archive v. system administrator defined periodicity
 - Standard naming conventions
 - Designated storage location(s)
- Update Mail Attender
 - Automated scheduling of the .pst creation and storage process
 - Better and consistent naming support
 - More reliable performance
- Use Microsoft Operation Manager (MOM) system management software to monitor each process and validate the integrity of the entire process
 - Alert the messaging team and NOC when the process fails so that remedial action can be taken immediately
- Implement a dedicate system that is intended for email archive, search and record management functions
 - Using vendor supported technologies to replace tools such as Find It will improve the quality of service
- Systematically- eliminate manual processes and potential points of failure from the process

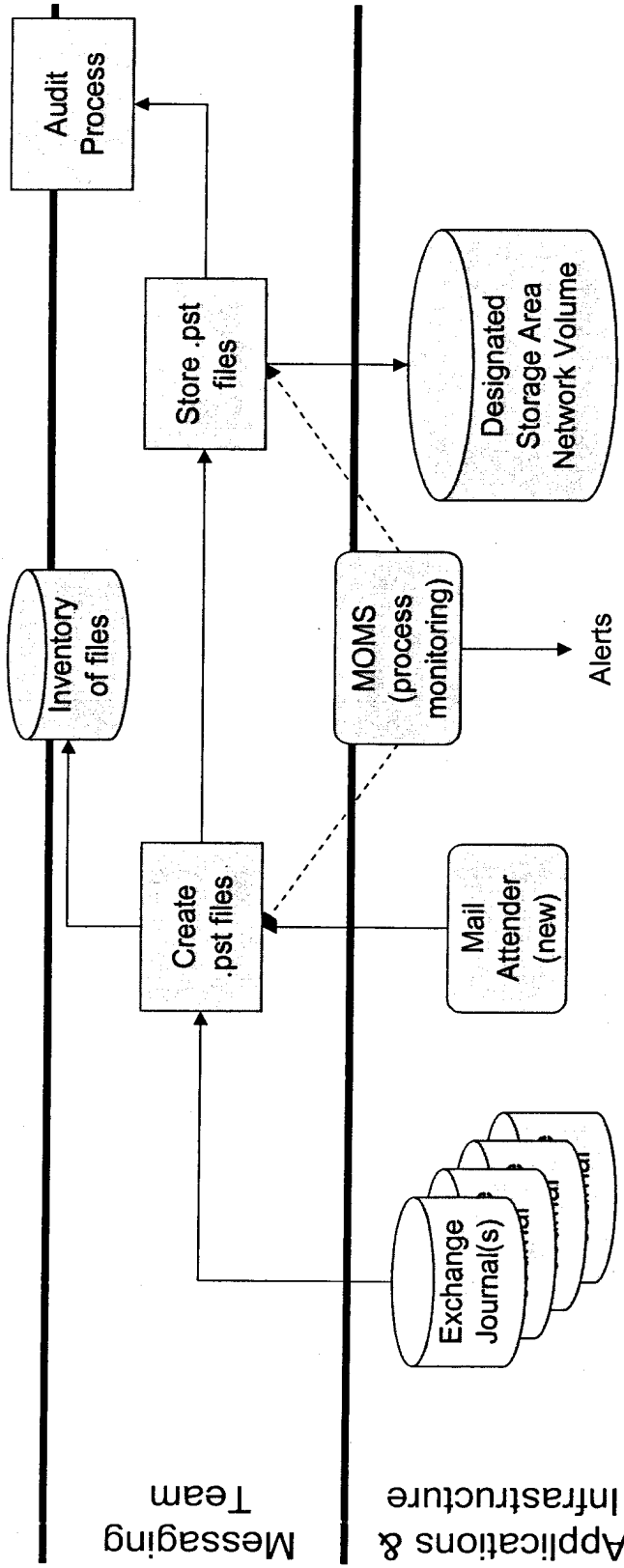
However, several steps...

- Release 1
 - Implement procedures
 - Update Mail Attender



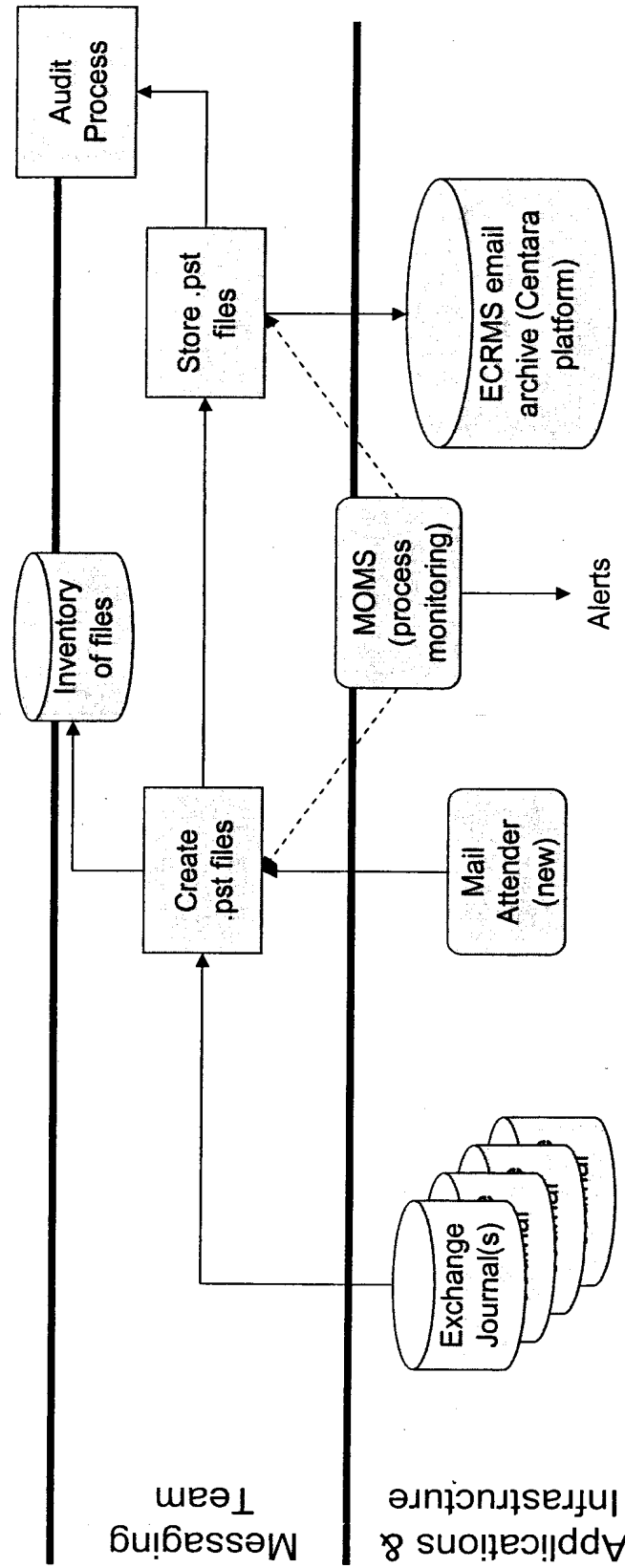
....must be taken....

- Release 2
 - Implement system monitoring



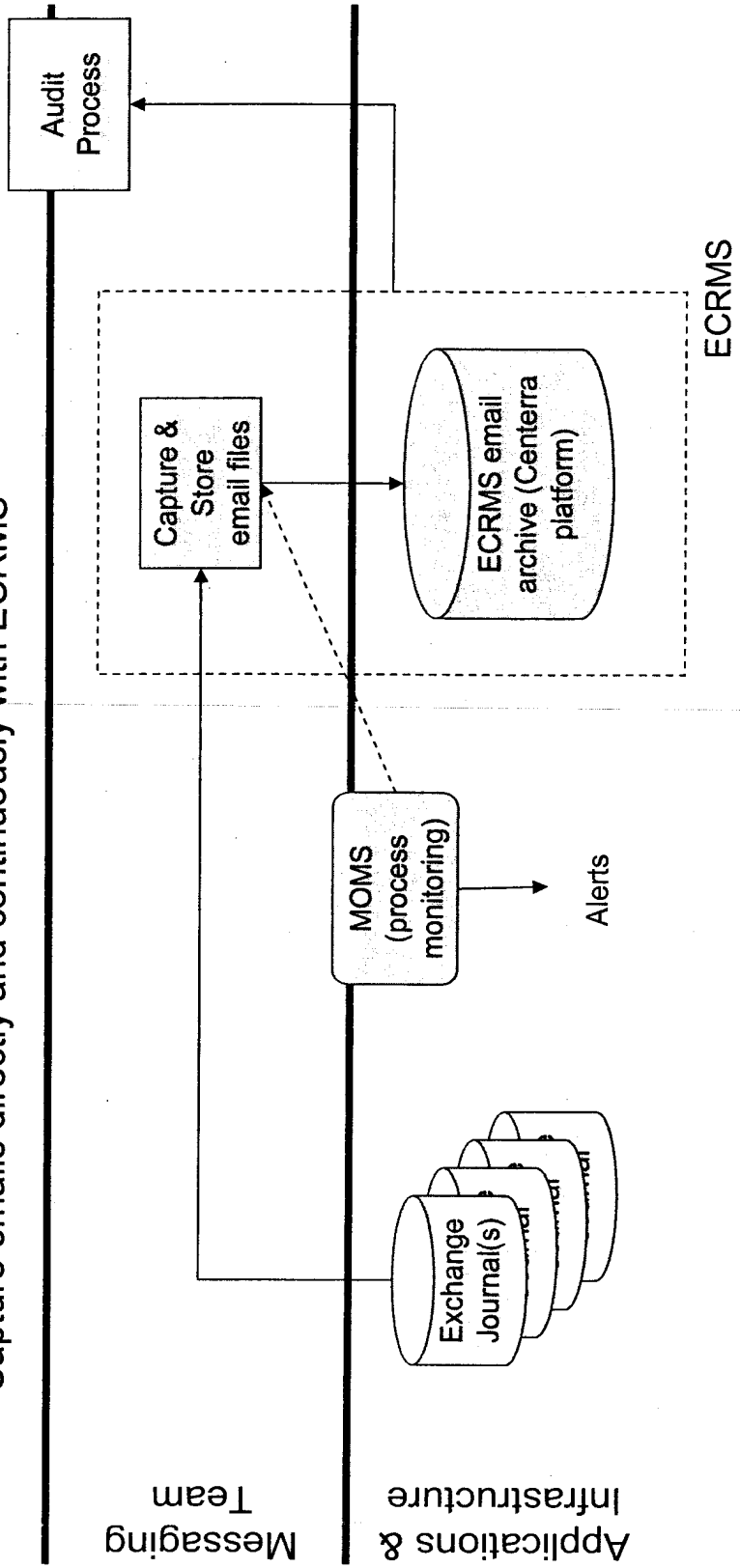
....over time....

- Release 3
 - Implement dedicated email archive



...to close exposures to risk.

- Release 4
 - Upgrade Exchange servers to Exchange 2003 (for “enveloping” capability)
 - Capture emails directly and continuously with ECRMS



Senior management authorization is required to proceed with risk mitigation recommendations.

- Procedures, tool upgrades and storage management decisions can be made by OCIO.
- Conversion of old emails to the ECRMS platform is time consuming. During the conversion process, the current storage volume and the ECRMS (Centerra) storage volume will need to be searched.
 - OCIO currently searches multiple volumes with Lotus Notes Mail and MS Exchange email platforms.
- Use of the ECRMS platform requires management authorization.
 - “Release 3” uses the ECRMS platform for archiving. No change to search tools is implied.
 - “Release 4” stores the email directly. Current search tools used on .pst files will need to be replaced. However, the *Find It* tool is not a vendor supported product and should be replaced.
- Failure to mitigate operational risks may result in an inability to comply with statutory requirements.

There are significant benefits to the recommendations.

- Reduces the frequency of error typical of manual processes.
- Closes exposure to risk by isolating the email archive from data and file storage that is managed to support production applications where data is more volatile.
- Provides safeguards to assure the integrity of the process.
 - System monitoring
 - Audit processes
 - Business rules and controls
- Manages data with supported technologies.