

Hybrid Cloud Migration for Messaging, Collaboration, and IT Support Operations

IT Service and Support Capstone System Design and Requirements Artifact

Executive Summary

This capstone project presents a complete system design and requirements plan for migrating a 250-user organization from a traditional on-premises messaging and collaboration environment to a secure Microsoft 365 hybrid cloud model. The current environment relies on Exchange, Active Directory, SharePoint, file services, VPN access, backup systems, and fragmented administrative tools. The design addresses recurring support pain points including slow Outlook performance, calendar sync failures, mobile email issues, password resets, mailbox permission problems, SharePoint access delays, and limited support visibility.

The proposed solution combines Microsoft 365, Azure AD, Azure AD Connect, Exchange Online, SharePoint Online, Teams, OneDrive, Exchange Online Protection, MFA, Conditional Access, monitoring tools, backup and recovery planning, role-based access, user training, support runbooks, and a proposed administrative support portal. The project demonstrates practical IT Service and Support skills across requirements gathering, system analysis, cloud migration planning, support workflow design, security planning, documentation, troubleshooting, cost modeling, and operational readiness.

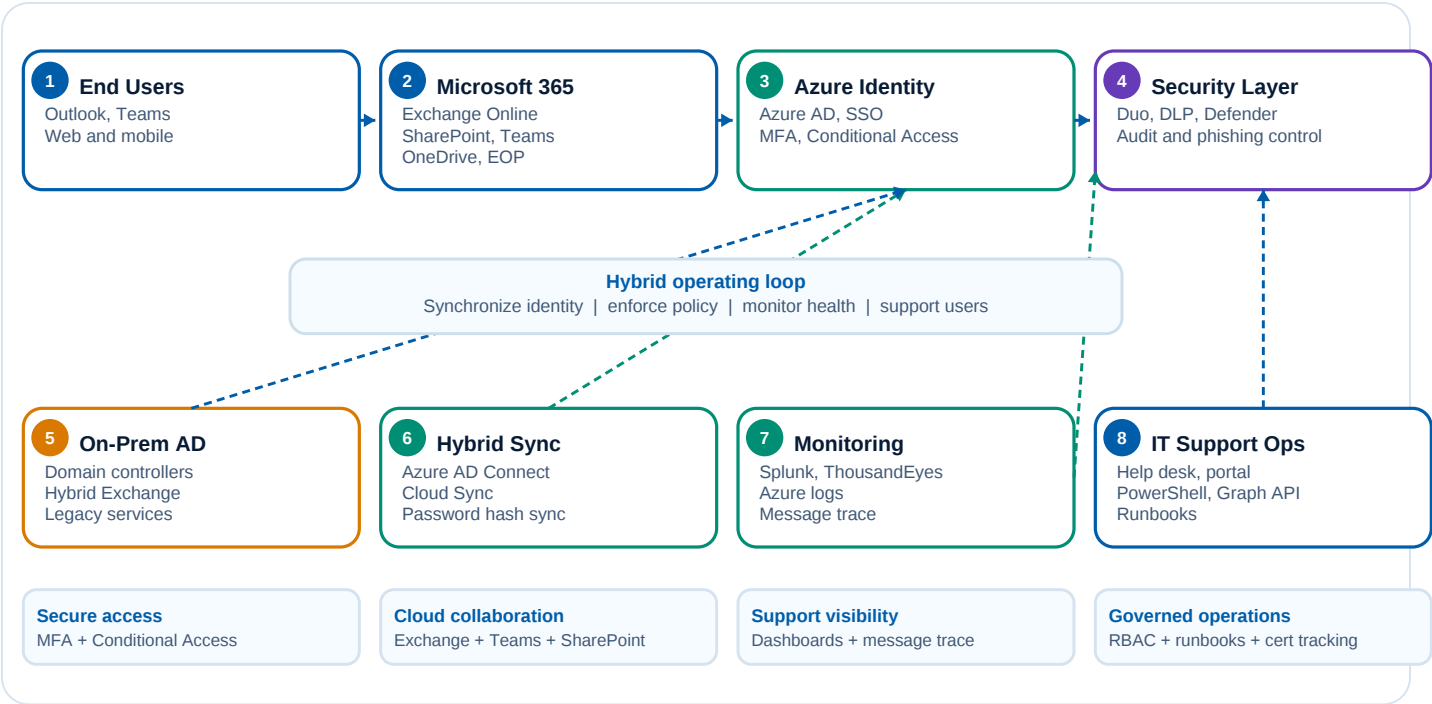
CURRENT-STATE PROBLEM

Support Area	Operational Challenge
Messaging	Slow Outlook performance, Exchange disconnects, shared mailbox issues, and mail-flow troubleshooting.
Collaboration	SharePoint sync delays, inconsistent Teams integration, and fragmented document access.
Identity	Manual AD administration, password resets, and limited modern access policy controls.
Security	Need for stronger MFA, DLP, audit trails, Conditional Access, and phishing protection.

TARGET-STATE SOLUTION

Layer	Design Response
Cloud Services	Exchange Online, SharePoint Online, Teams, OneDrive, Microsoft 365 Admin Center.
Identity	Azure AD, Azure AD Connect, SSO, MFA, Conditional Access, role-based access.
Visibility	Splunk for Azure, Cisco ThousandEyes, Azure logs, message trace, audit reports.
Support	Runbooks, training, help desk workflows, admin portal concept, knowledge base.

HYBRID CLOUD MESSAGING AND COLLABORATION SUPPORT ARCHITECTURE



System Design and Requirements

DESIGN OVERVIEW

The target system is a hybrid cloud architecture that connects existing on-premises identity and support services with Microsoft 365. On-premises Active Directory remains the source for selected identity attributes while Azure AD Connect synchronizes users, groups, devices, and authentication data into Azure AD. Exchange Online becomes the primary email platform while a hybrid Exchange role remains available for mail routing, compliance, transition support, and selected local requirements.

The design supports secure remote work, centralized administration, and improved help desk response. Support staff can use Microsoft 365 Admin Center, Exchange Admin Center, Azure Admin Portal, PowerShell, monitoring dashboards, and the proposed support portal to manage users, troubleshoot access, verify mail flow, and respond to incidents.

SOLUTION COMPONENTS

Layer	Technology	Purpose
Identity	Azure AD / Azure AD Connect	Synchronizes identities, supports SSO, MFA, Conditional Access, and group-based access.
Messaging	Exchange Online / Hybrid Exchange	Provides cloud email, calendaring, mail flow, shared mailbox support, and transition compatibility.
Collaboration	SharePoint Online / Teams / OneDrive	Modernizes file access, document collaboration, meetings, chat, and department workspaces.
Security	EOP, Defender, DLP, Duo, Audit Logs	Improves phishing protection, account security, data protection, and compliance reporting.
Operations	M365 Admin Center, PowerShell, Graph API	Supports provisioning, reporting, scripting, licensing, mail-flow checks, and support automation.
Monitoring	Splunk for Azure / Cisco ThousandEyes	Improves service health visibility, event correlation, network monitoring, and escalation.

ACCESS CONTROL MODEL

Global Admin

Restricted to designated cloud leads governs tenant-wide settings.

Exchange Admin

Mail flow, mailbox management, transport rules, shared mailbox support.

Help Desk T1

Password resets, account unlocks, basic MFA assistance, user intake.

Compliance

eDiscovery, legal hold, DLP reports, audit log review.

Permissions follow least privilege. Help desk staff receive controlled access for common support tasks, while high-impact changes require escalation or approval.

ADMINISTRATIVE SUPPORT PORTAL CONCEPT

Function	Support Value	Backend
User provisioning	Speeds onboarding/offboarding and reduces manual account steps.	Azure AD, AD, Graph API
Password/MFA support	Addresses high-volume help desk requests with controlled workflows.	Azure AD, Duo, SSO
Mailbox permissions	Improves shared mailbox and delegation troubleshooting.	Exchange Online PowerShell
Mail-flow checker	Supports delivery diagnosis, routing validation, and message trace escalation.	EAC, message trace, EOP
Certificate tracking	Prevents expired TLS certificates from interrupting mail flow.	Certificate DB, alert job

CORE REQUIREMENTS MATRIX

Requirement	Design Response
Identity sync	Azure AD Connect / Cloud Sync
Secure access	MFA, Conditional Access, Cisco Duo
Email modernization	Exchange Online with hybrid mail flow
Collaboration	Teams, SharePoint Online, OneDrive
Monitoring	Splunk, ThousandEyes, Azure logs
Recovery	Azure Backup, Blob Storage, retention plans

GOVERNANCE CONTROLS

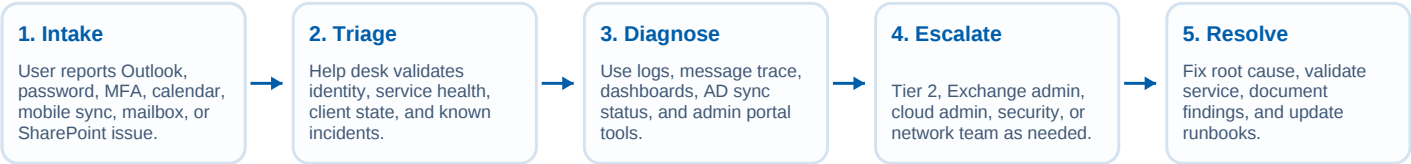
MFA Conditional Access RBAC DLP Audit Logs

eDiscovery Certificate Tracking Change Control

The design balances user productivity with controlled administration. Security controls protect privileged actions, cloud access, external collaboration, shared mailboxes, and sensitive data movement. Audit and monitoring data remain available for support, compliance, and post-incident review.

Support Operations, Data Governance, and Reporting

IT SUPPORT WORKFLOW



RECURRING SUPPORT SCENARIOS

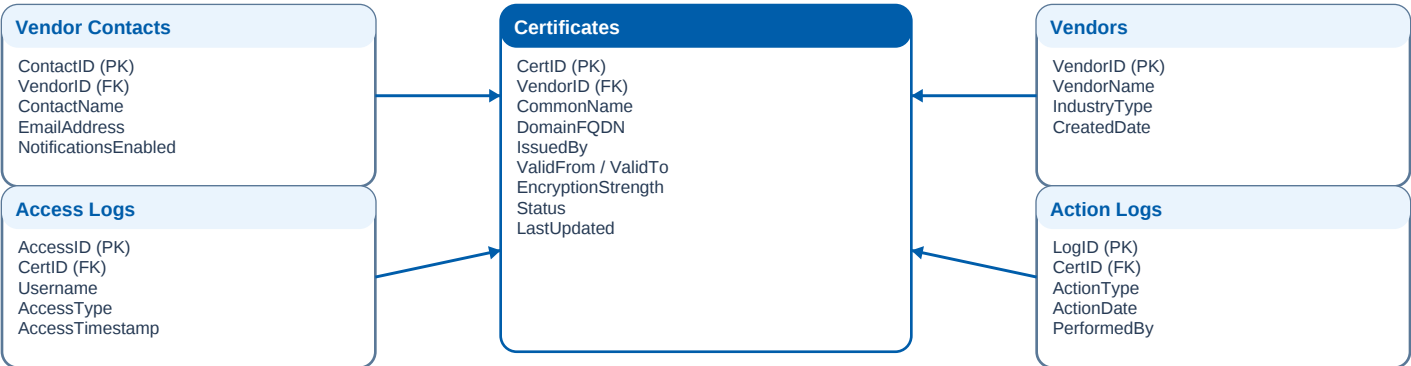
Ticket Type	Tools / Data Used
Password reset / account lockout	Azure AD, on-prem AD, MFA logs, support portal workflow.
Outlook not connecting	Service health, client auth state, mailbox status, message trace.
Calendar or mobile sync issue	Exchange Online, device status, Outlook profile, policy checks.
SharePoint access problem	Group membership, site permissions, sharing policy, audit logs.
Suspicious email or phishing	EOP, Defender, DLP, audit trail, SIEM alerts.

REPORTS AND VISIBILITY

Report	Audience
Azure AD sign-in and MFA reports	Security, help desk, administrators
Exchange Online mail-flow reports	Messaging team, support escalation
SharePoint and Teams usage reports	Admins, managers, project owners
DLP and incident reports	Security and compliance staff
Certificate health summary	Email security, cloud admin, leadership

CERTIFICATE MANAGEMENT DATA MODEL

The design includes a focused TLS certificate management database to protect hybrid mail flow and vendor communication. The database tracks certificate ownership, domain names, expiration dates, encryption strength, status, renewal actions, vendor contacts, and access logs. This gives administrators early warning before certificate expiration and creates an audit trail for compliance.



DATA RETENTION

Certificates: retained for five years after expiration. **Vendor records:** retained while the relationship remains active. **User access logs:** retained for at least two years. **Certificate action logs:** retained for five years to support compliance, troubleshooting, and audit review.

OPERATIONAL READINESS

Runbooks, QA checklists, training guides, support workflows, and migration wave logs are stored in a central knowledge base. This reduces knowledge silos and helps future staff understand why the design was built, how to support it, and where to find authoritative procedures.

OPERATIONAL DELIVERABLES CREATED BY THE DESIGN

Deliverable	Purpose	Support Value
Runbooks	Step-by-step guidance for common admin tasks and escalations.	Improves consistency and reduces guesswork.
QA and migration checklists	Pre-migration, mid-migration, and post-cutover validation.	Prevents missed steps during change windows.
Training materials	End-user and administrator guidance for Outlook, Teams, SharePoint, MFA, and support requests.	Improves adoption and reduces avoidable tickets.
Knowledge base	Central location for diagrams, troubleshooting notes, known issues, and final as-built records.	Keeps the environment maintainable after go-live.

Implementation, Budget, Recovery, and Skills Demonstrated

IMPLEMENTATION STRATEGY

Phase	Purpose	Validation
Planning	Scope, stakeholders, risk, budget, architecture.	Approved plan
Pilot	Migrate IT and test accounts first.	AD sync, mail flow, MFA
Wave 1	Finance, HR, Marketing.	User access and UAT
Wave 2	Sales, Legal, Operations.	Teams, SharePoint, Outlook
Executive	High-security users and VIP mailboxes.	DLP and audit checks
Stabilize	Support, tune, train, document.	Ticket trends and QA

MAINTENANCE AND RECOVERY

The maintenance plan uses recurring cloud service reviews, update checks, access reviews, monitoring alerts, security policy validation, and formal change control. Backup and recovery planning covers Exchange Online retention, SharePoint and OneDrive versioning, Azure Blob storage, Active Directory snapshots, off-site backup, and scheduled failover tests.

Area	Control
Email	Retention, archiving, mail-flow validation, recovery playbooks.
Files	Version history, backup, permissions review, restore process.
Identity	Azure AD Connect status, MFA reports, access reviews.
Security	DLP, Defender, Sentinel/Splunk alerts, audit review.

BUDGET AND ROI SUMMARY

\$486,760

Total project budget model including hardware, software, cloud, staffing, setup, and support.

250 Users

Migration scenario size for messaging, collaboration, identity, training, and support planning.

5 Years

Business case horizon for modernization, operating cost comparison, and savings analysis.

PROJECT COST BY CATEGORY

Staff and engineering effort are the largest category, followed by cloud services and support.



VALUE CASE

Benefit	Operational Impact
Centralized support	Less tool switching, faster triage.
Cloud collaboration	Better remote access and shared workspaces.
Real-time monitoring	Faster issue detection and escalation.
Security modernization	MFA, DLP, auditability, Zero Trust concepts.

SKILLS DEMONSTRATED

Requirements Gathering

Questionnaire, support pain points, admin needs, project limits.

System Analysis

Current-state environment, dependencies, risks, constraints.

Cloud Migration

Microsoft 365, Azure AD, Exchange Online, SharePoint, Teams.

Support Design

Help desk workflow, escalation paths, runbooks, training.

Security Planning

MFA, Conditional Access, DLP, RBAC, certificates, audit logs.

Data Modeling

Certificate database, reports, retention, access logs.

Budget Modeling

Hardware, software, cloud, staffing, support, ROI planning.

Documentation

Requirements, design, QA, reflection, presentation-ready artifact.

LINKEDIN FEATURED ARTIFACT FIELDS

Title: Hybrid Cloud Migration for Messaging, Collaboration, and IT Support Operations

Description:

Capstone system design and requirements artifact for my IT Service and Support degree at Wake Technical Community College. This project demonstrates a complete hybrid cloud migration plan for a 250-user organization, including Microsoft 365, Azure AD, Exchange Online, SharePoint, Teams, MFA, Conditional Access, monitoring, support workflows, backup and recovery, budget modeling, and help desk operational planning.