Application Deployment Design Plan

Workload Optimization & Migration to Azure

6450-ARMS

Deployment Design Summary (Executive Summary)

This document outlines the Deployment Design for the Accounts Receivable Management System (MOTS 6450) application from on-premises to Azure. The deployment design summarizes the details required for the application to deploy successfully to Azure. The document describes the migration/deployment strategy for the application. It includes details such as the target architecture and the mapping of VMs to the application. The document includes a link to the Deployment/Migration Playbook which provides task-level details of activities along with ownership, dates, and status. This document will be appended by the Deployment playbook which will include all necessary cutover steps, and which will be documented in conjunction with AT&T application and operations team.

The Deployment Design is based on:

- Information available in MOTS: https://mots.web.att.com/asset_detail/6450
- Information collected from the Migration Catalog in CRM
- The results of the Cloud Suitability Assessment
- Compatibility and supportability assessments
- Information and artifacts provided by AT&T Inc such as the Unified Assessment Questionnaire (UAQ) and details gathered during Architectural Design Sessions.

1.1 Source Application Details

Application for accounts receivables collections for legacy B, S, and T wholesale and business retail customers. Supports SOX biller validation and AR results reporting.

1.2 Application Architecture

The diagram below shows the source architecture for 6450 - ARMS and interfacing applications.

ARMS_Highlevel_Arch.pdf

1.3 Application Servers

The table below contains the application compute details which include environment, server role, on-premises utilization metrics, etc. These considerations will be used when planning to migrate the infrastructure to Azure.

Utilization Data: Specify the duration of performance data used for Utilization in the table below: xx days.

Prod												
Source Server Name (FQDN)	**IP Address**	**Operating System**	**CPU Cores**	**Memory (GB)**	**Allocated. Disk Size (GB)**	**Environment**	**Server Role**	**CPU Utilized (95th Percentile)**	**Override CPU Utilized (95th Percentile)**	**Avg Memory Utilized (%)**	**Override Avg Memory Utilized (%)**	**Raid Number**
CLDPRD8IIS61975.itservices.sbc.com	135.143.107.161	Windows 2016	1	4	240	Production	Application	15		75		
CLDPRD8SQL74546.itservices.sbc.com	135.143.107.160	Windows 2016	1	32	4580	Production	DB Server	15		98		

Non-Prod												
Source Server Name (FQDN)	**IP Address**	**Operating System**	**CPU Cores**	**Memory (GB)**	**Allocated. Disk Size (GB)**	**Environment**	**Server Role**	**CPU Utilized (95th Percentile)**	**Override CPU Utilized (95th Percentile)**	**Avg Memory Utilized (%)**	**Override Avg Memory Utilized (%)**	**Raid Number**
CLDCER8SQL40636.itservices.sbc.com	135.41.174.113	Windows 2019	1	64	2007	Test	DB Server	8		99		
CLDCER8SQL51508.itservices.sbc.com	10.99.234.193	Windows 2016	1	64	3584	Test	Web Server	15		67		
CLDCER8IIS48630.itservices.sbc.com	135.41.174.114	Windows 2016	1	4	235	Test	DB Server	10		75		

1.4 Application Storage

The table below contains the application disk details, which include disk size, number of disks, etc. These considerations will be used when planning to size the storage in Azure.

Prod						
Source Server Name (*.vci.att.com)	**Environment**	**Number of Disks**	**OS Disk Size (GB)**	**Disk Size (GB)**	**Max. IOPS (Total)**	**Max. Throughput (MBps)**
CLDPRD8SQL74546.itservices.sbc.com	Production	9	80	4580	32K	NA
CLDPRD8IIS61975.itservices.sbc.com	Production	9	80	240	566	NA

Non-Prod						
Source Server Name (*.vci.att.com)	**Environment**	**Number of Disks**	**OS Disk Size (GB)**	**Disk Size (GB)**	**Max. IOPS (Total)**	**Max. Throughput (MBps)**
CLDCER8SQL40636.itservices.sbc.com	Test	9	80	2007	97K	NA
CLDCER8SQL51508.itservices.sbc.com	Test	9	80	3584	36K	NA
CLDCER8IIS48630.itservices.sbc.com	Test	9	80	235	5K	NA

1.5 Application Interfaces and Dependencies

The table below lists the application and database related dependency information.

Source Application Acronym	MOTS ID	Source Server Name	Location	Input/Output	Target Server IP Address (or URL for HTTP connections)	Protocol	Port	Interface Type	Target Application/ Server Name	Encrypted?	TLS 1.2 Compliant?	Current Latency	Comments
AIRS	1174	155.241.248.90	On-Prem	Input	135.170.230.144 135.170.242.10	FTP	1364	File Transfer	ARMS	No	No	NA	NA
THRIFTY - AS400	13261	135.38.22.14	On-Prem	Input	135.170.230.144 135.170.242.10	ConnectDirect	445	File Transfer	ARMS	No	No	NA	NA
ISB	14084	fts1.ims.att.com fts1dal.mvs.sbc.com	On-Prem	Input	135.170.230.144 135.170.242.10	ConnectDirect	1364	File Transfer	ARMS	No	No	NA	NA
ECS	14883	162.248.83.35	On-Prem	Input	135.170.230.144 135.170.242.10	ConnectDirect	1364	File Transfer	ARMS	No	No	NA	NA
PD Track	19255	ACE2P19255AP002	On-Prem	Input	135.170.230.144 135.170.242.10	Connect Direct Secure+	1364	File Transfer	ARMS	Yes	No	NA	NA
CENT Singleview	20616	135.62.134.250 135.41.174.113	On-Prem	Input	135.170.230.144 135.170.242.10	ConnectDirect	1364	File Transfer	ARMS	No	No	NA	NA
AspectAOD	20943	NCCHAR9ASPALM01	On-Prem	Input	135.170.230.144 135.170.242.10	ConnectDirect	1364	File Transfer	ARMS	No	No	NA	NA

ATWS	21685	ATMAPXFER01CN ATMATXFER01CN 162.248.83.36 162.248.83.46 135.66.64.105 162.248.83.36 162.248.83.46 135.41.174.113 135.41.174.113 162.248.83.36 162.248.83.46	On-Prem	Input	135.170.230.144 135.170.242.10	ConnectDirect	1364	File Transfer	ARMS	No	No	NA	NA
EDD	17689	NA	On-Prem	Input	135.170.230.144 135.170.242.10	Data Router	1364	File Transfer	ARMS	No	No	NA	NA
TAXI	578	NA	On-Prem	Input	135.170.230.144 135.170.242.10	ODBC - DB2 Connect	1364	DB Connectivity	ARMS	No	No	NA	NA
CENET(Web phone)	2022	NA	On-Prem	Input	135.170.230.144 135.170.242.10	ODBC	1364	DB Connectivity	ARMS	No	No	NA	NA
TLD-PROD(used by DMT)	7547	NA	On-Prem	Input	135.170.230.144 135.170.242.10	ODBC / Oracle Direct DB Connection	1364	DB Connectivity	ARMS	No	No	NA	NA
RBS(File placed manually Nancie	3958	NA	On-Prem	Input	135.170.230.144 135.170.242.10	SQLNET - Manual Export to local drive	1364	DB Connectivity	ARMS	No	No	NA	NA
CPE Billing	5337	NA	On-Prem	Input	135.170.230.144 135.170.242.10	File Share	1364	File Transfer	ARMS	No	No	NA	NA
JDE	12627	NA	On-Prem	Input	135.170.230.144 135.170.242.10	NA	1364	NA	ARMS	No	No	NA	NA
VTNS	13440	NA	On-Prem	Input	135.170.230.144 135.170.242.10	File Share	1364	File Transfer	ARMS	No	No	NA	NA
RPMS via business Ops	NA	NA	On-Prem	Input	135.170.230.144 135.170.242.10	File Share	1364	File Transfer	ARMS	No	No	NA	NA

CIA ABS	NA	NA	On-Prem	Input	135.170.230.144 135.170.242.10	File Share	1364	File Transfer	ARMS	No	No	NA	NA
SDN-ONENET	13715	NA	On-Prem	Input	135.170.230.144 135.170.242.10	File Share	1364	File Transfer	ARMS	No	No	NA	NA
ATBS	13806	158.155.92.130	On-Prem	Input	135.170.230.144 135.170.242.10	ConnectDirect	1364	File Transfer	ARMS	No	No	NA	NA
UNIVERSAL BILLER RESULTS	14191	NA	On-Prem	Input	135.170.230.144 135.170.242.10	File Share	1364	File Transfer	ARMS	No	No	NA	NA
Billing Consolidator	14972	135.48.240.49	On-Prem	Input	135.170.230.144 135.170.242.10	ConnectDirect	1364	File Transfer	ARMS	No	No	NA	NA
BEST	17955	best-eastus2-prod-app-vm-01.az.3pc.att.com best-eastus2-prod-app-vm-02.az.3pc.att.com	On-Prem	Input	135.170.230.144 135.170.242.10	Connect Direct Secure+	1364	File Transfer	ARMS	Yes	No	NA	NA
GISDN	18756	NA	On-Prem	Input	135.170.230.144 135.170.242.10	File Share	1364	File Transfer	ARMS	No	No	NA	NA
ANC Biller (Convergsys)	NA	NA	On-Prem	Input	135.170.230.144 135.170.242.10	ODBC and File received from Net Cracker	1364	DB Connectivity	ARMS	No	No	NA	NA
MplsTools	24511	CAHYWR1MPLSAD01	On-Prem	Input	135.170.230.144 135.170.242.10	Direct DB Access / SQL Linked Server	1364	DB Connectivity	ARMS	No	No	NA	NA
TERADATA	NA	bhpm1.bhdc.att.com	On-Prem	Input	135.170.230.144 135.170.242.10	ODBC / Teradata Direct DB Access	1364	DB Connectivity	ARMS	No	No	NA	NA
OMNIBILL (ACC)	13630	ACE2P13630AP001 135.170.196.255 GAALPA1DTS1XD04	On-Prem	Input	135.170.230.144 135.170.242.10	Connect Direct Secure+	1364	File Transfer	ARMS	Yes	No	NA	NA
ARMS	6450	,155.241.248.77	On-Prem	Output	Not Known	ConnectDirect	1364	File Transfer	AIRS	No	No	NA	NA

ARMS	6450	a7db.it.att.com	On-Prem	Output	Not Known	File Share and ODBC Connection	445	File Transfer	OARS(Additional analysis with DMT team) via business OPS	No	No	NA	NA
ARMS	6450	CLDPRD0SRV06317	On-Prem	Output	Not Known	ConnectDirect	1364	File Transfer	CCProcMech	No	No	NA	NA
ARMS	6450	ALHOOV1MPLSAA01	On-Prem	Output	Not Known	Connect Direct Secure+	1364	File Transfer	ADAPT	Yes	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	ConnectDirect	1364	File Transfer	Equifax(Need more analysis)	No	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	Data Router	443	File Transfer	EDD	No	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	Data Router	443	File Transfer	ASLA	No	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	ODBC - DB2 Connect / ConnectDirect	1521	DB Connectivity	TAXI	No	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	ODBC - DB2 Connect	1521	DB Connectivity	ExClaim	No	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	File Share	445	File Transfer	CPE Billing(engage DMT for more details)	No	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	ConnectDirect	1364	File Transfer	ATT MACS	No	No	NA	NA
ARMS	6450	ATMAPXFER01CN ATMATXFER01CN 162.248.83.36 162.248.83.46 135.66.64.105	On-Prem	Output	Not Known	ConnectDirect	1364	File Transfer	ECS	No	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	Connect Direct	1364	File Transfer	CCAX	No	No	NA	NA
ARMS	6450	NCCHAR9ASPALM01	On-Prem	Output	Not Known	ConnectDirect	1364	File Transfer	AspectAOD(Replaced by MOTS# 17706 (Aspect Unified IP Platform))	No	No	NA	NA
ARMS	6450	CAHYWR1MPLSAD01 ACE2P26718SQ001.az.3pc.att.com ACE2D26718SQ001.az.3pc.att.com	Azure	Output	Not Known	Direct DB Access / SQL Linked Serv1433er	1521	DB Connectivity	MplsTools	No	No	NA	NA

ARMS	6450	scd-sna-0001	On-Prem	Output	Not Known	Connect Direct	1364	File Transfer	WIFI-BS(need more information)	Yes	No	NA	NA
ARMS	6450	NA	On-Prem	Output	Not Known	Connect Direct Secure+	1364	File Transfer	CRFT	Yes	No	NA	NA

1.6 Application SLA Details

The table below provides application performance SLAs. These SLAs will be the benchmark for conducting performance testing during MAT.

The table below provides application performance SLAs. These SLAs will be the benchmark for conducting performance testing during MAT.

RPO <= 72 hours and RTO <= 14 days
Recovery Type - Application Impact Analysis (AIA) – 2B
Recovery Type Implemented (RTI) - 3B

Source Application/Server Name	Recovery Point Objective	Recovery Time Objective	Downtime Allowed in hours
CLDPRD8IIS61975.itservices.sbc.com	<= 72 hours	<= 14 days	RTO >28 days
CLDPRD8SQL74546.itservices.sbc.com	<= 72 hours	<= 14 days	RTO >28 days
CLDCER8SQL40636.itservices.sbc.com	<= 72 hours	<= 14 days	RTO >28 days
CLDCER8SQL51508.itservices.sbc.com	<= 72 hours	<= 14 days	RTO >28 days
CLDCER8IIS48630.itservices.sbc.com	<= 72 hours	<= 14 days	RTO >28 days

1.7 Application Owner Details

The table below lists the application owners along with their roles and contact details.

Name	Role	Contact Details
MARTIN KELLY	Technical Director	mk8945@att.com
KIMBERLY A FOPPE	Director	km0347@att.com
ERIC D BOYER	VP IT	eb5490@att.com
TERRY L GARGUS	Application Architect	tg0276@att.com
SAURABH DHANOTIA	Application DBA	sd065j@att.com

2.1 Migration Strategies

The table below provides the details for the Accounts Receivable Management System application migration strategy, primarily focusing on database migration strategy and application deployment.

Migration Strategy	Description
App tier OS ->> Source: Desktop Application (C++) & Apache Tomcat 8.5 Target: Azure App Service (Tomcat 9.0)	The client application is presently a desktop application written on C++. It will be rewritten in Angular 9, Spring boot 5.3 as a web application and deployed to Azure App Service (PaaS) on Tomcat 9.0.
OS ->> Source: Windows Server 2016 (Prod DB) & Windows Server 2019 (Pre-Prod DB) Target: Windows Server 2019 (Prod DB & Pre-Prod DB)	Currently database is hosted on Windows Server 2016 (Prod DB) and Windows Server 2019 (Pre-prod DB). With migration to Azure, operating system will be upgraded to use Windows Server 2019 for both Prod and Pre-prod DB
DB tier: Source: SQL Server Standard Edition 2014 Target: SQL Server Standard Edition 2016	The On-premises database (hosted on SQL Server Standard Edition 2014) will be migrated to SQL Server Standard Edition 2016 using IaaS VM. Along with the migration to Azure, SSIS packages will also be migrated to SQL Server 2016
Protocol changes-Encryption Source: Connect: Direct for Windows 4.7 Target: Connect: Direct Secure+ for Windows 6.1	The On-premises file fed to/from interfacing systems via Connect: Direct for Windows 4.7. With migration to Azure, protocol will be encrypted with Connect: Direct Secure+ 6.1 for Windows.
MTA Agent - Postfix 3.5.8	smtptls.it.att.com:25 will be used along with an MTA host postfix provisioned out of the App RHEL VM.

2.2 Cloud Suitability Assessment

To determine if the application servers were suitable for cloud migration, the assessment team considered a variety of factors. These factors included: current technology stack and software versions, hardware requirements, application interfaces and protocols, and Azure security requirements.

Cloud pre-assessment and assessment activities included completing the UAQ (Unified Assessment Questionnaire), interviewing application owners about the application architecture through discovery sessions, and conducting Architectural Design Sessions (ADS).

During assessment, the migration team performed the following high-level activities:

•Architectural Design Sessions were scheduled with the application team to finalize the target design of the application.
•Necessary binaries for application and database installation were requested from the respective teams.
•Service dependency mapping was done to understand all the internal and external interfaces with the application.
•BOM mapping was done to compute Azure SKUs, considering required CPU cores and memory utilized by on-premises servers.

See the next section for the results of the assessment.

Technology Type	Technology	Version	Vendor	Option	Recommended Technologies	Override Technologies	Raid Number
Software Development	Microsoft SQL Server 2016 Standard Edition	2017	Microsoft Corp.	IaaS	Visual Studio Professional 2017		
Data Management	Microsoft SQL Server 2016 Standard Edition	13.3.7016.1	Microsoft Corp.	IaaS	SQL Server Standard Edition 2014		
Data Management	SQL Server Standard Edition	2008 All	Microsoft Corp.	IaaS	SQL Server Standard Edition 2014		
Middleware	Tomcat	8.5.72	Apache Software Foundation	PaaS	Azure App Service (PaaS) on Tomcat 9.0		
Infrastructure Services & Management	Connect:Direct for Windows	4.7.04	IBM Corp	IaaS	Connect: Direct Secure+ for Windows 6.1		

2.3 Results

Servers were assessed for cloud suitability. The following table summarizes the results for servers assessed as suitable.

Prod			
Server Name	**Environment**	**Suitable for Azure Server Migration**	**Comments**
CLDPRD8IIS61975.itservices.sbc.com	Production	Yes	C++ desktop application launched from intranet web page by internal users. C++ desktop installed presentation layer running as an ActiveX Thick Client over .net framework will be rewritten in Angular 9 and Spring boot 5.3 deployed on Azure App Service plan with Tomcat 9.0 web server stack.
CLDPRD8SQL74546.itservices.sbc.com	Production	Yes	SQL Server Standard Edition 2016 on Windows Server 2016 (Production DB) to be migrated to Azure SQL Server IaaS VM on Windows Server 2019 and hosting SQL Server 2016.

Non-Prod			
Server Name	**Environment**	**Suitable for Azure Server Migration**	**Comments**
CLDCER8SQL40636.itservices.sbc.com	Test	Yes	SQL Server Standard Edition 2016 on Windows Server 2019 (Pre-Production DB) to be migrated to Azure SQL Server IaaS VM on Windows Server 2019 and hosting SQL Server 2016 and also SSIS packages will be migrated to Azure SQL Server IaaS VM.
CLDCER8SQL51508.itservices.sbc.com	Test	Yes	SQL Server Standard Edition 2016 on Windows Server 2019 (Pre-Production DB) to be migrated to Azure SQL Server IaaS VM on Windows Server 2019 and hosting SQL Server 2016 and also SSIS packages will be migrated to Azure SQL Server IaaS VM.
CLDCER8IIS48630.itservices.sbc.com	Test	Yes	C++ desktop application launched from intranet web page by internal users. C++ desktop installed presentation layer running as an ActiveX Thick Client over .net framework will be rewritten in Angular 9 and Spring boot 5.3 deployed on Azure App Service plan with Tomcat 9.0 web server stack.
ACE2D06450SQ00.ITSERVICES.SBC.COM	Install	No	Server is in building phase and not part of application
ACE2D06450SQ004.ITSERVICES.SBC.COM	Install	No	Server is in building phase and not part of application
ACE2D06450SQ005.ITSERVICES.SBC.COM	Install	No	Server is in building phase and not part of application
ACE2D06450SQ006.ITSERVICES.SBC.COM	Install	No	Server is in building phase and not part of application

2.4 Migration Consideration

• IaaS Migration
 o Prod and Pre-prod database servers will be migrated to SQL Server IaaS VM on Windows Server 2019 hosting SQL Server 2016.
 o All application web URLs will be secured using HTTPS (using TLS 1.2).
 o Azure VMs will be configured to use HTTPS by using SSL certificate (certificate will be uploaded to Key Vault).
 o Azure VM will be integrated with VNet so that it can connect with Key Vault using private endpoints deployed in the same VNet.
 o Premium managed disks will be used for production environment which provides SLA of 99.99% for availability

• PaaS Migration
 o The On-premises C++ desktop application installed presentation layer running as an ActiveX Thick Client over .net framework will be rewritten in Angular 9 and Spring boot 5.3 deployed on Azure app service
 (PaaS).
 o Runtime Stack: Java 8, Angular 9 and Spring boot 5.3, Java web server stack: Tomcat 9.0, OS: Linux.
 o Application team will provide Tomcat compatible .war file which will be deployed on Azure WebApp.

• Monitoring, Log Analytics
 o Azure Monitor will be used to monitor the environment and collect metrics for Azure VMs.
 o Log analytics workspace will be created for each environment and will be used by Prod and Non-Prod environments. Azure VM metrics and WildFly logs will be stored in log analytics workspace.
 o Azure Key Vault will be created to store all secrets (encrypted keys, certificates, secrets).

• Security: Azure Key Vault
 o As part of the migration to cloud, we are required to handle secrets through Azure Key Vault. Azure Key Vaults will be setup in East US 2 region to store the following items:
 o Application Setting will be configured to refer to key vault for these settings.
 o SSL certificate.
 o Disk encryption set for VM's OS disk using Customer Managed Key (CMK).
 o Virtual machine secrets.
 o VM will integrate with Azure Key Vault using Private Endpoint connection.
 o System managed identity will be used to provide access from Azure VM to Azure Key Vault.
 o ADO service principle will be used to provide access from ADO Pipeline to Azure Key Vault.
 o All programmatic integration with Azure Key Vault will be done through configuring the application host with a system managed identity (for Azure Key Vault run time integration) or using ADO service principle

(for Azure Key Vault integration during automatic deployment via pipeline execution).

• Security: Azure Key Vault Keys Rotation
o A key-rotation process should be considered for each of the keys stored in the Key Vault (with a maximum period of up to 2 years).
o This is applied to all keys, including CA Certificate. When a certificate is created, an expiration date should be set per key-rotation policy.
o Key rotation to be applied as part of application owner's methods and procedures.

• Security: At-Rest Encryption
o VM OS disk are encrypted at-rest by default and encryption cannot be turned off.
o It will use Customer Managed Key (CMK) stored in Azure Key Vault.

• Security: In-Transit Encryption
o Interfacing Applications: Inbound HTTP communication will be secured using HTTPS protocol (using TLS v1.2). SSL certificate will be provided by venafi and will be stored in Azure Key Vault. SFTP will be used
for file transmission which is also secured using TLS v1.2. Connect: Direct Secure+ will be used to transfer files to and from mainframe systems using TLS v1.2
o Connection to VM in Azure from on-prem via TLSv1.2
o Azure VM will accept the encrypted connections only.

• Identity
o CSO comm host will be used to provide access to Azure Linux Virtual Machine.
o Cookies based Global Logon (CSP-GLO) identity system is being used for authentication to the EAI website.

• URL Change
o Currently Application is using HTTP protocol in code to access the application URL. While a HTTPS connection will be provided on Azure to access the application. This will result in providing a new URL to the
users for accessing the application with a secure connection.

2.5 Optimization Opportunity

The table below describes the optimization opportunity for the application.

Optimization Opportunity	Description	Comments
Improved Security	We are migrating from insecure connect: Direct to Connect: Direct w/Secure+ for application service and service dependencies. ODBC to secured connection.	Security will be optimized by implementing more secure network connections.
Upgrade the software and OS	Operating system version & upgrades to be compliant with AT&T standards.	Databases will be deployed on Azure IaaS VM on Windows Server 2019.
App Server : Source: Desktop Client application with C++	Operating system version & upgrades to be compliant with AT&T standards.	Application component will be deployed on Azure App Service with Tomcat 9.0 runtime. C++ desktop application launched from intranet web page by internal users. C++ desktop installed presentation layer running as an ActiveX Thick Client over .net framework will be rewritten in Angular 9 and Spring boot 5.3 deployed on Azure App Service plan with Tomcat 9.0 web server stack.
Server footprint reduction	The total number of the servers will be reduced from 5 to 3 to decrease the footprint since we won't be needing HA within region.	Cost saving.

2.6 Six Principles

Core Principle	Description	Comments
Secure the Network	NSG Private Endpoint	Each subnet will be secured with a network security group to allow access only as required. Network Security Groups (NSGs) applied on Subnet to control the incoming and outgoing traffic. VMs are exposed to consumption using load balancers by leveraging Private Endpoints, it has been created in bastion to support ingress traffic from on-premises systems.
Protect the Data	Data-at-Rest Encryption Data-in-Transit Encryption	Data-at-rest will be encrypted with customer managed keys. Data-in-transit will be encrypted with TLS v1.2.
Control the Access	Azure Active Directory	At Azure Subscription level, RBAC (Role Based Access Control) is already in place using security groups as per the guidance. Federation with on-premises IT Services domain will ensure restricted access for authorized users
Monitor the Environment	Azure Monitor Log Analytics Mandatory integration with CSO Astra monitoring solution. Full data access log capture for traceability. Netcool integration with Log Analytics.	The Azure Monitor is used to configure workbooks and dashboards for monitoring. Log Analytics is used to monitor the infrastructure matrix on VM. All subscription activity logs and NSG flow logs will be injected into CSO Astra subscription's log storage for further security analysis and remediation. Netcool will create AOTS tickets based on the generated alerts on the VM.
Deploy Infrastructure as Code	Azure DevOps	The CD pipeline is created for infrastructure and custom software installation and application configuration. The Azure DevOps is used for fully automated deployments
Make Allocation Match Demand (Elasticity) PaaS VMSS	Right VM sizing and cost optimization PaaS Solution The Azure App Service is a PaaS solution that is elastic and scalable based on demand.	Optimized VM SKUs are chosen as per the current on-Prem uses to reduce the cost. PaaS Solution for Application tier: The Azure App Service is a PaaS solution that is elastic and scalable based on demand.

2.7 Pattern Consideration

The table below lists the patterns utilized in the design of the application on Azure. The design patterns documents can be accessed by visiting the Patterns Catalog on the Azure DevOps wiki: https://aka.ms/ATTMSPatternsCatalog

Note: For AT&T users who may not have access to the Azure DevOps wiki, a copy of the pattern documents is published on AT&T SharePoint here: https://aka.ms/ATTAzurePatternsCatalog

Design Pattern Name	Version	Comments
Design.Identity.Authentication_Model_Determination	1.1	This pattern document is used to help users identify the authentication protocols used for the authentication of a human authentication to an application that uses HTTP/HTTPS protocol with HALO.
Design.Identity.CSP_IDM	1.1	Used to grant access to the database.
Design.Identity.MyLogins_Remediation	1	This pattern document outlines the remediation steps for MyLogins when an application moves to Azure. MyLogins uses a ticket-based workflow to grant and remove access based on the approval of a business application owner's approval. Additionally, MyLogins provides the ability for direct supervisors to audit/review access on a periodic basis.
Design.Identity.Upstart	1	This pattern document outlines the remediation steps for UPSTART. UPSTART (Access Provisioning & Account Management System) is used to manage access to applications to their resources.
Design.Security.Secrets_Management	1.4	Applications moving to Azure are required to use Azure Key Vault for storage of keys, secrets, and certificates. Used to store secrets in AKV. All private keys for application users, as well as all encryption keys for disks/storage account, will be stored in Azure Key Vault.
Design.Security.Encryption_In_Transit	1.1	Used to implement encryption on database communication and ensure communication with the interfaces.
Design.Backup.Azurebackup	1	Describes how to use Azure Backup for backing Azure Database for SQL Server.
Design.Storage.StorageAccount	1	Outlines guidance on leveraging Azure storage accounts for workloads, includes use cases, recommended and required configuration elements, and explanations of when other technologies would be recommended in favor of a storage account.
Design.Monitoring.Monitoring_Agents	1	Diagnostics Agents is used to store the syslogs in a storage account and monitor the health of Azure VMs and VMSS.
Design.Monitoring.Monitoring_StorageAccounts	1	Storage accounts are required for keeping logs used by the monitoring solution.
Design.Monitoring.Application_Insights	1	This guidance is to enable the application level monitoring solution, Application Insights.
Design.Networking.Private_Link	1	Describes how disconnected Workload VNets will connect to one another, to Azure-hosted PaaS services, and to AT&T services through the use of Azure Private Link Service (PLS) and Network Address Translation (NAT). PLS and PLE are used for inbound and outbound connections.
Design.Networking.Private_DNS	1	Describes how workloads will deploy private DNS zones within their own subscriptions to provide name resolution within VNets, as well as for Azure-hosted PaaS services and AT&T hosted datacenter services.Used to provide FQDN resolution within VNets.

Design.DataMigration.SQLServer_IaaS-VM-SQLServer	2.3	This pattern describes the Migration of an on-premises SQL Server database to a SQL Server database on Azure IaaS VM Win SQL Server.
Azure App Service	1.1	This document outlines the guidance on usage of Azure App Services for any web application migrating to Azure. The guidance is based on Cloud Foundation framework/principles and is an extension of existing App services Pattern.
Design.Compute.AzureVM	1	This pattern document outlines guidance on leveraging Virtual Machines in Azure for a workload. This includes recommended configuration, deployment method, and agents.
SMTP Pattern	0.1.0	Used to send email from Azure to AT&T DLs for providing alerts in-house.

2.8 Jumpstart kit(s) utilized for the application

The table below lists the jumpstart kit(s) utilized for the application.

Jumpstart kit Name	Version	Comments
jumpstart-windows-vm	6.1.0	This jumpstart kit is used to build deployment automation for windows VM to host SQL Server IaaS
appservice	5.1.0	This jumpstart kit is used to build deployment automation for Azure App service.

3.1 Target Azure Architecture

The architecture diagram below depicts the target environment in Azure. All resource names follow the Azure Naming and Tagging Standard <v1.5.1>. (Visio template version: <1.1>.)

Target Architecture Description: Provide the target architecture description here.

3.2 Detailed Design

This section describes Azure resources leveraged in the target architecture.

Category	Topic	Decision	Reasoning	Compliant	Raid Number
DevOps	Deployment CD Pipelines	Azure YAML Pipeline	As per agreed & defined standard		
DevOps	Deployment Tool	Azure Pipeline	As per agreed & defined standard		
DevOps	Infrastructure Automation	Terraform	Terraform scripts will be used for infrastructure and application deployment automation		
Networking	Load Balancer	Standard load balancer and HA Proxy will be used for Application Ingress traffic. Global Load Balancer will be used to route traffic from on-premise clients to <Application Name> is Azure via Global Load Balancer.	As per agreed patterns and defined standard.		
Networking	Virtual Network	Two Virtual Network for each region (one for Linux Workload and one for Windows Workload)	Virtual network to create services like Virtual Machines, NIC etc.		
Networking	Subnet	Each Linux Workload Virtual Network has N Subnets and each Windows Workload has N Subnets	Separation of subnets based on Private Endpoint, Private Link Service, Jump & other Frontend & DB Tiers		
Networking	External Access	Outbound external access will be allowed via the Azure Firewall/ Application Gateway	As per agreed patterns and defined standard and it provides AT&T ability to monitor inbound activity.		
Networking	Azure service Connectivity	Network Security Groups to control traffic	NSGs to allow/deny the inbound and outbound traffic		
Networking	Private Link Service	For application Ingress Traffic	To establish Inbound communication from On-Premises to Azure Workload environment		
Networking	Private Link Endpoint	For application Egress Traffic	To establish outbound communication from Azure to On-Premises along with other PaaS services like Storage Account & Key Vaults		
Networking	Network Security Groups	To control Ingress/Egress Traffic	NSG to allow/deny the inbound & outbound traffic		
Networking	Azure service endpoint Connectivity	RSV & Log Analytics Workspace	Azure Service endpoints will be used with Service Tags available to be used within NSG Rules		
AKS Cluster Management	Kubenet or Azure CNI	Azure CNI	Advanced features and network resources proximity to POD's. The pod per node limitation can be raised to 250. A maximum number of Pods per server is defined though application requirements. 15 nodes pods will be deployed.		
AKS Cluster Management	Ingress Controller	NGNIX ingress controller	NGNIX will be used as LB for application		

AKS Cluster Management	Node Scalability	Auto scaling with autoscaler profile will be enabled.	AKS cluster creation will have --enable-cluster-auto scaler, enabled. A default 10 node cluster will be deployed and Max pod nodes 30 will be deployed.		
AKS Cluster Management	POD Scalability	Horizontal POD Auto scale will be enabled.	AKS uses a horizontal pod auto scaler (HPA) to monitor resource demand and automatically scale the number of replicas.		
AKS Cluster Management	Configuration	YAML and Helm chart	For quota, policies, roles binding etc.		
AKS Cluster Management	Cluster Access Control	Azure AD with service principle and access only from Authorized IP (RBAC enabled)	AAD with a service principle is the only supported mode in current AKS.		
AKS Cluster Management	POD networking	Azure CNI	Azure CNI will be used to use advance network features with AKS		
AKS Cluster Management	POD Secrets / Identities	Self-sign certificate, DigiCert, AAF / CADI & RBAC	AKV will be used to store secrets		
AKS Cluster Management	Cluster Outbound Egress Access	External Access will be via the Azure firewall.	All egress traffic will be regulated by AFW, as directed by Microsoft documentation.		
AKS Cluster Management	POD security policy	Azure AD with the service principle and access only from authorized IP (RBAC enabled)	At Azure Subscription level, RBAC (Role Based Access Control) is already in place using security groups as per the guidance. Federation with on-prem IT Services domain will ensure restricted access to Authorized users. Check Section 4.15 of this document for additional details.		
AKS Cluster Management	Azure service Connectivity	Service Endpoint	it is hostname/mS/version/ and then context path		
Observability	Infrastructure Monitoring	Azure Monitor	Azure Virtual machines will be monitored using Azure Monitor		
Observability	Application Monitoring	Application Insights	Application Insight will be used for application monitoring.		
Observability	DB Tier Monitoring	Oracle Enterprise Manager	Oracle Enterprise Manager is being used as an On-Prem Solution. Post migration, changes will be done in OEM to support DB monitoring within Azure.		
Observability	Audit Logs	Consumed by ASTRA	Storing all logs in the storage account provided by ASTRA		
Observability	Boot Diagnostics Logs	Storage Account for Diagnostic Logs	VM Boot logs will be captured in a Storage Account dedicated for Diagnostics Logs		
Observability	Log Analytics	Common Log Analytics Workspace for both Subscriptions	All Virtual Machines logs to be captured in Log Analytics Workspace		
Security	Key Vault	To store sensitive data	Storage for Secrets, Certificates & Keys		

Security	Storage Secure Transfer	Secure communication for storage account	Communication for Storage Account will be done via HTTPS APIs for secure communication		
Security	BYOK	Customer Managed key for Storage Side Encryption (AES256, AES192, AES128)	CMK Keys to be used for Azure Disks using Storage Side Encryption		
Security	Communications Host	Application Admin Access Pod-Pod communication over the TLS 1.2	CSO Communication Host to be used as strategic solution which uses existing MUAM to connect servers. Public Cloud Team's Jump Server accessing the Cloud Jump servers are leveraged interim solution until CSO communication host is available.		
Database	Storage Account	For uploading/downloading	To store Oracle DBs flat file backups		
Storage	Storage Account	Azure Files/File Share Azure Blobs	Azure files will be used to store application metadata files, which will be uploaded to Database via CRON jobs. Azure File Share will be used to store data application specific data. Azure Blobs will be used to store Terraform State files.		
Azure Firewall	Cluster of Outbound Egress Access	External Access will be via the Azure firewall.	AKS cluster allow External Access via the Azure firewall.		
Azure App Service Container (Linux)	Azure App Service	App Service in Azure PaaS hosting	We are migrating Source CDP hosted containers to App Service in Azure PaaS; Migrating the web app to App service will reduce the application teams' dependency on AT&T server help desk for Management and patching and can concentrate on app development.		
Azure App Service (code)	Azure App Service	App services(code)	Onprem application is hosted on the window servers and will be migrated to Azure App Service (code).Migrating the web app to App service will reduce the application teams' dependency on AT&T server help desk for Management and patching and can concentrate on app development.		

3.3 Unencrypted Interface Solution

This section describes encryption solutions used for the unencrypted interfaces that the application communicates with.

Source Application	Source Server Name – Location	Interface Type	Protocol	Target Application/Server Name	Encryption Solution	Remarks

3.4 Application Security Groups

The following Application Security Groups will be created for Production and Non-Production environments.

Prod			
Environment	**Application Security Groups (ASG)**	**Members**	**Description**

Non-Prod			
Environment	**Application Security Groups (ASG)**	**Members**	**Description**

3.5 Private Link Services and Private Endpoints

The following Private Link Services and Private Endpoints will be created for Production and Non-Production environments.

Prod				
Environment	**Name**	**Type**	**Location**	**Description**

Non-Prod				
Environment	**Name**	**Type**	**Location**	**Description**

3.6 Firewall or NSG rule details Inbound/Outbound Connections

The table below describes the Inbound/Outbound connection details to Azure network source and destination Ips, along with ports that need to have firewalls opened for communication.

Prod									
NSG Name	Environment	Source IP/Subnet	Target IP /Subnet	Inbound/Outbound	Protocol	Port	Action	Priority	Comments

Non-Prod									
NSG Name	Environment	Source IP/Subnet	Target IP /Subnet	Inbound/Outbound	Protocol	Port	Action	Priority	Comments

3.7 Azure Bastion F5 NVA Rules

The table below lists the NVA rules established for connectivity from Azure to Conexus for binary protocol traffic.

PLS IP	NVA Rule	Target IP	Port

3.8 Azure IaaS Virtual Machines, VMSS, PaaS and SaaS Specifications

The table below lists the Azure virtual machine, VMSS, PaaS, and SaaS specifications.

NOTE: Choosing “Other” for the Operating System field or the RHEL Allowed Products field requires a documented RAID with approval.

Prod											
Target Server Name (*.vci.att.com)	**Environment**	**Resource Type**	**Operating System**	**RHEL Allowed Products**	**Azure Resource Group**	**Target Azure Region**	**CPU Cores**	**Memory (GB)**	**Storage (GB)**	**Azure SKU**	**RAID**

Non-Prod											
Target Server Name (*.vci.att.com)	**Environment**	**Resource Type**	**Operating System**	**RHEL Allowed Products**	**Azure Resource Group**	**Target Azure Region**	**CPU Cores**	**Memory (GB)**	**Storage (GB)**	**Azure SKU**	**RAID**

3.9 Jump Server Specifications (if required)

Prod								
Target Server Name (*.vci.att.com)	Environment	Operating System	Azure Resource Group	Target Azure Region	CPU Cores	Memory (GB)	SKU Deviation RAID	Jump Server RAID

Non-Prod								
Target Server Name (*.vci.att.com)	Environment	Operating System	Azure Resource Group	Target Azure Region	CPU Cores	Memory (GB)	SKU Deviation RAID	Jump Server RAID

3.10 Azure Scaling In/Out Configuration Specifications

The table below lists the Azure scaling related settings.

Prod								
Target Server Name (*.vci.att.com)	Environment	Azure Resource Group	Target Azure Region	Min Instance	Max Instance	Scale Out Settings	Scale In Settings	Additional Details

Non-Prod								
Target Server Name (*.vci.att.com)	Environment	Azure Resource Group	Target Azure Region	Min Instance	Max Instance	Scale Out Settings	Scale In Settings	Additional Details

3.11 Detailed Reasoning if Scaling is Not in Place

Detailed Reasoning	
Plan and Timeline for Enabling Scaling in the Future	
RAID Number	

3.12 Optimization Achieved Over On Premise Deployment

The tables below detail the optimization achieved for Production/DR sites and Non-Production.

Prod										
Environment	Servers On-Prem Configuration (Source)	CPU On-Prem Configuration (Source)	RAM On-Prem Configuration (Source)	Servers Azure Configuration (Target)	CPU Azure Configuration (Target)	RAM Azure Configuration (Target)	CPU Footprint Reduction	RAM Footprint Reduction	CPU % Reduction	RAM % Reduction

Non-Prod										
Environment	Servers On-Prem Configuration (Source)	CPU On-Prem Configuration (Source)	RAM On-Prem Configuration (Source)	Servers Azure Configuration (Target)	CPU Azure Configuration (Target)	RAM Azure Configuration (Target)	CPU Footprint Reduction	RAM Footprint Reduction	CPU % Reduction	RAM % Reduction

3.13 Azure Resource Deallocation Schedule

In the table below, please provide deallocation schedule details for the unused azure resources.

Prod									
Environment	**Resource Name**	**Resource ID**	**Scheduled Start Date**	**Scheduled End Date**	**Time Zone**	**Deallocate Time**	**Startup Time**	**Recurrence**	**Days for Weekly Schedule**

Non-Prod									
Environment	**Resource Name**	**Resource ID**	**Scheduled Start Date**	**Scheduled End Date**	**Time Zone**	**Deallocate Time**	**Startup Time**	**Recurrence**	**Days for Weekly Schedule**

3.14 Azure Storage Specifications

The table below describes the storage information for the virtual machines.

Prod							
Target Server Name (*.vci.att.com)	Environment	Number of Disks	Disk Type (SKU)	Disk Size (GiB)	IOPS Per Disk (MBps)	Throughput Per Disk (MB/Sec)	Diagnostic Logs Storage Account

Non-Prod							
Target Server Name (*.vci.att.com)	Environment	Number of Disks	Disk Type (SKU)	Disk Size (GiB)	IOPS Per Disk (MBps)	Throughput Per Disk (MB/Sec)	Diagnostic Logs Storage Account

3.15 Azure Network Specifications

The table below describes the Azure network information for the virtual machines.

Note: Please specify a note here, if any. Example: The nomenclature and other information of the servers will get changed as the environment is provisioned.

Prod							
Target Server Name (*.vci.att.com)	**Environment**	**Azure VNet**	**Subnet**	**No. of NICs**	**IP Address**	**Network Load Balanced?**	**Comments**

Non-Prod							
Target Server Name (*.vci.att.com)	**Environment**	**Azure VNet**	**Subnet**	**No. of NICs**	**IP Address**	**Network Load Balanced?**	**Comments**

3.16 Source to Target Mapping

This table maps the Source server details with Target server details like Target Azure Resource Name, Resource Group, Environment, Role, etc.

Prod					
Subscription Name	**Source Server Name**	**Target Resource Name**	**Azure Resource Group**	**Environment**	**Role**

Non-Prod					
Subscription Name	**Source Server Name**	**Target Resource Name**	**Azure Resource Group**	**Environment**	**Role**
	CLDDEV0SRV07346				
	MISOUT7ARMSXD01				
	MISOUT7ARMSXW01				
	WIWAUK4ARMSXD03				
	WIWAUK4ARMSXD04				

3.17 Azure Tags

The table below describes the tag information applied on the Azure resources.

Prod		
Target Server Name	**Environment**	**Azure Tags**

Non-Prod		
Target Server Name	**Environment**	**Azure Tags**

3.18 Cost Projection

This section provides details on the monthly cost estimation for enabling the solution as-is on Azure and with same comparison of recognized optimization opportunities to this solution. It includes the services, IaaS, or related resources migrated to Azure and does not include 3rd party and other supporting solutions.

Assumptions:

•Costs are calculated using AT&T rate cards.

•Costs are calculated for Compute and Storage only. Network usage, Management, etc. are not included in this estimate.

•Estimates may change if recommended SKU is changed for any reason in Target Environment.

•To optimize the costs of managing the Non-Production environment, the Application team can decide to shut down the Non-Prod virtual machines (VMs) when the environment is not being used for development, testing, or training activities. The Non-Prod resources can be restarted as needed. Be aware that storage costs for the Non-Prod environment will NOT be paused and will continue to be incurred, even when the VMs have been shut down.

Prod Subscription Cost				
Mots ID	**SKU: Compute**		**Storage (GB & Type)**	
6450	**Monthly Cost:**	0.0	**Monthly Cost:**	0.0
	1 Year:	0.0	**1 Year:**	0.0
	Grand Total (Annual Charges, AT&T rate card):			0.0

3.19 Deployment Strategy

The deployment strategy for the Accounts Receivable Management System application is as follows.

Note: Terraform template will be provided to provision Azure Workloads, and manual steps will be followed for Private Link Service and Private Endpoint approvals/creations.
The Terraform template will also deploy the database servers using the golden images provided by the AT&T team, and the images are baked using Oracle Database installation.

Deployment Pattern	Deployment Tool	Artifact Location

3.20 Role Based Access Control

Provide Role-Based Access Control details for Production and Non-Production environments.

Prod			
Environment	**Security Group Name**	**Access Level /Inheritance**	**Members**

Non-Prod			
Environment	**Security Group Name**	**Access Level /Inheritance**	**Members**

3.21 DNS Updates

The table below describes the DNS updates required for the Accounts Receivable Management System environment.

Note: DNS records may vary depending on the use of load balancers.

Prod			
Environment	**DNS Suffix/A-Record**	**Type**	**IP Address**

Non-Prod			
Environment	**DNS Suffix/A-Record**	**Type**	**IP Address**

3.22 Backup

The table below describes the backup information.

Server Name (*.vci.att.com)	Current Backup Solution	Backup on Azure

3.23 Disaster Recovery

The following approach has been taken for disaster recovery and the high availability of the application:

•Within a single Azure region deploying <insert application component details>

•Deployment in multiple Azure regions: <insert name of Azure regions>

In the event an Azure region is completely unavailable, the application can be accessed from another region.

Server Name	Current BCDR Protection	Planned BCDR Protection

3.24 SSL Offloading

The table below describes the SSL offloading information.

Server Name	Current Setup	Planned Setup

3.25 Jobs – Database / Batch / Cron

The table below describes the scheduled job information.

Prod		
Environment	**Server Name**	**Jobs**

Non-Prod		
Environment	**Server Name**	**Jobs**

3.26 Database Assessments

The table below describes the database assessment for the application.

Prod		
Application	**Environment**	**Comments**

Non-Prod		
Application	**Environment**	**Comments**

3.27 Database Migration Solution Strategy

3.28 Monitoring Requirements

The table below describes the monitoring requirements for Accounts Receivable Management System.

Server Name	Current Monitoring Solution	Planned Monitoring Solution

3.29 Decommission of Infrastructure: Application completed Server Decomm Artifact Link

3.30 Azure Resource Decommission Schedule

In the table below, please provide decommission schedule details for the azure POC resources.

Prod			
Environment	Resource Name	Decommission Date	Decommission Time

Non-Prod			
Environment	Resource Name	Decommission Date	Decommission Time

3.31 Cutover Process

Selected Cutover Scenario	

3.32 Selected Cutover Scenario

4.1 Playbook

The Playbook will provide detailed implementation tasks being performed in both non-production and production environments by assigned application team and Microsoft team members. As part of the Playbook Task Step Review, the Public Cloud Solution Architecture and Migration Team and CSO will complete validations of Network Security Groups (NSGs) to confirm alignment with the ASPR requirements; regarding Role Based Access Controls (RBACs). The Playbook Task Step Review will also include confirmation of Astra Onboarding (https://wiki.web.att.com/pages/viewpage.action?spaceKey=astra&title=Azure+Account+Prep+for+Astra+Onboarding) as required by AT&T Cloud Governance. As detailed in the AT&T Public Cloud Standards Practice R190710 (http://tss.att.com/tssr/ppsDocument.cfm?ppsid=490), application teams must implement user access levels for CSP console access that defines privileged access and documents: How access is separated for audit purposes according to ASPR-0088: Least Privilege, ASPR-0099: Developer Access to Production Systems and Data (https://attegrc.cso.att.com/ATTeGRC/apps/ArcherApp/Home.aspx).

Note: The links referred above are accessible only through the AT&T network.

Playbook for detailed steps that are being performed in the non-production environment.

For the Playbook, please refer to the link below:

4.2 Cut Over (Link to Playbook)

4.3 Roll Back Plan

In the event of a major issue encountered during migration or an issue with any services on which the migration is dependent, Microsoft will shut down the VMs on Azure and on-premises virtual machines will be powered on.

In general, the rollback plan would be to turn off the target virtual machines and start using the source servers. There are no changes done on the source servers and all the applications and their configurations will be preserved. In case of a rollback, it is agreed that the AT&T infrastructure team will revoke the DNS changes performed after the servers are migrated to Azure.

Rollback Steps	Task Owner
GO/NO-GO decision for roll back	AT&T - App Owner
Stop and disable app on target Azure servers	AT&T - Migration
Stop and disable DB services on target Azure servers	AT&T - Migration
Roll back DNS records as per Microsoft's rollback request	AT&T - Infrastructure Team
Shut down the target VM/services on Azure	AT&T - Migration
Start DB services on on-premises source server	AT&T - DBA
Start required application services on on-premises source server	AT&T - App Owner
Verify application and database connectivity	AT&T - App Owner
Perform the source server validation and smoke test	AT&T - App Owner

4.4 Tentative Migration Schedule (ADO Links to Schedule)

4.5 Post-Migration Support and Stabilization

For all applications that are migrated to Azure, for any migration-related issues escalated beyond AT&T's first level of support, Microsoft will provide:

Azure-related support for ten (10) days from the team that performed migration activities, beginning once production go-live has started for the application.

After the 10-day go-live support period, Microsoft will provide extended support for additional thirty-five (35) days using a remote overlay team of fixed capacity of four (4) resources, with the ability to engage the migration team within four (4) hours for severity "1" business impacting issue. This 35-day support window begins once production go live has completed, meaning that 100% of the application's traffic and processing has been cutover to Azure (Canary go live is complete).

After forty-five (45) days, AT&T shall follow the regular Microsoft premier support and account management channels.

The following table lists the support roles for the migration process and the primary contacts for each role.

Support Role	Description	Responsibility
Cloud Hosting Team	Responsible for coordinating support activities for technical issues that occur with the underlying infrastructure, such as Azure Compute, Storage, Azure Networking etc.	AT&T Inc. / Microsoft
Application Support Lead	Responsible for coordinating support activities for technical issues that occur with Applications/applications that experience issues because of migration activities.	AT&T Inc. / Microsoft
Migration Lead	Responsible for coordinating support activities for technical issues that occur in the post migration process.	AT&T Inc. / Microsoft

5.1 Deployment Templates: Terraform templates repository link and execution steps

5.2 Database Migration Steps: Link to the Playbook for database migration steps

5.3 Reviewers

Name	Version Reviewed	Role	Date

5.4 Approvers

Name	Email ID (AT&T)	Version Approved	Role	Date
Akiva Marks	akiva.marks@intl.att.com		Pre-Approval SDS Design/Architecture lead	
Akiva Marks	akiva.marks@intl.att.com		SDS Design/Architecture lead	
			Modernization Development Coordinator(SDS/GSI/Vendor)	
Eric Johnson	ej2401@att.com		AT&T Decommission Lead	
JAIN, VAIBHAV	vj191n@att.com		AT&T Application Owner	