MANAGED CLOUD SERVICE FOR AZURE - SERVICE GUIDE

Last Modification Date: 02/13/2025
Exported and Shared on: 02/14/2025

For additional information, visit www.intervision.com

CONTENTS

1 Managed Cloud Service for Azure - Service Guide 1
1.1 Overview 1
1.2 Assumptions 1
1.3 Minimum Security Requirements 1
1.4 Recommended Security Features 2
1.5 Managed Cloud Services (MCS) for Azure: Leveraging InterVision as Your Cloud Solution Provider (CSP) Best Practices 2
1.6 Service Delivery Policy: Escalation to Microsoft Support 2
2 Managed Cloud Services for Azure Details 3
2.1 Cloud Platform Management and Support 3
2.2 Virtual Machine and Operating System Support 4
2.3 Azure Virtual Desktop Support 5
2.4 Operational Processes 5
2.5 Managed Cloud Foundation Services 6
2.6 Environment Monitoring 7
2.7 Azure Virtual Desktop Monitoring 8
2.8 Managed Cloud Service for Azure Containers 8
2.9 Managed DevOps Automation Service 12
2.10 Onboarding 16
2.11 Recurring account review 17
2.12 Subscription renewal 17

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

3 Managed Cloud Service for Azure - Service Guide Change Log 17

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

1 MANAGED CLOUD SERVICE FOR AZURE - SERVICE GUIDE

1.1 OVERVIEW

The InterVision Managed Cloud Service (MCS) for Azure is a managed service for operations of your Microsoft Azure environments. InterVision provides the tools, processes and personnel for the ongoing operations management of your Azure servers, such as patch, backup, continuity management, cost management, security management and IT processes such as incident, change and service requests. Customers have access to our certified Azure engineers 24/7.

As part of the service, InterVision provides the following:

- 24/7 support team
- Customer portal and ticket system
- Set up and configuration of monitoring, logging and alerts
- Response time SLAs and resolution time objectives as specified in the managed service work order
- Customized escalation procedures for service events
- Support and management of your Azure environment as specified in the service description below
- Incident response for support services as specified in the service descriptions below
- Service reporting including key service performance indicators that includes operational metrics, SLA adherence, financial metrics around Azure spend

This service can be combined with additional InterVision services including Migration, Cost Optimization, Network, Security and Service Management services. See associated service guide and service description for details regarding these additional services. This Service Guide covers the Managed Cloud Service for Azure and each of the service modules.

1.2 ASSUMPTIONS

The managed service is designed for Day 2 operations of existing Azure environments. The initial build of the environment is completed. Minor changes to existing environments is included as part of the service as outlined below. Significant architectural changes or migration activities would require an additional Statement of Work.

1.3 MINIMUM SECURITY REQUIREMENTS

For the successful operations of the Managed Cloud Services for Azure the following minimum-security requirements must be enabled. If these are not currently enabled, these can be enabled during onboarding.

- **Customer Bastion Hosts –** Bastion hosts will need to be deployed for access to compute resources. Bastion hosts are special-purpose servers that are hardened and host minimal applications with all other services removed to reduce the threat. They are typically located outside the firewall or inside a DMZ to provide access to untrusted networks.
- **Active Directory** – For Windows Environments, customers will need to provide Active Directory or equivalent solution to manage users and groups. This can either be dedicated Active Directory servers or Azure AD. This is not required if the environment only consists of Linux servers.
- **Anti-Virus Software** – For Windows server environments, customer will need to deploy Anti-virus/Anti-malware software solution. InterVision recommends TrendMicro Cloud One but the specific software vendor can be substituted for any enterprise grade endpoint protection solution. This is not required if the environment only consists of Linux servers.

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

1.4 RECOMMENDED SECURITY FEATURES

In addition to the above security requirements, we also recommend the following security features:

- **Onboarding Security Checks -** During the Onboarding Phase, InterVision will review Microsoft Defender for security recommendations. We will work with the Customer to remediate these during the onboarding process.
- **Ongoing Security Posture Management –** Customers may elect to adopt InterVision's Security Posture Management Service which will provide ongoing monitoring of best practices and compliance framework adherence.

1.5 MANAGED CLOUD SERVICES (MCS) FOR AZURE: LEVERAGING INTERVISION AS YOUR CLOUD SOLUTION PROVIDER (CSP) BEST PRACTICES

For your Managed Cloud Services (MCS) on Azure, InterVision acts as your Cloud Solution Provider (CSP) whenever possible. This strategic approach provides several key benefits designed to optimize your cloud experience and ensure seamless access to support:

- **Streamlined Support:** By working directly with InterVision as your CSP, you gain a single point of contact for all your Azure-related needs, including support. This simplifies the support process, eliminating the need to navigate multiple vendors and ensuring faster response times. We have established relationships and escalation paths with Microsoft, allowing us to efficiently resolve any issues that may arise.
- **Proactive Management:** InterVision's proactive approach to managed services includes continuous monitoring, performance tuning, and security patching. As your CSP, we have direct access to the tools and resources necessary to identify and address potential issues before they impact your operations.
- **Direct Access to Microsoft Resources:** Being a CSP allows InterVision access to enhanced support resources from Microsoft, including direct escalation paths and specialized technical expertise. This ensures that even the most complex issues are addressed quickly and effectively.

By leveraging InterVision as your CSP for Azure MCS, you gain a comprehensive, integrated solution that simplifies cloud management, enhances support access, and optimizes your overall cloud experience. We are committed to providing you with the highest level of service and ensuring your Azure environment performs at its best.

1.6 SERVICE DELIVERY POLICY: ESCALATION TO MICROSOFT SUPPORT

To ensure the optimal performance and stability of your managed cloud environment, and to effectively fulfill your service requests, InterVision MCS Team may, at times, need to escalate support tickets directly to Microsoft Support. This is a standard industry practice for resolving complex technical issues and ensuring timely resolution.

Depending on the nature of the issue and the required level of support, it may be necessary to increase the support level associated with your Microsoft account. This will only be done if your current support model does not adequately cover the specific requirements of the issue or your service request. The InterVision MCS Team will communicate with you prior to any changes to your support level being implemented and discuss any associated costs. This direct engagement with Microsoft Support, and potential adjustments to your support level, are essential for delivering high-quality service and maintaining your cloud environment.

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

2 MANAGED CLOUD SERVICES FOR AZURE DETAILS

Service Description and Details - Managed Cloud Service for Azure

InterVision will provide the following Managed Azure server environment Services and Deliverable(s) as a part of our engagement, including but not limited to:

2.1 CLOUD PLATFORM MANAGEMENT AND SUPPORT

InterVision will provide management and support activities related to the Azure cloud platform, including support for tenants, subscriptions, virtual networks, subnets, route tables, Azure load balancers, Azure firewall, network security groups, access control lists, Azure Traffic Manager and VPNs/VPN Gateway. Management and Support of the following services is included:

Cloud Platform Management and Support	InterVision	Customer
Tenant Creation, Onboarding, Management	R/A	C/I
Subscription Management	R/A	C/I
Azure Virtual Network Management	R/A	C/I
Subnet Management	R/A	C/I
Route Table Management	R/A	C/I
Azure Load Balancing Management	R/A	C/I
Azure Firewall Management	R/A	C/I
Azure Network Security Groups Management	R/A	C/I
Azure Network Access Control Lists Management	R/A	C/I
Azure Traffic Manager Management (DNS level traffic routing, load balancing, failover)	R/A	C/I
VPN/Private Connection/VPN Gateway Management	R/A	C/I
Access Control (IAM) - Create Users and Groups	R*	R*

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Access Control (IAM) - Add/Remove Users/Groups from Resource Groups	R*	R*
Access Control (IAM) - Assign Roles to Users/Groups	R*	R*
Synchronize on-prem deployment of AD with Azure AD using Azure AD Connect	C/I	R/A
Modify AD Group Membership	C/I	R/A

*Both InterVision and Customer may modify Access Control (IAM) users and groups. Customer may request changes or perform those changes directly via the Azure console.

2.2 VIRTUAL MACHINE AND OPERATING SYSTEM SUPPORT

InterVision will provide management and support activities related to virtual machines and operating systems. Management and Support of the following services is included:

Virtual Machine and Operating System Support	InterVision	Customer
Virtual Machine Creation	R*	R*
Compute Instance Resizing/Family Changes	R/A	C/I
Reserved Instance Creation	R/A	C/I
Windows VM Monitoring	R/A	C/I
Windows VM Management	R/A	C/I
Windows OS Patching	R/A	C/I
Configure Anti-Malware Protection	R/A	C/I
Azure Backup Management	R/A	C/I
Removal of Malware on Managed Instances, meaning isolating the server, deleting it and restoring it from backup or image	R/A	C/I
Database administration	C/I	R/A

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

*Both InterVision and Customer may create/deploy new virtual machines. Customer may request that InterVision create virtual machines via service request or Customer may create virtual machines directly via Azure console.

2.3 AZURE VIRTUAL DESKTOP SUPPORT

Azure Virtual Desktop Support	InterVision	Customer
Monitor/Receive Alerts	R/A	C/I
Monitor/Manage Storage	R/A	C/I
Disk Space Cleanup	R/A	C/I
Add/Remove Session Hosts from Host Pool	R/A	C/I
Clear out Hung Sessions	R/A	C/I
Backup Images and Session Hosts	R/A	C/I
Backup FSLogix User Profiles (hosted in Azure)	R/A	C/I
Backup FSLogix User Profiles (hosted On-Prem)	C/I	R/A
Image Management	C/I*	R/A*
Profile Management (using FSLogix)	C/I*	R/A*
Group Policy Administration	C/I*	R/A*
Update/Deploy New Desktop Applications	C/I*	R/A*
Create New Host Pools	C/I*	R/A*
End User Support	#	R/A

* These activities could be provided through InterVision Professional Services

End User Support is the customer responsibility unless managed Help Desk Service is also purchased.

2.4 OPERATIONAL PROCESSES

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Support includes 24x7 monitoring, event and incident management, service, problem and change management, and also includes installation, move, add, change and delete requests.

The assumption here is that the customer's Azure environment is already built, and support activities exclude migration activities.

Operational Processes	InterVision	Customer
Incident, Service, Problem and Change Management	R/A	C/I
Installation, Move, Add, Change and Delete Requests	R/A	C/I

2.5 MANAGED CLOUD FOUNDATION SERVICES

As part of the managed service, InterVision will provide a designated team of a Cloud Service Delivery Manager and Cloud Engineer which complements our 24/7 service desk of level 2 and level 3 cloud engineers.

For each managed cloud environment, InterVision offers Managed Cloud Foundational Services that compliments and is tailored to the specific managed cloud service you are consuming. This service includes the following:

- Designated team of a Client Service Delivery Manager and Cloud Engineer which complements our 24/7 service desk of Level 2 and Level 3 cloud engineers
- Provides architectural and operational guidance
- Provides escalation management
- Coordinate FinOps and cost management reviews
- Liaison with InterVision technical teams and customer on high-risk changes/projects
- Creation and maintenance of customer runbooks
- SLA reporting
- Facilitates game days sessions that include:
-
    - Launching a virtual machine
    - Connecting to Windows virtual machine
    - Connecting through Bastion Host
    - Defining Security Groups and Access settings
    - Connecting to Linux Instance
    - Monitoring walkthrough
    - Patching & backup walkthroughs
- Facilitate business, service & technical reviews

Managed Cloud Foundation Services	InterVision	Customer

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Provide architectural and operational guidance	R/A	C/I
Escalation management	R/A	C/I
Coordinate FinOps and cost management reviews	R/A	C/I
Liaison with InterVision technical teams and customer on high-risk changes/projects	R/A	C/I
Creation and maintenance of customer runbooks	R/A	C/I
SLA Reporting	R/A	C/I
Facilitate business, service & technical reviews	R/A	C/I

2.6 ENVIRONMENT MONITORING

InterVision will provide 24x7 monitoring of the following services related to the Customer Azure environment:

Environment Monitoring	InterVision	Customer
OS Level Monitoring	R	C
Virtual Machine Instance CPU/Memory/Disk Monitoring	R	C
Load Balancer Monitoring	R	C
Cache Service Monitoring	R	C
Serverless Code Execution Monitoring	R	C
DNS Monitoring	R	C
Content Delivery Network Monitoring	R	C
Notification System Monitoring	R	C

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Queueing System Monitoring	R	C
URL Monitoring (up/down)	R	C
Alert Escalation	R	C
Website Monitoring: Availability	R	C
Database Monitoring (Performance/ system health / DB health / sizing / replication)	R	C
Data Warehouse Monitoring	R	C

2.7 AZURE VIRTUAL DESKTOP MONITORING

Azure Virtual Desktop Monitoring	InterVision	Customer
Connection Diagnostics	R/A	C/I
Connection Performance	R/A	C/I
Host Diagnostics	R/A	C/I
Host Performance	R/A	C/I
User Report	R/A	C/I
Utilization Report	R/A	C/I
Client Report	R/A	C/I

2.8 MANAGED CLOUD SERVICE FOR AZURE CONTAINERS

Service Description and Details - Managed Cloud Service for Azure Containers

InterVision will provide 24/7 monitoring, incident response, support and management for Azure containers environments as a part of our engagement.

Supported for the following Azure Services:

- Azure Kubernetes Service

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Managed Service include:

- Provide 24/7 monitoring and management of the Azure infrastructure.
- Monitoring and responding to incidences for Kubernetes Cluster using Azure Monitor
    - Monitor POD health metrics after deployments and detailed metrics/monitoring
    - Monitor application/API endpoints and publicly exposed services
- Provide Incident response / troubleshooting of notified issues
- Provide AKS cluster upgrade and maintenance that includes:
    - Kubernetes version upgrades
    - Upgrades to AKS supporting services: CoreDNS, Azure CNI networking, KubeProxy, Metrics Server, Ingress Controllers
- Perform Kubernetes security benchmarks using Kube-bench that includes:
    - Check the worker nodes configurations for risks in these environments
    - Scan Image / Programming Language for Vulnerabilities and provide support
- Provide Kubernetes applications package management tool Helm
- Provide Kubernetes deployment troubleshooting assistance

Roles and Responsibilities - Managed Cloud Service for Azure Containers

The Service manages customer's Azure infrastructure. The table below provides an overview of the responsibilities of customer and InterVision for activities in the lifecycle of an application running within the Managed Environment.

- "R" stands for responsible party that does the work to achieve the task.
- "C" stands for consulted; a party whose opinions are sought, typically as subject matter experts; and with whom there is bilateral communication.
- "I" stands for informed; a party which is informed on progress, often only on completion of the task or deliverable.

* Items marked with "*" are items that InterVision Professional Services can augment client responsibility and may be specified in the Professional services Statement of work.

ONBOARDING	**Customer**	**InterVision**
Perform manual review of existing environment, remediating any issues as necessary	C, I	R
Perform manual review of CI/CD pipelines	C, I	R
Perform manual review of logging, alerting and monitoring integrations	C, I	R
Perform manual review of deployment manifests	C, I	R
Perform manual review of SCM Repositories	C, I	R
INCIDENT AND EVENT MANAGEMENT	**Customer**	**InterVision**
Monitor and respond to incidences for Kubernetes Cluster using Azure Monitor	C, I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Monitor POD health metrics after deployments	C, I	R
Monitor application/API endpoints and publicly exposed services	C, I	R
Provide incident response/troubleshooting of notified issues	C, I	R
Approve remediation recommendations for the infrastructure	R	I
Implemented remediated recommendations post approval	C,I	R
APPLICATION PACKAGE MANAGEMENT	**Customer**	**InterVision**
Provide Kubernetes applications package management tool Helm	C, I	R
Assist in containerizing the application and tweaking container images	C, I	R
Perform Containerization of the Application	R,C	I
Set up Container Image Repositories	C, I	R
Set up Continuous Integration tools	C, I	R
Set up additional integrations (Code Quality, Vulnerability management, Container Image Scanning)	C, I	R
Set up monitoring and alerting for Continuous Deployment Pipelines	C, I	R
DEPLOYMENT ASSISTANCE	**Customer**	**InterVision**
Provide Kubernetes deployment troubleshooting assistance	C, I	R
Setup IaC Scripts for Infrastructure provisioning	C, I	R
Setup Cloud Network Infrastructure / IAM Resources	C, I	R
Setup AKS Cluster	C, I	R
Initial Security benchmarking for AKS Cluster	C, I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Create Application deployment manifests (Kubernetes yaml/helm/kustomize)	C, I	R
Set up Continuous Deployment or GitOps Pipelines	C, I	R
Set up monitoring and alerting for Continuous Deployment Pipelines	C, I	R
Setup Infrastructure monitoring for AKS Cluster	C, I	R
Setup Backups for AKS Configurations (Velero)	C, I	R
Setup Log Aggregation for AKS Cluster (Datadog, Azure Monitor)	C, I	R
Setup monitoring for AKS cluster (Datadog, Azure Monitor)	C, I	R
Setup Kubernetes access for Development Team members	C, I	R
Guidance on Resource Optimization and cost optimization (Containers, Worker Nodes)	C, I	R
CHANGE MANAGEMENT	**Customer**	**InterVision**
Perform AKS cluster upgrade and maintenance activities	C, I	R
Perform AKS WorkerNode Upgrade	C, I	R
Perform Kubernetes version upgrade	C, I	R
Perform upgrade for Kubernetes Add-Ons/Plugins	C,I	R
Perform upgrade/tweakings for CI/CD Tools	C,I	R
Perform revisions and upgrades for supporting services tools (Ingress controller, Metrics Server, Cluster AutoScaler)	C, I	R
SECURITY MANAGEMENT	**Customer**	**InterVision**
Perform Security Benchmarking for Azure Infrastructure	C, I	R
Perform Security Benchmarking for AKS Cluster	C, I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Check worker node configurations for risks	C, I	R
Review Image Scanning / Code Scanning reports for vulnerabilities	C, I	R
REPORTING	**Customer**	**InterVision**
Configure and retrieve audit history on demand (Azure Monitor)	I	R
Provide access to incident history	I	R
Provide access to change history	I	R

Onboarding and Provisioning - Managed Cloud Service for Azure Containers

In addition to general onboarding tasks, an assigned onboarding project manager will provide a list of customer dependencies and InterVision set up tasks during a kickoff meeting.

2.9 MANAGED DEVOPS AUTOMATION SERVICE

Service Description and Details - Managed DevOps Automation Service

InterVision will：

- Supported CI/CD tools/services: Azure DevOps, Jenkins, Bitbucket Pipeline, GitHub Actions, Gitlab, CircleCI and other tools as approved by InterVision
- Supported Infrastructure as Code (IaC) tools: Terraform, Azure Resource Manager (ARM)
- Supported configuration management tools: Ansible, Puppet, Chef
- Build and configure CI/CD deployment pipelines for the infrastructure
- Implement pipelines using Infrastructure as Code (IaC)
- Provide management of the pipeline
- Monitoring and responding to incidents from CI/CD tools
- Provide incident response / troubleshooting of notified issues
- Provide deployment-based troubleshooting assistance

Roles and Responsibilities - Managed Cloud Service for Azure DevOps Automation Service

The Service manages customer's Azure infrastructure. The table below provides an overview of the responsibilities of customer and InterVision for activities in the lifecycle of an application running within the Managed Environment.

- "R" stands for responsible party that does the work to achieve the task.
- "C" stands for consulted; a party whose opinions are sought, typically as subject matter experts; and with whom there is bilateral communication.
- "I" stands for informed; a party which is informed on progress, often only on completion of the task or deliverable.

* Items marked with "*" are items that InterVision Professional Services can augment client responsibility and may be specified in the Professional services Statement of work.

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

GENERAL	**Customer**	**InterVision**
Resource Stack Recommendation and Selection	R	C
Build and Configure Infrastructure	C, I	R
Develop and Maintain Pipeline Configurations	C, I	R
CODE CREATION	**Customer**	**InterVision**
Application Code Creation	R	I
Source Code Management	R	I
BUILD AND PACKAGE	**Customer**	**InterVision**
Implement CI/CD Pipelines using tools like Azure DevOps and Jenkins	C, I	R
Integration Testing	R	I
Integrate Source Code Repository with Build Tool	C, I	R
Package management - Configure the CI/CD pipeline to pull build files (pre-built package containers/docker images)	C, I	R
Use deployment tool to deliver packages	C, I	R
Automated deployment of code to non-production customer environments using Jenkins, Azure DevOps, etc.	C, I	R
Deployment into Production environment	R	C, I
TESTING	**Customer**	**InterVision**
Test application code	R	
DEPLOYMENT	**Customer**	**InterVision**
Perform test deployments in the infrastructure	C,I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Making sure the deployment process works	C,I	R
Monitor deployments for success/failure	C,I	R
Troubleshoot failed deployments to production	C,I	R
INFRASTRUCTURE AS CODE (IaC)	**Customer**	**InterVision**
Provision Azure Resources using Azure Resource Manager or Terraform	C,I	R
Managing Servers using Ansible Package Installations or Webserver Setup	C,I	R
Request/Approve package installations	R	C,I
Requests for user creation or IP additions	R	C,I
Create users or add new IP address to security group as per request	C,I	R
Requests and Approvals for change request or change management process	R	C,I
Impact review and solution recommendation for major change requests	C,I	R
Maintenance Review recommendation and scheduling	C,I	R
Version control for configuration files	C,I	R
Test and monitor configurations	C,I	R
Managing manifests of Kubernetes deployments	C,I	R
RELEASE MANAGEMENT	**Customer**	**InterVision**
Configure the Release Management process per client	C,I	R
Define Release Management Stages based on different environments	C,I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Own Release Management to Production Environment	R	C,I
DATABASE UPDATES	**Customer**	**InterVision**
Update the required database schema with the new code that requires it	R	I
OPERATIONS	**Customer**	**InterVision**
Configure Logging & Backups of the Infrastructure	I	R
Implement Monitoring tools for the Azure Infrastructure	I	R
Created Build Documentation and Architectural Diagrams	I	R
Analyze Application Performance	R	C
Review Azure Monitor metrics - connection counts to load balancers, bottlenecks, connection buildup to DB servers - can involve an APM if the client has one	I	R
MANAGED SERVER SERVICE*	**Customer**	**InterVision**
Implement workflow for internal and external incident response teams	C,I	R
Patching of the infrastructure and guest OS services	C,I	R
Recommend and provision maintenance windows	C,I	R
Service-specific patching within scheduled maintenance windows	C,I	R
On-demand patching to address service-impacting bugs	C,I	R
Right-size the infrastructure and reservation management	C,I	R
Configure Backup policies using the Azure Backup service	I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Data restoration requests	R	I
Restore data as required	I	R

*The Managed Server Service list of tasks applies if the customer is using GitLab or Jenkins installed on an EC2 instances. These would then be managed by InterVision as part of the CI/CD pipeline.

Onboarding and Provisioning - Managed Cloud Service for DevOps Automation Service

In addition to general onboarding tasks, an assigned onboarding project manager will provide a list of customer dependencies and InterVision set up tasks during a kickoff meeting.

2.10 ONBOARDING

InterVision will provide a project manager to assist with onboarding the customer to the Managed Cloud Service for Azure. During this process InterVision will collect customer information, escalation data, runbook information, service set-up policy information and other critical data for the successful set up on managed services. During the workload onboarding process the following will be performed unless otherwise noted:

- Configure Entra ID access to managed cloud environment for InterVision and Customer access.
- Addition of Bastion servers (if necessary)
- Implement account-wide environment controls for access control, security, and infrastructure best practices
- Configure monitoring and log collection
- Security assessment of each Azure subscription and remediation recommendations.
- Additional service specific onboarding activities are detailed below
- VPN tunnel turn-up
- Add to Monitoring and Log Collection
- Add to Backup
- Add to Patching

Typical onboarding tasks include:

Onboarding	InterVision	Customer
Create Role and Identity Provider in Azure Console to enable IV SSO Access	C/I	R
Azure Tenant Creation	I	R*
Customer Escalation Information	I	R*
Anti-Virus subscription (if not already present. Trend Micro recommended)	C, I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

VPN Tunnel turn-up (Customer firewall)	I	R*
VPN Tunnel turn-up (Azure Side)	R	I
Synchronize on-prem AD with Azure AD by using Azure AD Connect	I	R*

*Asterisk means these tasks can also be performed by InterVision Professional Services.

Service onboarding is not inclusive of workload migration or workload implementations; these are separate services. MCS is designed to be initiated once workloads have been initially built or migrated to Azure.

2.11 RECURRING ACCOUNT REVIEW

During regularly scheduled account reviews throughout the Order Term, the InterVision CSDM will address the operational activities to be performed by InterVision, as for instance the following, as needed:

- Strategic: Service trend reports, business planning initiatives, customer satisfaction, annual plans and evaluation, and focused recommendations in the space of the Services
- Tactical: InterVision support processes associated with the Services, disruptive incidents, planned and completed changes and key known issues/problems, operational improvement, approaching events, and any other input for the day-to-day tactical engagement with the Services

2.12 SUBSCRIPTION RENEWAL

The InterVision CSDM will work with InterVision Client Success Manager (CSM) to track, notify and facilitate software and services renewals.

3 MANAGED CLOUD SERVICE FOR AZURE - SERVICE GUIDE CHANGE LOG

Below are the changes to this service guide.

Change date	Change Type	Change Details
06/20/2022	New Document	Initial release
11/28/2022	Addition	Added Azure Virtual Desktop Support responsibility matrix
04/07/2023	Addition	Added responsibility for "Removal of Malware on Managed Instances, meaning isolating the server, deleting it and restoring it from backup or image"

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Change date	Change Type	Change Details
08/14/2023	Addition	Added support information for Managed Cloud Service for Azure Containers. Added support information for Managed DevOps Automation Service.
02/13/2025	Addition	Added Service Delivery Policy stating Escalation to Cloud Support Vendor procedures and justification

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute