Contents

SERVICE OVERVIEW

The primary objective of the Managed Azure Core service is to offer customers managed Azure Foundation Platform (The platform) to migrate, build or run their application workloads. The service was developed and continuously maintained in alignment with Microsoft Cloud Adoption Framework and its Ready methodology. The framework follows the best practices, tools, documentation, and narrative, helping customers to better align with their business and technological goals.

Azure Foundation Platform

The IFX Managed Azure Core service delivers a fully managed Azure Foundation Platform, developed and continuously maintained in alignment with Microsoft's **Cloud Adoption Framework** and its **Ready methodology**. This solution helps organizations accelerate their cloud adoption journey by reducing complexity and bridging knowledge gaps in platform provisioning and operational support.

From a high-level perspective, the Azure Foundation Platform acts as a secure and scalable hosting environment for applications and workloads. Through Managed Azure Core, customers gain a robust foundation for their cloud strategy, with platform operations provided as an outsourced service for maximum efficiency.

The service is built on reference **architecture based on Landing Zone principles**, ensuring compliance, governance, and best practices for enterprise-grade deployments.

There are two main landing zone types:

- Platform Landing Zone
- Application or Workload Landing Zone(s)

Platform Core Components

Design Area	**Description**
Azure billing and Entra ID tenant	Azure Billing and Entra ID Tenant represent the topmost part of the reference architecture and focuses on the highest level across whole Managed Azure Core deployment. This design area covers subscription provisioning/decommissioning, customer billing, invoicing and consumption tracking across all CSP provisioned subscriptions associated with the customer Entra ID tenant. Managed Service Provider provides monthly billing and consumption tracking for all CSP subscriptions it has provided to the customer. Information about the consumption per resource will be generated at the end of the billing period and delivered at the beginning of the next billing period. The billing period starts beginning on the first day of the month. The Managed service provider can use existing or provision new customer Entra ID tenants. The Customer Entra ID tenant is always owned by the customer, represents customer organization, and serves as a security boundary.

Identity and access management	Identity and access management implements customer Active Directory extension to Azure and synchronization of customer identities with customer Entra ID tenant. Extension of customer Active Directory to Azure will ensure support for legacy applications or Azure resources requiring legacy authentication protocols such as Kerberos or NTLM. It also serves as a managed service provider to support management of platform specific workloads.
Network topology and connectivity	Network topology & connectivity implements traditional Hub-and-Spoke networking design and connectivity within the underlying Managed Azure Core service in form of virtual networks, subnets, virtual network peering, routing, and protecting inbound/outbound network traffic for virtual network subnets connected to central hub. It covers on-premises network connectivity in the form of Site-to-Site or Point-to-Site VPN or Express-Route circuit. Managed Azure Core offers IP address management (IPAM) of customer delegated IP address block with ability to request new IP addresses for Azure resource(s) over the API from predefined workload IP blocks. DNS name resolution within Azure and between Azure and customer on-premises.
Resource organization	Resource organization implements management groups hierarchy and organization of CSP subscriptions.
Security	Security compliance design area implements basic or advanced protection for CSP subscriptions including evaluation of security posture.
Governance	Azure resource naming is supported through central naming tool and exposed over API or web-based user interface. Customer workload teams or automated provisioning can make use of queries against the tool API to enforce standardize Azure resource names. Platform guardrails are implemented through IFX Baseline Governance Policy Set.

Platform Provisioning and Management

Design Area	**Description**
Management	Access to customer Azure environment: • Access to customer Entra ID tenants through Granular Delegated Access Control Permission (GDAP). a. T1 group (Helpdesk administrator, License administrator, User administrator, Billing administrator, Service support administrator, Global reader) b. T2 group (Global Administrator) • Access to customer subscriptions through Azure Lighthouse. The delegation can be initiated by MSP or by the customer. • Access to customer operating systems running on Azure virtual machines is ensured through MSP managed Active

	Directory Domain Services provisioned inside the customer Identity and Access subscription.
Platform automation and DevOps	Entire platform is defined as a code and stored within IFX customer specific repository.

Supported Regions

Managed Azure Core deployment is only supported by non-government Microsoft Azure regions.

Licensing

There are no specific initial licenses associated with Managed Azure Core provisioning.

PRODUCTS AND SERVICE DESCRIPTION

Platform Management

1) **Basic Platform Management**: Management of the underlying Azure Foundation Platform components defined within the core layer such as Tenant and Billing, Network Topology and Access, Governance and Security. In addition, management of the components defined within the Platform Management Baseline such as Inventory and Visibility, Resource Provisioning and Operational Compliance. (Monthly fee)

2) **Advanced Platform Management:** Custom solutions and resource provisioning, platform extensions and architecture support. (Per engagement)

Azure billing and Entra ID tenant

1) **Billing and Invoicing:** Provides customer billing, invoicing, consumption tracking and reporting.
2) **Subscription vending process:** The process covers Azure plan, CSP subscription provisioning and decommissioning.
3) **Entra ID Tenant provisioning:** Provisioning new or use of existing customer Entra ID tenant.

Identity and access management

1) **Active Directory Domain Service:** Extension of existing customer Active Directory domain forest to Azure, support for legacy application and services requiring Kerberos or NTLM authentication protocols.
2) **User identity synchronization:** Supports synchronization of customer identities to Entra ID tenants with use of Microsoft Entra Cloud Connect Sync or Microsoft Entra Cloud Sync.
3) **Entra ID management:** Basic customer Entra ID management to support Managed Azure Core service onboarding and operations such as create or decommission service principals, system or user managed identities, access management for CSP subscriptions, Azure Policy assignment, user, or group assignment to allow/deny access to managed service provider provisioned workloads.

Network Topology and Connectivity

1) **Network topology:** Provides traditional Hub-and-Spoke networking design, network connectivity between virtual networks and subnets, virtual network peering and routing.
2) **Traffic protection:** Provides inbound and outbound traffic protection from the central hub network.
3) **On-premises Connectivity:** Supports customer connection to Azure in form of Site-to-Site VPN, Point-to-Site VPN or ExpressRoute circuit.
4) **DNS Name Resolution:** Provides DNS name resolution within Azure and customer cross-premises.

Resource Organization

1) **Management Groups:** Management group hierarchy in the customer tenant supports management of CSP subscription and Azure policy assignment.

Governance

1) **Governance Baseline:** The governance baseline represents set of default Azure Policies and Initiatives to govern Azure Landing Zone reference architecture. It provides required guardrails for the platform and workload teams. List of applied policies and initiatives can be requested and delivered on demand.

Security

1) **Microsoft Defender for Cloud:** Basic security management at CSP subscription scope, measuring security posture, remediation of Azure resources.

RESPONSIBILITY MATRIX

Service Provisioning

Task	Service Provider	Client	Description
Customer assessment		x	Assessing customer requirements concerning number of subscriptions, workload types, asset criticality, on-premises connectivity method, network bandwidth, network traffic routing and filtering, IP address blocks, user synchronization, authentication and authorization for applications, users, and groups.
Initial setup and configuration	x	x	The service provider is responsible for delivering the Managed Azure Core foundation platform and implements the following areas: • Azure billing and Entra ID tenant • Identity and access management

			• Network topology and connectivity • Resource organization • Security • Management • Governance • DevOps organization The client is responsible to participate on delivering the outcome from specified design areas.

Table 1. Service provisioning.

Components Setup

Task	Service Provider	Client	Description
Azure billing and Entra ID tenant	x		The service provider is responsible for: • Set up new Entra ID tenant. ○ Setup Entra ID Connect Sync or Entra ID Cloud Sync. • Request Granular Delegation Admin Permissions to the Entra ID tenant for T1 and T2 users. • Track and optimize costs for Managed Azure Core Foundation platform. • Generate and deliver invoices for Azure resource consumption and licenses.
Identity and access management	x	x	The service provider is responsible for: • Install AD DS and support customer on-premises AD DS extension to Azure. • Set up and maintain AD DS trust with the customer on-premises AD DS forest. The client is responsible for participating in delivering the outcome for AD DS extension.
Network topology and connectivity	x	x	The service provider is responsible for: • Setup virtual networks and subnets. • Establish HUB to HUB connectivity between multiple Managed Azure Core instances. • Establish Hub-and-Spoke connectivity within Managed Azure Core instance. • Prepare VPN or ExpressRoute gateway in Azure for connectivity with the customer on-premises. • Configure routes within Azure and to the customer on-premises.

			• Setup DNS name resolution between Azure and customer on-premises. • Deploy and set up Azure Firewall within Managed Azure Core instance. The client is responsible for: • Prepare on-premises for VPN or ExpressRoute connectivity. • Define IP address block for Managed Azure Core instance. • Define network firewall rules for Azure application workloads.
Resource organization	x		• Deploy management group hierarchy in customer Entra ID tenant. • Associate subscription(s) with management groups. • Assign Azure Policies within managed service provider management group hierarchy or directly on CSP subscriptions.
Security	x		• Protect subscription(s) by Microsoft Defender for Cloud Foundational CSPM. • Evaluate security posture across CSP subscriptions.
Special Request	X		• Change, addition etc. defined as additional managed service is billed separately.

Table 2. Core components.

Basic Platform Management

Task	Service Provider	Client	Description
Subscription and licenses	x	x	The service provider is responsible for: • Provision new CSP subscription(s). • Decommission CSP subscription(s). • Delegate CSP Subscription(s) to service provider. • Create Azure reservation for Azure virtual machines. • Track and optimize costs for platform related resources. • Manage access to CSP platform subscription(s). • Manage access to CSP workload subscription(s).

			The client is responsible for: • Request new CSP subscription(s). • Request to decommission existing CSP subscriptions(s) • Request Azure reservation for Azure virtual machines. • Manage management group hierarchy outside of managed service provider management group hierarchy in Client Entra ID tenant.
Entra ID Tenant	x	x	The service provider is responsible for: • Create and maintain service principal for Azure resource provisioning to CSP subscription(s). • Create temporary guest accounts in customer Entra ID tenant to perform tenant wide administrative tasks related to service provider managed workloads and applications. • Access management for service provider managed workloads and applications. The client is responsible for: • Entra ID management.
Identity & Access	x	x	The service provider is responsible for: • Azure AD DS user and group policy management for managed service provider provisioned workloads and applications. • Manage access to managed service provider workloads and applications. • Maintain AD DS forest trust. The client is responsible for: • Azure AD DS user and group policy management.
Network topology & connectivity	x		The service provider is responsible for: • Maintain existing virtual networks, virtual network peering and virtual network subnets. • Maintain existing routing for virtual network subnets. • Maintain DNS records for Private DNS zone and DNS zone hosted on AD DS domain controllers. • Integrate platform DNS zone with new or existing virtual network(s).

			• Maintain DNS name resolution between Azure and customer on-premises. • Deploy and maintain Azure firewall rule groups, rule collections and rules. • Deploy and maintain Azure Application Gateway. • Deploy and maintain private or public Azure load-balancer. • Prepare VPN or ExpressRoute gateway with additional customer branch offices. • Maintain IP address ranges for IPSec tunnel.
Governance	x		• Provision and maintain platform Baseline Policy set to govern platform resources.
Security	x		• Manage Microsoft Defender for Cloud foundational CSPM. Manage and remediate non-compliant platform resources.

Management Baseline

Task	Service Provider	Client	Description
Inventory & Visibility	x	x	The service provider is responsible for: • Maintain platform IPAM and IP address space allocated to Azure. • Monitor Managed Azure Core platform and process platform related events. • Monitor Azure resources and forward workload related events to customer ITSM tool. The client is responsible for: • Process workload or application related events.
Operational compliance	x	x	The service provider is responsible for: • Maintain Azure naming tool and naming policy standards for Azure resources. Maintain existing default naming rule set. • Use Azure Naming tool to generate names for Azure platform or workload resources. The client is responsible for:

			• Use Azure Naming tool to generate names for Azure workload resources.
Protect & recover	x		• Primary support contact for platform or workload related issues.
Special Request	x		• Change, addition etc. defined as additional managed service is billed separately.
VM provisioning	x		• Provision Azure virtual machine(s).
Protect & recover	x		• Maintain virtual machine(s) backup. • Perform backup and restore operations for Azure virtual machines or individual files. • Maintain Azure storage account(s) backup. • Track and report Managed Azure Core platform security posture. • Perform backup and restore operations for Azure storage account(s) data. • Default backup protection (Datacenter only/LRS)
Inventory & Visibility	x		• Maintain platform virtual machine inventory. • Monitor changed on Guest operating system (Limited to certain Azure region).
Operational compliance	x		• Setup and maintain Windows/Linux update management for server operating system instances. • Remediate failed updates. • Monitor compliance of Azure resources. Remediate non-compliant Azure resources • Maintain customer ITSM connector to ensure proper event routing.
*Special Request	x		• Change, addition etc. defined as additional managed service is billed separately

Table 3. Basic platform management

Advanced Platform Management

Task	**Service Provider**	**Client**	**Description**
Extend or adjust existing platform architecture	x	x	• Architectural extension of the underlying platform to support new functionality or workload provisioning.

On-demand Azure resource provisioning	x		• Provision on-demand Azure resources which are not published in self-service catalog.
Package custom Azure resources	x		• Package Azure resource(s) that require regular provisioning by the customer workload teams as approved solutions. • Publish approved solution to self-service application catalogue.
Reporting	x		• Provide custom platform related reports.
Governance	x	x	• Transform company regulation(s) into custom Azure policies and initiatives.
Design disaster recovery concept for secondary Azure region	x	x	• Setup Managed Azure Core platform instance in customer chosen secondary Azure region.
Backup & Recovery test	X		• Perform backup and recovery test for Azure virtual machine(s), Azure virtual machine(s) file(s) or Azure file storage file(s).
Disaster recovery test	x	x	• Perform on-demand DR test.
Provision Azure DevOps organization	x		• Provision dedicated Azure DevOps organization with connection to customer workload(s) subscription(s).

Table 4. Advanced platform management

Service Level Types

Ticket resolution time by priority per product

The following ticket resolution relates to Managed Azure Core platform landing zones.

a) Definitions

Service Level	Value <=	Target	Service Hours	Type	Incident Ticket	Request Ticket	Calc. Method	Met Criteria
P1 – CRITICAL Resolution Time	4 hours	95%	24x7	SLO	Yes	N/A	Value	Above
P2 – HIGH Resolution Time	8 hours	95%	24x7	SLO	Yes	N/A	Value	Above
P3 – MEDIUM Resolution Time	24 hours	90%	9x5	SLO	Yes	N/A	Value	Above
P4 – LOW Resolution Time	72 hours	90%	9x5	SLO	Yes	N/A	Value	Above

b) Tickets are dispatched to a Service Provider's Support Team for resolution when it is in scope of a Service Provider's Service sold to Client. Tickets are closed when resolution is out of scope of Service Provider's Services sold to Client; and Client's Support Team is then responsible for resolution.

c) Ticket Resolution Time by Priority is default for all Service Provider Services sold to Client. They may be superseded if explicitly defined in the service description for another Service Provider Service sold to Client.

d) Ticket Resolution Time by Priority is measured automatically per ticket based on its initial priority as the sum of the Service Provider Service Level Clock times recorded for each ticket.

e) Due to the high variability of Service Request delivery times, Service Request tickets are excluded from Ticket Resolution Time by Priority. Any expected Service Request delivery times shall be defined in a Service Request Catalog. If a Service Request is not defined in a Service Request Catalog, the PSM and CSM shall mutually agree on the details and set expectations.

List of Abbreviations

Abbreviation	Description
CSP	Cloud Solution Provider. Organization who provisions or delivers cloud services.
MSP	Managed Service Provider. Organization who manages provisioned and delivered cloud services.