Insight – Managed Cloud Platform - Azure - GC14 L3 – Service Definition

1 Service Offering

Managed Cloud Platform - Azure

2 Introduction

The purpose of this document is to provide a Global Service Description that creates and maintains a common definition of the Managed Cloud Platform - Azure Managed Service.

The Managed Cloud Platform - Azure service offering is made up of the following service descriptions which together deliver Managed Cloud Platform – Azure services:

Managed Cloud Platform – Azure – This document.

3 Service Description

The Managed Cloud Platform service is Insight's foundation Managed Service for Azure Infrastructures and is based on Modern Operations techniques following the Well Architected Framework guidance from Microsoft. It provides support for the core platform and governance elements of an Azure tenancy including, cost, network, policy management, platform observability, deployment, and provisioning. The Managed Service extends to the landing zones which contain the underlying resources and functions being consumed by the Client.

4 Service Scope

- The scope of the Managed Service defined here is based on the monitoring, management and support of resources within an Azure Infrastructure based on the Windows and Linux Operating Systems.
- All Managed Services defined here are delivered in English for verbal and written communication.
- All Managed Services defined here are delivered on a 24x7x365 basis.
- The Managed Services defined here are delivered remotely using Insight's Global Delivery Network, which includes personnel in India, North America, Europe, Asia Pacific regions.
- Insight's ITSM Platform is ServiceNow.
- PaaS Monitoring for URLs is for up to 20 web sites.

5 Service Outcomes

Insight provides the following value as part of the service. Section 5 provides overviews of the activities that Insight performs as part of the service. Detailed breakdown of specific scope is detailed in section 6.

The following outcomes are delivered as part of the service.

5.1 Monitoring and Alerting

- Reactive Issue Detection: Detect and address issues promptly, minimizing downtime and ensuring continuous availability and performance of the Azure Infrastructure.
- Faster Issue Resolution: Receive intelligent alerts and notifications, enabling you to proactively address issues, troubleshoot problems, and reduce mean time to resolution (MTTR).
- Increased Security and Compliance: Report security events and configurations to protect your Azure Infrastructure, identify vulnerabilities, and meet regulatory requirements.

5.2 IaaS and PaaS Management

- Operational Management: The management of IaaS and PaaS Azure Environments delivers operational efficiencies and costs effective delivery.
- Enhanced Performance and Reliability: Proactively managing the Azure Infrastructure and applications optimizes response times, enhances user experience and increased reliability.
- Scalability and Agility: Manage auto-scaling groups in IaaS and PaaS environments by assisting in scaling resources up or down based on demand in response to changing requirements.
- Azure IaaS and PaaS in scope resources within this service are listed as follows (Unless explicitly listed other Azure resources are out of scope for this service):

Azure Site Recovery	Azure Kubernetes Service (AKS)	Microsoft Azure portal
Application Gateway	Azure Lighthouse	Microsoft Cost Management
Archive Storage	Azure Monitor	Network Watcher
Azure Advisor	Azure Policy	Storage Explorer
Azure Backup	Azure Service Health	Traffic Manager
Azure Bastion	Cloud Shell	Virtual Network
Azure Blob Storage	Event Hubs	Virtual WAN
Azure DNS	Key Vault	VPN Gateway
Azure ExpressRoute	Linux Virtual Machines	
Azure Files	Load Balancer	

5.3 Cloud Native Network Management

- Improved Network Performance: Optimizing the Azure Network infrastructure results in enhanced performance, reduced latency, and improved application response times.
- Enhanced Security and Compliance: Implementing robust security measures ensures compliance with industry regulations whilst leveraging Azure's advanced security features to protect network infrastructure, data, and applications from threats, vulnerabilities, and unauthorized access.
- Increased Agility and Scalability: An Azure Network must adapt to changing business needs by scaling to handle increased workloads and support new applications.

5.4 Cost Management

- Cost Transparency: Full visibility of Azure spending to show how costs are distributed and identify areas for optimization.
- Cost Savings and Optimization: Leverage cost optimization recommendations and insights to identify and implement cost-saving measures through optimizing resource usage, leveraging discounts and adopting best practice.
- Improved Financial Planning: Forecasting future Azure spending and analyzing cost trends to enhance the financial planning processes.

5.5 Security Configuration Management

- Enhanced Security Posture: Strengthen the security of your Azure environment with optimized security configurations, adherence to best practices, and continuous monitoring. Mitigate the risk of security breaches, data leaks, or unauthorized access.
- Compliance and Regulatory Alignment: Align with industry-specific regulations, data protection laws, and compliance frameworks by implementing and maintaining secure configurations that meet the required security standards.

6 Service Building Block Definitions

The Managed Cloud Platform service comprises the following Service Building Blocks:

6.1 Monitoring and Alerting

Monitoring and Alerting utilizes intelligent anomaly alerting and event correlation to ensure the continuous availability, performance and security of the Azure Infrastructure. The Monitoring and Alerting Service ensures any issues are identified and resolved within SLO's listed in section 8 of this service description. Alerts and response by the Insight support team optimizes resource utilization and the overall reliability of the environment.

In response to any Alerts that are raised through Monitoring the Alert Response Process is followed:

- Alert correlation and investigation.
- For all Alerts within Insight's scope the following actions will be undertaken:
  - Known Error – the Incident Management process will be followed to take remedial action following a Runbook.
  - Unknown Error – initiate triage escalating the appropriate Resolver Group.
  - Error Auto-Recovers – alert auto-close.
- For Alerts outside of Insight's scope these will be escalated by Insight to the Client for resolution by the Client's Resolver Groups or Client contracted Third Party Resolver Group.

The Monitoring and Alerting Service is based on the following Baseline Monitoring Profiles:

6.1.1 PaaS Monitoring:

PaaS Monitoring in scope resources within this service are listed as follows (Unless explicitly listed other Azure resources are out of scope for this service):

- Azure API Management Service – Availability.
- Azure App Service –Response Time, Memory, CPU, Availability, HTTP 5xx Errors.
- Azure App Gateway – Backend Connect Time, Current Connections, Failed Requests, Availability, Throughput.
- Azure Bastion – Availability.

- Azure CosmosDB – Availability.
- Azure Data Factory – Availability.
- Azure DNS Zones – Availability.
- Azure Event Hub – Namespace Availability, User Errors.
- Azure Function App – Availability.
- Azure Key Vault – Availability, ServiceApiHit.
- Azure Kubernetes Service – Node and Pod Status, Node CPU, Node Memory.
- Azure Queue – Availability.
- Azure Files – Availability.
- Azure Recovery Service - Vault Backup Health.
- Azure Traffic Manager – Profile Availability.
- Azure SQL Database – CPU, Deadlocks, DTU, DWU, Storage Capacity.
- Storage Accounts – Capacity.
- URL Monitoring.

6.1.2 Network Monitoring:

Network Monitoring in scope resources within this service are listed as follows (Unless explicitly listed other Azure resources are out of scope for this service):

- Network Interface I/O, VNET Network I/O.
- Azure Firewall – Availability, Health.
- Network Load Balancer – Health Probe, Availability, VIP Availability.
- Network Gateway – Availability, P2S Count.
- Virtual Network – Connected Peer Status, Peer Count, Bandwidth.
- Express Route – CPU (Gateway), Network I/O, BGP Availability.

6.1.3 MS SQL Database Monitoring:

MS SQL Database Monitoring in scope resources within this service are listed as follows (Unless explicitly listed other Azure resources are out of scope for this service):

- MS SQL - Utilization, CPU, Memory, Data In/Out, Time, Disk Performance, Filesystem, Network In/Out.
- Deadlocks, DTU, DWU, MS SQL Storage Capacity, Database State.

6.2 IaaS and PaaS Management

The IaaS and PaaS Service provides management and optimization of the Azure Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) environments. This ensures the Azure Infrastructure hosting client applications are running efficiently and securely.

The activities undertaken are:

- Moves, Adds, Changes and Deletes of IaaS and PaaS deployed resources.
- Optimization - Auto Start/Stop of Compute Resources (IaaS only), Rightsizing, Orphaned resource cleanup.
- Trend Analysis and Remediation of Performance Metrics.
- CMDB Management related to the in-scope Azure Environments.
- Rightsizing Image types, Network Interface attachment to VNET, Auto scale Management, Auto on/off schedules.

6.3 Cloud Native Network Management

The Cloud Native Network Management Service for Azure provides management and optimization of the Native Network Infrastructure to ensure its scalability and resiliency. With a focus on cloud-native principles and leveraging Azure's advanced networking capabilities, our service empowers you to maximize the performance, security, and agility of your network infrastructure.

The activities undertaken are:

- Moves, Adds, Changes and Deletes of IaaS and PaaS Network deployed resources under management.
- Firewall and Application Gateway configuration.
- VPN Configuration and troubleshooting - P2S, S2S.
- Network Security Gateway (NSG) Configuration, Port blocking / unblocking, Security filtering (Port, Public IP etc.), Access Lists.
- Load Balancer Configuration.
- Azure VNET Configuration and Management – Subnet creation, VNET-VNET peering, VWAN.
- Express Route Gateway – Peering Configuration (Microsoft Edge), VNET Configuration, VNET linking to IaaS.
- Recommendation for High Availability & Security.

6.4 Cost Management

The Cost Management service supports the optimization of Azure resource usage, control costs, and maximizes the value of the investment. The Service provides insights into Azure spending, identifies cost-saving opportunities, and supports informed decisions being made to optimize cloud expenditure.

The activities undertaken are:

- Configuration and maintenance of Azure Cost Manager.
- Provision of Cost Optimization Reports to provide the Client with visibility of cost efficiencies.
  - Cost Reports are set up to show the highest utilized resources by subscription, by resource type, by resource group, by customer tag (if customer tagging is already deployed and enabled) to drill down to what specific areas of Azure are cost host spots.
  - Configure Budget Threshold monitoring and Alerting - Set with Standard threshold (50% - 85% - 100%) based off client budget guidance.
- Provision of Optimization Recommendations comprising.
  - Configure Auto Start / Stop of VM’s.
  - Identify and upon request, delete unused resources, orphaned disks, network interface, public IP’s, allocate/de-allocate storage (delete).

- VM Image & Disk resizing.
- Storage Account Management.
- License optimization recommendation changes such as Pay-as-go vs Reserved Instances.

6.5 Security Configuration Management

The Security Configuration Management service provides reporting of compliant or non-compliant security configurations within the Azure Infrastructure by assessing the deployed resources against 50+ possible security frameworks. The service identifies where resources are not configured securely and may cause risk and vulnerabilities, which in turn ensures the integrity, confidentiality and availability of the Azure Infrastructure, while meeting compliance requirements.

The activities undertaken are:

- Running reports to provide visibility into security posture. The reports consist of security score, categorized vulnerabilities, detailed analysis and recommendation of remedial actions to be taken.
- Upon request remediate security findings from reports to improve security posture.

The standard Infrastructure Security Monitoring and Reporting categories are:

6.5.1 Infrastructure

- Cloud accounts without policies set.
- Container with critical security vulnerabilities.
- VM, AKS and Database instance security misconfiguration.
- Storage accounts with public access.
- Volume encryption disabled.
- Resources with overly permissive access.
- Identify users with permissive access (Full, Admin, Power, Owner).

6.5.2 Orphaned resources (Disk, Public Ips, Snapshots older than 60 days) Network Security

- Firewall Access List misconfiguration findings.
- Hosts and Storage accounts with public internet access.
- ACL’s allowing public RDP and SSH access.
- Instances without Access Lists.
- SSL Certificates expiring for up to 20 web sites.
- Compliance Reporting measured by standard cloud security frameworks.
- App Services not enforcing HTTPS and TLS Versions.

6.5.3 IPsec VPNs secure remote connectivity

- Cloud Native VPN Gateway and Tunnel Configuration Management.
- Cloud Native WAF HTTP/HTTPS Management - Restricting flow of traffic to specific IP address or range for the ports 80 & 443.

7 Pre-Requisites and Assumptions

The following are the Pre-Requisites and Assumptions that apply to the Managed Service:

1. Managed Service pricing is based on the Monthly Cloud Consumption where a monthly analysis is performed to determine the fees for that month. Pricing is based on the Microsoft invoiced monthly consumption including Reserved Instances. Charging will commence once monitoring of the Azure Infrastructure commences.
2. Insight will deploy, maintain, and administer its own tooling to deliver the Managed Service. Client access to Insight's tooling is not provided.
3. Client will deploy Insight specified resource tagging to enable Insight to deliver monitoring and reporting of the Azure Infrastructure.
4. Client shall provide Insight Granular Delegated Access Privileges (GDAP) relationship configuration so that Insight can leverage Insight's Microsoft Azure Premier Support. Failure to have a Microsoft support contract associated to the Client's cloud tenant may impact Insight's ability to meet Service Level Objectives (SLO) targets.
5. Insight is not responsible for any SLO breaches because of inadequate Client procured Third-Party vendor support.
6. Client shall assist the Insight team in creating operational run books necessary to respond to deliver monitoring, Incident and Request Management of the service.
7. The Client shall be responsible for reviewing all Status Reports and raising any queries with the Insight Technical Delivery Service Manager and/or Service Delivery Manager within 10 business days of the Status Reports being issued.
8. The Client shall fully cooperate with Insight and shall keep Insight apprised of all information relevant to the successful delivery of the Managed Services in a timely manner.
9. The Client understands and agrees that any delay in providing such information to the Insight Technical Delivery Manager and/or Service Delivery Manager may result in delays for which Insight shall not be liable. Failure by the Client to notify Insight, in a timely manner, of concerns arising out of the Managed Services, whether identified in the Status Reports or otherwise shall be deemed an acceptance of such Services by Client.
10. The Client is responsible for granting Insight the required access and authorization rights, logins and documentation to deliver the Managed Service.

8 Service Levels

Insight Managed Services are delivered to a standard set of service levels that address response and resolution times as well as fulfillment expectations for service requests. To maintain the highest levels of service delivery these definitions are consistent across all clients. Insight may update service level and service request definitions periodically with the intent being to deliver improved services, drive clarity in our offerings, and remain market competitive.

Service levels for this service are governed by the G-Cloud 14 Framework Service submission or can be provided separately upon request.

9 Service Management

The delivery of Managed Cloud Platform is underpinned by the following ITIL Service Management Processes:

- Incident Management - An unplanned interruption to a service, or reduction in the quality of a service.
- Service Request Fulfilment - A formal request from a user for something to be provided – for example, a request for information or advice.
- Event Monitoring and Management – An Event is any change of state that has significance for the management of a service or other configuration item (CI). Events are typically recognized through notifications created by the monitoring tool.

- Change Enablement - The process of tracking and managing a change throughout its entire life cycle, from start to closure, with the aim to minimize risk.
- Problem Management - To reduce the likelihood and impact of incidents by identifying actual and potential causes of incidents and managing workarounds and known errors.

9.2 Communication Channels

The Client can engage Insight through any of the following methods:

Priority 1-4 Incidents:

- Self-service ticket submission for Client IT Administrators via the Insight Client Service Portal.
- Phone-based access is available by calling the provided Telephone Number.

Service Requests:

- Self-service ticket submission for Client IT Administrators via the Insight Client Service Portal.

9.3 Incident Management

For all Incidents related to the Managed Service defined here, all Client contact will be through designated Client IT Administrators.

Once an Incident has been logged by Insight via one of the methods described in Section 11, the following process will be used for recording and resolving Incidents:

1. Categorize Incident type and technology.
2. Determine and assign Incident priority based on Urgency and Impact.
3. Troubleshoot Incident, engaging Client IT Administrators as necessary.
4. Escalations to level 2 and 3 Insight staff, then Microsoft.
5. Resolve Incident, document resolution, and close the Case.
6. Escalate to Client IT Administrators.

9.4 Service Request Fulfilment

For all Service Requests related to the Managed Service defined here, all Client contact will be through designated Client IT Administrators.

Service Requests are defined as minor (standard) changes that may be requested by clients in support of normal IT operations. Service Requests may be initiated through Insights service request catalog made available through the service management portal. Service Requests are considered low risk changes that can be carried out quickly using standard operational change processes, may include automation, and do not require advanced planning, scheduling, or change controls. The expected time to fulfil the request varies and is specific to the type of request. The expected delivery time will be displayed on each request item. Request Fulfillment is offered as an inclusive service for certain tiers of offerings.

Once a Service Request has been logged via one of the methods described in this document, Insight will follow the process for recording and actioning Service Requests.

Service levels for this service are governed by the G-Cloud 14 Framework Service submission or can be provided separately upon request.

9.5 Service Delivery Management

The Insight Service Delivery Manager ensures the Client is receiving the Managed Services contracted and will act as the primary point of contact for the Client on all Service Delivery matters including the following:

- Central point of contact for any Service Delivery questions and escalations.

- Attendance, Chairing and Minuting of Service Reviews.
- Service Reporting including reporting of Service Level Achievement.
- Respond and Resolve Service Billing and Service Reporting queries.
- Acting as an entry point to Insight for any queries outside of the Managed Services defined here.

9.6 Change Enablement

To maximize the number of successful changes made within a client environment, Insight Managed Services adheres to a Change Management process to properly evaluate proposed changes. Insight will leverage either the clients Change Process or for clients without a Change process, Insight will leverage the Insight ITIL Change Processes.

- Insight will identify a change required, open a change ticket in the Insight ITSM platform and work with the client to review the change and identify a maintenance window.
- For Emergency changes, Insight will contact the client primary contact to describe why the Emergency Change is required, what is being changed and ensure the client is aware of the change.
- Clients are responsible to inform Insight about change blackout windows or change freezes in the client Azure environment.

Anytime there is a request to make a change to a Configuration Item (CI) in the CMDB, a Change Request will be opened. If the CI is affected a change will be opened. Changes will typically have an approval process defined and tracked within the Change form. Insight Managed Services will adhere to Client Change Control Processes, as needed. This can include participation in a Client Change Advisory Board.

Insight's Phases for a Change has 3 main areas:

1. Schedule Change - requested by, planned start date, planned end date.
2. Planning of the Change – change plan, backout plan, test plan.
3. Execute Change Completion - completion code, close notes, closed date.

9.7 Problem Management

Problem Management aims to manage the lifecycle of all Problems. The primary objectives of this ITIL process are to prevent Incidents from happening, and to minimize the impact of incidents that cannot be prevented. 'Proactive Problem Management' analyzes Incident Records, and uses data collected by other IT Service Management processes to identify trends or significant Problems.

ITIL defines Problem Management as the process to prevent Incidents from occurring, and to minimize the impact of incidents that cannot be prevented through workarounds. Within Insight Managed Services, there are two types of Problem Management tickets:

1. Proactive: Analyze Incident Records, and use data collected by other IT Service Management processes to identify trends or significant Problems before they impact services.
2. Reactive: Investigation into multiple Incidents or a Major Incident. This process typically involves a Post-Incident Report or Root Cause Analysis.

Insight Managed Services conducts Problem Management as part of overall continuous service improvement. Insight conducts exercises to analyze and ultimately reduce incidents and reviews Incident trends in the Service Review Meetings. In addition to the Incident analysis, Insight looks at which CI's within the CMDB are creating the most Incidents. Additionally, reactive Problem Management can be leveraged to help track real-time problems as they are identified.

9.8 Service Reporting

Insight provides regular Service Reporting on various elements of the Managed Service. The Service Reporting is accompanied by Service Review Meetings, which are held monthly.

Service Reporting comprises:

- Service level metrics – Incidents & Requests created and resolved.
- Monitoring metrics – Incidents created from monitoring systems.
- Cost – Cloud Spend by subscription, resource type, resource group.
- Security – Critical security findings and security score.

10 Service Exclusions

The following items and activities are out-of-scope and are not part of the Managed Service:

1. Any activities not stated in this Service Description are excluded.
2. Marketplace purchased Appliances.
3. Application Middleware, like but not limited to Java, .Net, Springboot, Node, MQ, etc.
4. Application code or deployed applications hosted on Azure IaaS or PaaS.
5. Client deployed Infrastructure as Code environments, DevOps, Repo's, CI/CD Pipelines.
6. Azure features in Preview, End of Sale or End of Support.
7. Identity Management in managed environments.
8. Support for third-party tools related to the Microsoft Azure environment.
9. Responding to and resolving antimalware or endpoint security alerts and incidents.
10. Support for on-premises solutions and services, including compute, storage and network capabilities.
11. Support for any features and applications defined as service exclusions.
12. Virtual Machine management, including OS patching, password resets and configuration.
13. The following activities are deemed project work; scoped and invoiced separately:
    - Large or complex Change Requests defined as Normal Changes.
    - Operating System version upgrades, this will be deemed Project Work; scoped and invoiced separately.
    - Support for Cloud Migrations and Deployments.
    - Any other activities not explicitly stated in the Service Descriptions will be deemed project work; scoped and invoiced separately.

11 Service Transition

The activities for Service Transition, including Roles and Responsibilities between the Client and Insight, and the associated timelines are defined in the Managed Cloud Service Transition document, which comprise the Project Plan, Onboarding Checklist and Service Transition Process Flow. This will include information on the standard Service Configuration and Tooling deployment required to enable the Service to go live.

12 Tooling Architecture

The Tooling Architecture is defined in the Managed Cloud Tooling Architecture document.

13 Service Plan

The Service Plan for the Azure Managed Service is based on the Monthly Azure Consumption and Managed Service Requirements, which creates a consumption-based charge. An example scenario is shown below for reference:

For example, a client has subscribed to the managed service with an agreed 25% monthly fee. The clients Microsoft Monthly Azure Consumption Invoice is $80,000.00, Insight will charge the client a management fee of $20,000.00 per month, based on 25% of $80,000.00.

When the Monthly Azure Consumption exceeds $500,000.00 per month the Managed Service is considered Custom and a bespoke Service Plan is agreed with the Client to reflect the complexity and scale of the Azure Infrastructure being supported and the associated business demands.

Pricing is determined using a tiered pricing model.

The Service Plan is based on the activities defined in this Service Description.

For activities directly associated to Client demand, these being Service Requests, the Service Plan is based on a Fair Usage Policy as described below:

- Average Usage: the number of Service Requests is measured for the first 3 months of the Contract and divided by the average number of Azure Resources in scope during the same period to establish an Average Usage for the Service Plan. The Average Usage measure aligns the changes in Client demand for Service Requests with changes in the in-scope Azure Infrastructure.
- Reasonable Usage: is defined the Average Usage plus or minus 10% in any month, which is agreed with the Client as being reasonable and proportionate to their business requirements and usage of the Managed Service.
- Monitoring: Insight will monitor Service Requests on a quarterly basis to determine Actual Usage, based on the average number of Service Requests in that quarter, and identify any abnormal or excessive use that impacts the performance or stability of the Managed Service.
- Notification and Remedial Action: In the event of the Actual Usage being in excess of the Reasonable Usage, Insight will notify the Client and discuss changing the Service Plan to reflect the increased workload.
- Service Modifications: If the Client consistently exceeds the Reasonable Usage limits despite reasonable attempts to address the issue, Insight reserves the right to modify the Service Plan, impose additional charges, or terminate the contract, subject to any applicable notice periods and contractual obligations.

14 Roles and Responsibilities

The following matrix provides a view of the key activities in delivering the Managed Service where these activities are shared or there is a dependency between Insight and the Client.

Activity	Insight	Client
Monitoring and Alerting		
Deployment and Management of Insight Tooling and Platforms	X	
Deployment and Management of Alert Profiles	X	
Event Triage and Incident Response	X	
Reporting	X	
IaaS and PaaS Management		
Azure IaaS and PaaS	X	
Non-Azure Services		X

Activity	Insight	Client
Subscription and Tenant Management		X
Identity Management		X
Azure Portal Access		X
Azure Lighthouse	X	
Azure Bastion	X	
Cloud Native Network Management		
Azure Network (VNET, VWAN, Network Interface)	X	
Express Route (Microsoft Edge)	X	
Express Route (Client Datacenter Edge)		X
Express Route Circuits and Providers		X
3rd Party Firewall, SDWAN		X
Cost Management (upon request)		
Configuration and Maintenance for Azure Cost Manager	X	
Provision of Optimization Recommendations	X	
Actioning of Optimization Recommendations	X	
Clean up	X	
Reservations	X	
Right Sizing	X	
Focused Optimization	X	
Security Configuration Management		
Cloud Security Configuration Assessment	X	
Security vulnerability remediation		X
Vulnerability, Risk Management & Assessments		X
Security Incident Alerting & Response		X
Anti-malware, Anti-virus		X
Service Management		
Incident and Service Request Portal	X	
Incident Triage	X	
Incident Resolution and Service Request Actioning	X	
Escalation	X	
Major Incident Management	X	
Generating Requests	X	
Request Resolution	X	
Incident and Service Request Reporting	X	
Change Enablement		
Generating Change Requests	X	
Change CAB & Approvals		X

Activity	Insight	Client
Planned Maintenance Windows / Downtime Definition		X
Blackout Window Definition		X
Microsoft Maintenance Windows / Downtime	X	