STATEMENT OF WORK - Service Description

Managed Hosted Server

Contents

1 Scope of services

1.1 Managed Hosted Server Services

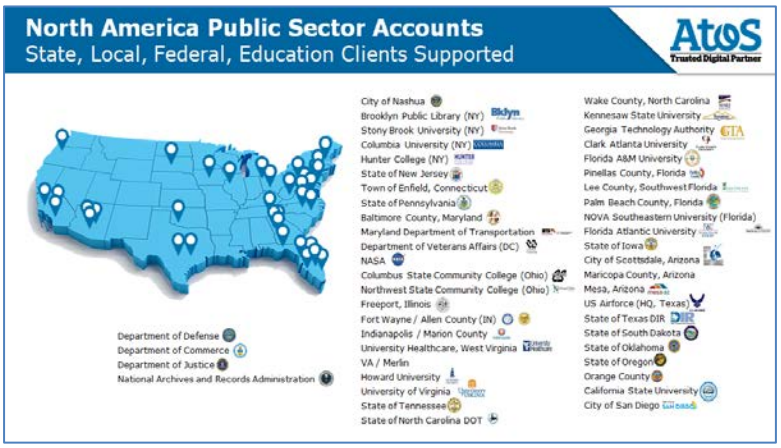
1.1.1 Description

Executive Summary

Atos is a comprehensive IT services provider who can provide any services that state and local entities need, from Mainframe to High Performance Computing. Atos has extensive experience in similar environments to yours and delivers with a "service Beyond Reason' mentality.

Government Expertise

With more than $13 billion in annual revenue, Atos provides IT services across the spectrum of technology with a **company focus in the State & Local and Public Sector** based on the following highlights:



- 11,000+ business technologists focused on delivering public sector projects and solutions
- More than 22 percent of total revenues coming from work for central, regional, and local governments
- 40 years' experience of designing and delivering public sector projects

We have experience in transitioning large, complex state and local governments, such as the State of Texas, from existing incumbent providers, including the provision of the future today via our Atos government cloud framework. This allows ultimate flexibility and service choice for state agencies, local governments and educational institutions.

Atos is an expert at providing advanced server services to local and state government entities with various compliance requirements. Atos has designed the services within this proposal to support normal generic state and local requirements, any specialized requirements can be accommodated with adjustments to meet the specific requirements. The following sections describe the services provided in more detail. What is included?

- Hosting of servers – data center infrastructure
- Server hosting can include both physical and virtual servers and databases
- Comprehensive server management both pro-active and re-active
- Basic server security
- A centralized, enterprise service desk to capture and record incidents and requests via email, voice, via mobile devices and chat if desired
- Storage management
- Network management
- System and data backups – Tape or replication based
- DR plans and architecture to support needs for sustainability

Atos delivers all these services with a client centered framework and more importantly, attitude that we call 'Service Beyond Reason'.

Service Beyond Reason

Atos' foremost objective is to ensure **we exceed expectations and fulfill our client's vision**. With **one of the highest contract renewal rates in the industry**, Atos lives and breathes a **"Client for Life" approach** for our clients.

What is Service Beyond Reason? It means understanding your goals and your needs and managing the services to those as opposed to a contract. It means over-communicating and going the extra mile to be sure we deliver for you and for your clients as well. Service Beyond Reason is not measured via SLAs or KPIs but purely via the satisfaction of our clients as communicated daily, weekly and monthly.

Being the **best in providing public sector services** to states, cities, and counties, no other company has the proven experience, capabilities, and happy clients like Atos, we are **bringing our best to you**! We look forward to meeting with you and working together to ensure your ongoing success.

Managed Server Services provides certain activities related to the Server Hardware and the Operating System, and addresses the following:

- Resolving Incidents
- Daily operations
- Retaining security
- Tooling required to execute these activities

The Supplier executes daily operations/monitoring for the Managed Server environment.

Managed Hosted Server Services is available in four variants:

- Windows Tier 1 (24x7 Support) Standard
- Linux Tier 1 (24x7 Support) Standard

Managed Server Services includes the following components:

- Service Desk and ITIL Support
- Operational Activities
- Security Management
- Virus Protection Management
- Virus Protection Management – Outbreak Management
- Software Distribution – Fixes & Patches
- Cluster Management – Single Data Center
- Server Decommissioning
- System Backup and Recovery
- Print Management

1.1.2 ITIL Process Delivery and Service Desk Support

Atos will provide our global ITIL-based process governance framework, branded as the Atos Service Management Methodology (ASMM). This methodology is designed using a combination of industry best practices and Atos' practical experience in delivering managed services in an enterprise environment. The services are delivered through an independent delivery organization; the US based Atos Service Management Center (SMC), which is dedicated to the process governance activities required to ensure the successful deployment and delivery of services in a managed outsourcing engagement. The SMC leads will define, document and maintain the

process flows, integration points and procedures necessary to support the mainframe services included in this contract. As shown in the following table the SMC will provide the following process level functionality in support of the mainframe services.

Process	SMC Responsibility
Incident Management	Responsible for managing lifecycle of all incidents. The SMC will monitor the process to ensure it is efficient and effective, identify trends, improve recovery time, and identify service improvements
Major Incident Management	Work to effectively and efficiently manage Major Incidents ensuring appropriate communication and swift resolution
Change Management	Manage IT changes and deliverables while managing risk. The SMC will manage changes related to the services and the change process including: Prioritize and categorize Authorize and schedule, implementation Review the implementation Participate in the CAB meetings Additionally, the SMC will ensure that standardized analysis, reviews and approval processes are followed, artifacts captured, and the appropriate audit focus given.
Problem Management	Responsible for managing the lifecycle of all problems. The SMC will identify needed corrective actions, create and manage action plans to resolve known errors, update the knowledge database, provide quality assurance (root cause analysis, actions identified and closed), and provide proactive problem analysis to identify trends
Request Fulfillment	Responsible for end-to-end management of the Service Request Lifecycle. The SMC will monitor the process to ensure it is efficient and effective, identify service improvements, provide management reporting and quality assurance (consistent delivery, manage backlog, information gathering)
Service Asset & Configuration Mgmt.	Provide and maintain information on Configuration Items required to deliver an IT service, including their relationships
Capacity Management	Responsible for ensuring that the capacity of the IT service meets the business requirements in a cost-effective, efficient, and timely manner
Knowledge Management	Responsible for working with the towers to ensure knowledge articles are developed and maintained with the internal and customer-specific knowledge
Process Service Manager	Contributes to overall service delivery improvement process strategy in collaboration with the AMO and other delivery lines

Atos will implement our Atos Technology Framework (ATF) including ITSM functionality and an extensive integrated toolset that serves as the foundation for Atos' service management services.

The underlying advanced autonomics, discovery, monitoring, and management tool sets are fully integrated within the platform and deliver alert information to automated processing correlation tools, which then trigger Atos ServiceNow for automated ticketing and direct routing to Atos support teams or automated resolution.

The Atos Service Desk will support the delivery of these ITIL process based services, taking calls for any needed changes or to report incidents and using ServiceNow will ensure that the processes described above are delivered effectively. Atos service desks take millions of calls per year and have experience across all sectors and services.

1.1.3 Managed Windows Server

Managed Windows Server:

- Applies to Servers running Microsoft workplace-related applications.
- Supports Windows Server 2016 and 2012 current version (N) and previous versions (N-1), and Service packs for all supported versions.
- Provides activities related to installation, configuration, and maintenance of hypervisor environments supporting virtualized Windows Servers.
- By default, the Supplier shall deploy Server instances virtualized, though may, at its option, deploy Servers physically.

The following Services are out-of-scope and are not part of the Managed Windows Server for Workplace:

- Special Server Hardware configurations and specific peripheral Equipment needed for specific Applications
- Cloud services
- First-line End User support by telephone
- Technical and functional management of the Applications running on top of the provided platform
- Services on delegation or project basis, such as technical consultancy

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 1 Managed Windows Server Responsibility Matrix

No.	Task	Supplier	Customer
1.	Provide a virtualized environment based on respective hypervisor tools.	X	
2.	Perform special backup functions.	X	
3.	Monitor and detect unexpected Hardware events.	X	
4.	Automatically monitor resource utilization against predefined thresholds.	X	
5.	Process error information of relevant Hardware manufacturers.	X	
6.	Notify Third Parties, when Incidents or Problems related to this Service require attention of a support vendor.	X	
7.	Perform management with performance tuning such as configuring the Hardware.	X	
8.	Perform operational activities such as regular housekeeping of the Servers.	X	

1.1.4 Managed Linux Server

Managed Linux Server supports Enterprise Linux, from Red Hat and Novell SUSE Linux Enterprise Server, current version (N) and the previous version (N-1), and Service packs for all the supported versions.

The Managed Linux Server is applicable for Servers running multi-discipline Applications.

The following are out-of-scope and are not part of Managed Linux Server:

- Special Server Hardware configurations and specific peripheral Equipment needed for specific Applications
- Cloud services
- First-line End User support by telephone
- Technical and functional management of the Applications running on top of the provided platform
- Services on delegation or project basis, such as technical consultancy

Managed Linux Server supports activities related to installation, configuration, and maintenance of hypervisor environments supporting virtualized Linux servers.

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 3 Managed Linux Server Responsibility Matrix

No.	Task	Supplier	Customer
1.	Provision of virtualized environment: ▶ Respective hypervisor tools ▶ Special backup functions ▶ Separate performance management and requires access to console facilities	X	
2.	Monitor and detect unexpected Hardware events.	X	
3.	Automatically monitor resource utilization against predefined thresholds.	X	
4.	Process error information of relevant Hardware manufacturers.	X	
5.	Notify Third Parties when Incidents or Problems related to this Service require attention of a support vendor.	X	
6.	Perform management with performance tuning such as configuring the Hardware.	X	
7.	Perform operational activities such as regular housekeeping of the Servers.	X	

1.1.5 Operational Activities

Operational activities address the administration, monitoring, maintenance, and support for the managed Server environment.

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 4 Operational Activities Responsibility Matrix

No.	Task	Supplier	Customer
1.	Monitor the managed Server management Infrastructure.	X	
2.	Monitor virtual and physical instances.	X	
3.	Via event management, detect unexpected Hardware events relating to memory, processors, disks, and Network.	X	
4.	Via event management, detect unexpected Operating System Software events.	X	
5.	Automatically monitor resource utilization such as disk, memory, and processor against predefined thresholds.	X	
6.	Review capacity for current utilization, maximum and available capacity.	X	
7.	Invoke overarching Capacity Management process when capacity thresholds are in jeopardy, at risk, underutilized or exceeded.	X	
8.	Where the Customer owns the Hardware, meet the costs of any additional capacity.		X
9.	Provide specialist support for Incidents that cannot be solved by a first-line support organization.	X	
10.	Manage the accounts that Supplier uses for the Operating System administration.	X	
11.	Create and manage accounts used by Services on the system.	X	
12.	Create and manage accounts used to administer such Services.	X	
13.	Create, manage, and remove temporary accounts for installation of Services.	X	
14.	At the Supplier's sole discretion, separate duties through its Delegation of Control models, which are based on the Supplier Security baselines.	X	
15.	Administer accounts and Application management accounts with relation to local server functions.	X	
16.	Agree to a rights and delegation model to confirm that admin rights are used correctly.	X	
17.	Agree to a rights and delegation model to confirm that admin rights are used correctly.		X
18.	Provide Customer-specific information (e.g., user accounts, passwords, account requirements).		X
19.	Schedule and perform regular housekeeping of the Servers.	X	
20.	Schedule and perform Server maintenance activities.	X	
21.	Schedule and control the correct functioning of the Servers.	X	
22.	Each day, check that the processes and automation are working as intended.	X	
23.	Coordinate Incident Management and monitoring related activities.	X	
24.	Update ticket status on applicable tickets.	X	
25.	Update work instructions.	X	
26.	Start, shut down, and re-start (scheduled and non-scheduled) Servers or Services/tasks and related Applications routinely, after a failure of the Operating System and for maintenance.	X	
27.	Coordinate recovery of Hardware/Software/Operating Systems to a known/consistent state after Failure.	X	
28.	Execute system commands on the console command line, such as commands needed to install patches, commands for Device information, check statuses.	X	
29.	Stop and start the Server, when instructed by the Application support owner, as part of an Application restart.	X	

No.	Task	Supplier	Customer
30.	Resolve Operating System-related incidents in the field between Operating System and Application, with the corresponding problem management activities.	X	
31.	Deliver Operating System support for the Application vendor.	X	
32.	Deliver support for the internal Storage under the Application data.	X	
33.	Work with Application-responsible personnel to determine that the Application is working correctly with the underlying Operating System and patches.	X	
34.	Distribute all patches in the Maintenance Windows defined in the 2.1.1 Service Levels section.	X	
35.	Before the Supplier can change the environment (Operating System or patches), provide authorized approval from Application-responsible people.		X
36.	Change the environment (Operating System or patches) following authorized approval from Application-responsible people.	X	
37.	As the Application owner, approve any changes to the Application environment.		X
38.	Change the Application environment based on approved changes from the Application owner.	X	
39.	Discuss and agree to a certain Operating System for the Application.	X	
40.	Discuss and agree to a certain Operating System for the Application.		X
41.	Discuss and agree to the resolution to events (Incidents) that are a combination of the Operating System or the Application.	X	
42.	Discuss and agree to the resolution to events (Incidents) that are a combination of the Operating System or the Application.		X
43.	Where the Customer manages the Application contract, the Customer is required to provide the Supplier with any necessary access to any Application manufacturer's support facilities required to perform the duties listed herein.		X
44.	Monitor and detect unexpected Hardware events.	X	
45.	Automatically monitor resource utilization against pre-defined thresholds.	X	
46.	Process Hardware manufacturers' error information.	X	
47.	Notify Third Parties when Incidents or Problems require support Supplier.	X	
48.	Provide performance tuning, such as configuring the Hardware.	X	

1.1.6 Security Management

Security management activities shall be performed within the scope of the managed Server Service to comply with the Supplier's Security standards.

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 5 Security Management Responsibility Matrix

No.	Task	Supplier	Customer
1.	Setup and Manage the Operating System environment, in accordance with the Supplier's baseline standards (a set of administrative Security guidelines that maintain a high level of Security at an organizational and technical level).	X	
2.	Automatically monitor Security settings.	X	

No.	Task	Supplier	Customer
3.	In the event of a Security setting deviation, notify the Supplier and the Customer's Security officers and take appropriate actions.	X	
4.	In the event of a Security setting deviation, notify the Supplier and the Customer's Security officers and take appropriate actions.		X
5.	Enforce a Security policy, such as password length, strength and duration, data protection, according to the Supplier's baselines.	X	
6.	Provide physical Security of the Hardware Infrastructure based on the Supplier's data center policies.	X	
7.	Request logical access to Infrastructure components for the Customer or on behalf of Third Parties for the purposes of Application-related incident resolution, Application Change implementation, or Application patching.		X
8.	For any access, adhere to the Supplier's Security Policy.		X
9.	Where a Security Incident exists, may be required to sanction unscheduled outages and authorize emergency changes.		X

1.1.7 Virus Protection Management

The virus protection management service shall confirm that the Operating System is protected against malware threats.

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 6 Virus Protection Management Responsibility Matrix

No.	Task	Supplier	Customer
1.	Use Supplier's endpoint protection Service to secure the Operating System.	X	
2.	Use pattern and heuristic technologies to provide traditional protection against malware.	X	
3.	Provide file reputation Services to detect malware.	X	
4.	Monitor the functioning of the servers' central components of the endpoint protection Service.	X	
5.	Notify the Supplier of all relevant and valid non-Microsoft Applications so that the Supplier can differentiate between acceptable configurations and viruses.		X
6.	Based on Customer-provided information of relevant and valid non-Microsoft applications, differentiate between acceptable configurations and viruses.	X	

1.1.8 Virus Protection Management – Outbreak Management

The virus protection management – outbreak management Service provides management of virus outbreaks. In the event a virus is not stopped by the endpoint protection Service, this Service shall manage the outbreak.

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 7 Virus Protection Management – Outbreak Management Responsibility Matrix

No.	Task	Supplier	Customer
1.	When there is a virus outbreak and there is a definition file, take appropriate actions to infected files/systems, such as ad hoc updates of the virus detection tool and virus definition file, and manual removal of malware.	X	
2.	As deemed appropriate solely by the Supplier, shut down the Server or Network as a preventive measure. If the time and situation allows, consult with the Customer.	X	
3.	Accept and support the necessary shut down of the Server or Network as a preventive measure.		X

1.1.9 Software Distribution — Fixes & Patches

The Software distribution — fixes & patches Service provides Software fix and patch Service based upon the respective vendor patch policy.

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 8 Software Distribution — Fixes & Patches Responsibility Matrix

No.	Task	Supplier	Customer
1.	Analyze respective vendor releases of new security or operating system patches. Implement as relevant in the Maintenance Window, defined in the 2.1.1 Service Levels section.	X	
2.	Analyze relevant patches from other Suppliers within the Supplier's Managed Server scope. Prepare for distribution and distribute in the Maintenance Window defined in the 2.1.1 Service Levels section to all instances of the corresponding Operating System version and release.	X	
3.	Define the order of patches to be implemented.	X	
4.	Inform the Customer which changes are executed at what time.	X	
5.	During the Maintenance Window defined in the 2.1.1 Service Levels section, reboot the Server when required.	X	
6.	Install Service packs when respective vendors regularly issue a Service pack.	X	
7.	Support the current and previous Service packs for all supported releases.	X	
8.	To maintain a secure environment, use Supplier-approved Tooling to monitor/report on the patches/Service packs status for the base Operating System.	X	
9.	Implement Tooling and policies for updating systems.	X	
10.	Analyze information for impact, deployment speed, sequence, and communication paths required.	X	
11.	Accept analysis of information for impact, deployment speed, sequence, and communication paths required.		X
12.	Deploy patches, hot fixes, and service packs during the Maintenance Window defined in the 2.1.1 Service Levels section.	X	
13.	Monitor the correct deployment of mandatory patch levels.	X	
14.	When present in Change Advisory Boards (CABs), approve Changes and sign off when completed.		X
15.	Where managing an application contract, provide the necessary information and access to the application manufacturers support facilities that affect the patching duties listed herein.		X

1.1.10 Cluster Management — Single Data Center

Microsoft clustering Service (MSCS) management provides high availability environment. A cluster is at least two Servers working together to provide the high availability. Applications running on the system must be cluster-aware on the respective cluster management Software.

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 9 Cluster Management – Single Data Center Responsibility Matrix

No.	Task	Supplier	Customer
1.	Manage the MSCS with optionally Microsoft certified external Storage or Hardware Network load balancing services for high availability in a Windows environment.	X	
2.	Manage the respective vendor cluster Software for high availability in a UNIX/Linux environment.	X	
3.	Check Changes for the effect on the cluster environment.	X	
4.	Prepare, communicate, plan, execute, and follow up on failover cluster tests.	X	
5.	Perform activities resulting from operating system Software distribution Changes, such as cluster Software updates.	X	
6.	Perform activities resulting from start and stop of cluster management Service.	X	
7.	Perform activities resulting from the addition of cluster monitoring.	X	
8.	Add/remove additional cluster nodes.	X	
9.	For existing clusters, conduct cluster installation assessment.	X	

1.1.11 Server Decommissioning

The Server decommissioning Service provides the removal of managed Servers that are no longer required in an environment.

The following Services are outside of the scope of this Service:

- Transport of Hardware to Customer or a Third Party, e.g. lease company
- Destruction of Hardware or Hardware components in an environmental friendly way
- Accounting for compliancy demands, e.g. erasing hard disks
- Final backup of data, safeguarding of application backup media for a longer period

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 10 Server Decommissioning Responsibility Matrix

No.	Task	Supplier	Customer
1.	When the Server is stopped, remove logical components of a physical or virtual Server.	X	
2.	Communicate to the Customer regarding stopping a Server or virtual Server and all its related items.	X	
3.	Remove the Server from administration.	X	
4.	Discontinue Hardware maintenance contract and inform owner.	X	
5.	In the event the Customer requests deletion of data, coordinate service with the disposal provider.	X	
6.	Dispose Supplier-owned Hardware, if not virtualized.	X	

No.	Task	Supplier	Customer
7.	Remove from monitoring systems and CMDB.	X	
8.	If required, specify that data destruction is necessary during Hardware disposal.		X

1.1.12 System Backup and Recovery

The system backup and recovery Service provides Operating System recovery in the event of a technical problem.

User and application data backup and recovery are included in this service, priced separately due to varying performance, sizing, and recovery requirements. Refer to pricing in Appendix B.

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 11 System Backup and Recovery Responsibility Matrix

No.	Task	Supplier	Customer
1.	Configure and verify routine Server operating system backups.	X	
2.	Define user and application data backup requirements.		X
3.	Configure and verify user and application data backups based on Customer requirements.	X	
4.	Restore the Operating System functionality, and user and application data as required, from backup media in the case of a system recovery.	X	
5.	Perform a scheduled check on the correctness of the backup procedures.	X	
6.	Perform tests when a procedure is changed.	X	
7.	Define backup and recovery schedule and review with the Customer.	X	
8.	Agree to the backup and recovery schedule.		X
9.	Provide central system backup and recovery.	X	
10.	Perform all local activities, such as tape handling and escort of Hardware maintenance engineers on the Customer's premises.		X

1.1.13 Print Management

The print management Service shall enable printing from an Application to a managed print queue by defining the relevant printer(s) in the Operating System, and making it available for configuring it in the Application. Print management shall be specific to the print queue and print drivers on the local Server.

The following features are not in the scope of the print management Service:

- End User Incidents that result in configuration Changes. For example, relocation of the printer without acknowledgement, change to printer
- Local printer hands-on activities
- Print Device Hardware issues
- Printer maintenance activities such as changing toner, adding paper
- Third-Party Applications, such as Adobe Output Manager
- Programming of printer drivers
- Printer installation/set-up

The Customer and the Supplier shall comply with the responsibilities, as set out in the following table.

Table 12 Print Management Responsibility Matrix

No.	Task	Supplier	Customer
1.	To print from an application to a (Network TCP/IP) printer, define the printer in the respective OS.	X	
2.	By default, restrict provisioning printer drivers by the Supplier to the respective OS-certified printer drivers only.	X	
3.	Assess and manage Application-specific printer drivers as a project.	X	
4.	In the event of a print Failure, identify if there is a local Operating System print related configuration issue.	X	
5.	Initiate change in the OS print management environment as standard Service Requests.	X	

2 Service levels and service requests

2.1 Managed Server Service Levels

2.1.1 Service and Support Availability

The following Service and Support Availability will be provided with this Service.

Table 13 Service and Support Availability

Element	Set 1 – Non-Critical	Set 2 – Productivity Supporting	Set 3 – Productivity Important	Set 4 – Business Critical
Service Availability	98.0 %	99.5 %	99.8 %	99.9 %
Hardware specifications	Offering I	Offering II	Offering III	Offering IV[1]
Service Availability Window 1, second line, (only Priority 1 incident support times shown here, all other support times are fixed) standard	5 days, 10 hours, 08:00 to 18:00, local time, on Business Days			
Service Availability Window 2, second line, (only Priority 1 incident support times shown here, all other support times are fixed) optional	Not applicable	7 days, 24 hours, all days		
Support Language	English			
Support Availability Window	5 days, 10 hours, 08:00 to 18:00, on Business Days			
Incident Handling Window – Priority 1	7 days, 24 hours, all days			
Incident Handling Window – Priorities 2, optional[2]	5 days, 9 hours, 08:30 to 17:30, on Business Days (optional for all offerings)			
Standard Change Handling Window	5 days, 10 hours, 08:00 to 18:00, on Business Days (standard for all offerings)			
Maintenance Window 1, standard [2]	5 days, 10 hours, 08:00 to 18:00, on Business Days			
Maintenance Window 2, optional 1	Not applicable	18:00 to 8:00, on Business Days, Next Day		
Maintenance Window 3, optional 2	Not applicable	Saturday 08:00 to Sunday 12:00		
Service continuity – Recovery Time Objective (RTO)	120 hours	48 hours	24 hours	2 hours

[1] Offering IV is only delivered when the cluster option is chosen.

[2] The Maintenance Window allows Supplier to install fixes, patches, and patch levels for the Operating System and associated Operating System tooling:

- Changes are executed to validate that the mentioned service availability can be reached and provided over time.
- It gives the possibility to execute planned Hardware maintenance.
- The Maintenance Window is not intended for Customer changes.

Maintenance is carried out in cooperation with the Customer and Application groups, as it mostly requires functionality to be shut down.

2.1.2 Standard Reports

The following Standard Reports will be provided with this Service.

Table 14 Standard Reports

Report Name	Description	Reporting Period
Managed Server Availability	Server availability (physical and virtual)	Monthly

3 Transition

3.1 General Principles

Supplier shall have the overall responsibility for completion of the Transition Program. Customer shall contribute by providing information, contributing to planning, and fulfilling its responsibilities as described in this SOW document. Supplier shall develop plans and manage the overall execution of the Transition. To achieve the principles defined herein, Customer and Supplier shall work in close cooperation with mutually written agreements (Project Definition).

3.2 Transition Approach

Supplier shall plan, manage, and implement the Transition Plan according to its methodology. Supplier Transition methodology, templates, and processes shall be used to execute and control the Transition Plan. The Transition methodology shall contain processes and procedures to manage the Transition Plan.

Supplier's Global Transition Management (GTM) is a methodology and set of tools that supports the technical and personnel-related aspects of outsourcing. GTM describes the processes and Projects required for managing the migration of Services and the transformation of the environment over time.

3.3 Transition and Transformation Program Overview

During the first 30 days of the Transition Project, Supplier shall complete a detailed, written Transition Plan. This baseline plan shall be mutually agreed by both parties and shall describe the tasks, schedules, milestones, Deliverables, and required acceptance criteria.

To the extent unforeseen factors have an adverse impact upon the completion of the milestones, the parties shall work together to make adjustments to the Transition Plan and requirements, and shall attempt to perform workarounds to achieve the dates or adjust the milestone targets as required. The parties shall work collaboratively to adjust the Transition Plan as required to mitigate unplanned Events negatively impacting the achievement or completion of the Transition Period.

3.4 Transition Activities

3.4.1 Pre-Transition Activities – Operational Readiness

Table 15 Pre-Transition Activities

	Activity
	Kickoff meeting
	Solution and data validation; Discovery
	Setting up and finalizing Transition Project Team (Customer and Supplier)
	Completion of Transition Plan
	Project Management and reporting
	Network connectivity and tooling implementation & configuration

	Initial Network and connectivity validation
	Knowledge transfer, update, and documentation of process and procedures

3.4.2 Transition Phases

Table 16 Transition Phases

	Activity
	End-to-end Network and connectivity testing
	System Assurance testing
	User Acceptance Testing and Pilot tests
	Go-Live and stabilization period

3.4.3 Transition Organization

Supplier shall have a program for Transition that shall be managed by the overall Program Director assigned by supplier. Supplier Program Director shall have overall responsibility for all tasks needed to migrate the in-scope Infrastructure environment from the Effective Date to the Transformation closure. Customer shall secure participation from its relevant Third Parties in the Transition Program and shall contribute with planning, managing, and fulfilling its responsibilities as set out in this SOW document.

3.4.4 Supplier Roles and Responsibilities

Supplier shall provide the main roles in the program, and shall comply with the responsibilities, as set out in the following table.

Table 17 Supplier Roles and Responsibilities

Role	Responsibilities
Supplier Transition Program Director	▶ Manages the Supplier Transition Program team to agreed Transition Plan (scope, time, cost, quality) ▶ Manages program issues, decisions, and risks, including escalation to Customer and Supplier sponsors ▶ Reports program progress, status, and forecast to defined governance bodies ▶ Manages scope Changes to the program ▶ Is the program's primary Supplier liaison to the Customer ▶ Provides access to the Customer and Supplier program sponsors ▶ Manages Supplier program staffing ▶ Establishes individual Projects that are properly planned, documented, and monitor progress against baseline through formal review ▶ Manages the governance of Changes within the programs and Projects ▶ Validates that the program and Projects conform to agreed standards ▶ Documents all Transformation Project completions in a close out report ▶ Is responsible to name the competencies required to fulfill the Transformation Deliverables where external support is required
Technical Project Lead(s)	▶ Provides design and technical leadership and guidance to produce Project Deliverables ▶ Tracks and escalates Project issues, decisions, and risks ▶ Reports Project progress, status, and forecast ▶ Captures and shares lessons learned ▶ Manages the delivery of agreed outcome, products, and artifacts, reporting Projects progress formally and as required

Role	Responsibilities
	▶ Defines the solution aligned to the program and business objectives, and defines Changes to the architecture for submission to the defined bodies ▶ Manages and governs the solution to verify the solution design, and effectively manages the governance of the solution baseline and solution Change management ▶ Supports the program director to deliver the program, establishes a clear documented baseline of the program, and manages process and governance under clear Change Management

3.4.5 Customer Roles and Responsibilities

Customer shall comply with the responsibilities as set out in the following table.

Table 18 Customer Roles and Responsibilities

Role	Responsibilities
Customer Transition Program Director (Single Point of Contact)	▶ Peer established to match the Supplier Transition Program Director ▶ Works and coordinates requirements of the Transition Services ▶ Manages program issues, decisions, and risks, including escalation to supplier program sponsors ▶ Provides access to the supplier program sponsors ▶ Coordinates the required inputs from technical, process, and administrative requirements
Subject-Matter Experts (SME)	▶ SMEs provide appropriate technical references on in-scope Services, such as Asset transfer, Third-Party contracts, procurement Service, and in-flight Projects

3.5 Communication

Customer and Supplier shall participate in communication activities for the purpose of Transition and transformation as set forth in the following table.

Table 19 Communications

Communication	Communication Subject	Medium	Frequency
Program status report by Supplier	▶ Overall Status Achievements ▶ Next Steps ▶ Critical Issues/Escalations ▶ Open Issues ▶ Timelines/Milestones ▶ Needed Decisions	Microsoft PowerPoint	Weekly
Transition Plan report by Supplier	▶ Timeline Base Plan/Current Plan ▶ Progress ▶ Achieved Milestones ▶ Delayed Milestones	Microsoft PowerPoint	Monthly

3.6 Transition Responsibilities

3.6.1 Transition Roles and Responsibilities

Customer and Supplier shall comply with the responsibilities as set out in the following table.

Table 20 Transition Responsibility Matrix

No.	Task	Supplier	Customer
1.	Plan the Transition Program.	X	
2.	Manage the Supplier Transition resources.	X	
3.	Manage the Supplier Production resources.	X	
4.	Develop a Communications Plan and processes.	X	
5.	Assess stakeholders and channels.		X
6.	Execute the Communication Plan.	X	
7.	Manage Customer Transition stakeholders.		X
8.	Provide in-flight Projects data.		X
9.	Assess in-flight Projects.	X	
10.	Implement Project Office.	X	
11.	Establish onsite office accommodations and facilities.		X
12.	Implement initial Service Levels as agreed in Section 2.1 of this SOW.	X	
13.	Implement initial Service Level reporting as agreed in Section 2.2 of this SOW.	X	
14.	Review Milestones achieved.	X	
15.	Conduct Operational readiness review.	X	
16.	Review Service commencement and stabilization of Service.	X	
17.	Conduct Go-Live and Service stabilization.	X	
18.	Set up Service Management.	X	
19.	Set up Interim process for Service Management if required.	X	
20.	Perform Test according to Test Concept.	X	
21.	Review Test results.		X
22.	Accept Test results.		X
23.	Perform Pilot according to Pilot Concept.	X	
24.	Accept Pilot results.		X
25.	Deploy Services and Processes.	X	
26.	Accept Services and Processes.		X
27.	Hand over to Steady State team.	X	X
28.	Conduct Project closure.	X	X

3.7 Customer Obligations

Supplier shall have overall responsibility for the Transition Program. In supporting the Program, Customer shall fulfill the following obligations:

- Customer will provide agreed information to support the development and delivery of the Transition Program in an accurate and timely manner.
- Customer will provide, free of charge, office space and ordinary/customary office Infrastructure as required during Transition, beginning on the Project start date.

- Customer will provide Customer personnel for the purposes of knowledge transfer until the Service Commencement Date of the respective Service according to the agreed detail Project plans.
- Customer will name pilot users for participation in the pilot stage and encourage pilot user participation according to agreed Project Plan.
- Customer will provide any existing documentation as available, such as a Service operation handbook, in electronic form within two (2) weeks of Transition start date.
- Customer will approve Transition Deliverables in a reasonable timeframe.

All Customer obligations and provisions will be provided by Customer promptly (or as otherwise agreed) free of charge and shall be of such quality as is reasonably necessary to enable Supplier to comply with the Transition Plan.

3.7.1 Knowledge Transfer

During Transition, Supplier shall develop a knowledge transfer plan that is a workstream within the Transition phase and will be tailored for the Customer to address the Transition of knowledge of the current environment and baseline the knowledgebase for Service delivery

Supplier will work with the Customer to clearly understand and define the knowledge elements that need to be transferred to deliver the Services and maintain Service continuity. These elements, once defined, will be documented into Supplier operating processes and procedures in support of the Customer so that the appropriate, Supplier steady-state personnel can be progressively trained in their use of such elements, provided they are constantly involved in the provisioning of Services.

3.7.1.1 Knowledge Transfer Process

Members of Supplier's Transition team will work with the Customer to clearly understand and define the knowledge elements that need to be transferred to provide for successful delivery of the Services. These elements, once defined, will be documented into Supplier's standard operating processes and procedures in support of the Customer so that the appropriate, Supplier steady-state individuals can be trained in their use.

Types of knowledge transfer include the following:

- **Knowledge Mining** – This would include knowledge exports from existing suppliers as well as documentation, policies, procedures, processes, and the identification of other knowledge collateral. The information is uploaded to a central repository on the Supplier site for the purpose of sharing across the transition team.
- **Knowledge Transfer** – The transfer process includes assessment activities that are managed through workshops and also includes a formal process to transfer work from existing operational resources to the Supplier through what is called our Work Transfer Process.
- **Knowledge Creation** – Following our assessment of the existing documentation, gaps in the knowledge repository will be identified, and documentation will be created so that all Customer processes and procedures are documented. Subject matter experts from the Customer and Supplier will be engaged to help develop any missing elements.

Customer and Supplier shall comply with the responsibilities as set out in the following table.

Table 21 Knowledge Transfer Responsibility Matrix

No.	Task	Supplier	Customer
1.	Identify knowledge areas and key expectations to be met.	X	
2.	Identify procedures and standards.	X	

No.	Task	Supplier	Customer
3.	Identify current experts and SMEs.		X
4.	Assess current knowledge.	X	
5.	Decide on the required Transition approach.	X	
6.	Create Transition Knowledge Transfer Plan.	X	
7.	Establish organizational setup.	X	
8.	Approve Transition Knowledge Transfer Plan.		X
9.	Gather information.	X	
10.	Identify gaps.	X	
11.	Create documentation.	X	
12.	Validate that all knowledge has been explained, understood, and handed over.	X	

3.7.2 Pilot Testing

The entire solution shall be piloted in a full life environment with selected pilot users.

Customer and Supplier shall comply with the responsibilities as set out in the following table.

Table 22 Pilot Responsibility Matrix

No.	Task	Supplier	Customer
1.	Define pilot concept.	X	
2.	Define number of pilot users.	X	
3.	Define pilot use cases.		X
4.	Define pilot acceptance criteria.		X
5.	Execute pilot test(s).	X	
6.	Document pilot test results.	X	
7.	Pilot acceptance and declaration of readiness.		X

Customer and Supplier shall apply the following acceptance criteria:

No.	Deliverable	Acceptance Criteria
1.	Pilot use cases successfully executed	All pilot use cases are executed in the defined quantity and the defined thresholds are met.

3.7.3 Deployment of Service Management and Services

After the pilot passes, the implementation phase shall commence.

Customer and Supplier shall comply with the responsibilities as set out in the following table.

Table 23 Deployment Responsibility Matrix

No.	Task	Supplier	Customer
1.	Deploy Service Management and Services according to Transition Plan.	X	
2.	Define interim acceptance points/quantities per Service.	X	
3.	Review and approve acceptance points/quantities per Service.		x
4.	Accept services as deployed according to solution design.		X
5.	Support the Deployment as agreed.		X

Customer and Supplier shall apply the following acceptance criteria in defining the Program preparation tasks.

Table 24 Deployment Acceptance Criteria

No.	Deliverable	Acceptance Criteria
1.	Interim Acceptance points	As agreed interim acceptance points have to be performed. These can be according to sites, user groups etc. completed
2.	Final acceptance	Deployment is completed

3.7.4 Handover

After deployment is completed, both parties will hand over responsibility for service management to the line organization.

Customer and Supplier shall comply with the responsibilities as set out in the following table.

Table 25 Handover Responsibility Matrix

No.	Task	Supplier	Customer
1.	Handover final Supplier service responsibility to steady state organization – Supplier Account Management and Service Delivery Management.	X	
2.	Declare Supplier internal handover complete.	X	
3.	Handover final Customer service responsibility to steady state organization.		X
4.	Provide Customer acceptance for Handover.		X

Customer and Supplier shall apply the following acceptance criteria:

Table 26 Handover Acceptance Criteria

No.	Deliverable	Acceptance Criteria
1.	Handover acceptance report	The completion of the project including handover to the line organization is accepted by Customer

4 Appendix A: Volumes and Assumptions

4.1 Minimum volumes

The following table lists the Managed Hosted Server minimum volumes required to obtain the published pricing. Deviations from this requirement can be reviewed and agreed to on a case by case basis.

Table 27 - Minimum Volumes

Quantity	Resource Unit
100	Windows Tier 1 (24x7 Support) Standard
N/A	Linux Tier 1 (24x7 Support) Standard
N/A	Platinum Storage Allocated (GB)
N/A	Gold Storage Allocated (GB)
N/A	Silver Storage Allocated (GB)
N/A/	User and Application Data Backup Retained (GB)

4.2 Assumptions

- All services are Atos standard SSR's and SLA's
- US only labor resources required with commercially accepted employment verification/screening/background checks
- Atos ATF2 Service Now is the IT Service Management Platform (ITIL Processes)
- Services provided to a single Agency consolidating IT Service Management practices
- Engagement must be Full-Service with OS management - not just hosting of hardware
- Agency requested compliance reports or audit documentation is T&M
- Server hardware and Operating System Levels at supported vendor version levels
- Agencies provide for Operating System Software/licensing, and hypervisor software/licensing
- Server hardware hosted at an Atos datacenter (Regulatory compliance is not required at Datacenter)
- Excludes migration costs for existing systems to Atos Datacenter
- Virus protection - McAfee software and virus definitions -- Excludes Endpoint Protection Services (EPS)