# Managed Services SOW

## SCOPE

The Managed Services consist of:

(a) **Transition Services.** As of the Managed Services SOW Effective Date, Contractor shall commence performing the Transition Services described in Exhibit B (Transition), in accordance with the Transition Plan to be developed and agreed to by the Parties pursuant to Exhibit B (Transition).

(b) **Base Services.** On the date of Transition completion pursuant to Exhibit B or such other date as the Parties may mutually agree following completion of the Transition (the "**Base Services Commencement Date**"), Contractor shall provide the Base Services in accordance with the roles and responsibilities matrices described in Exhibits C to K, and the Service Levels set forth in Exhibit M (Service Levels).

(c) **Termination Assistance Services.** Commencing at the earlier of (i) six (6) months prior to the expiration of this Managed Services SOW, or (ii) delivery of any notice of termination or non-renewal of this Managed Services SOW, and continuing until the effective date of expiration or earlier termination of this Managed Services SOW, Contractor, at Company's sole discretion, shall provide reasonable assistance and services to re-transition the Base Services to Company or its designee ("**Termination Assistance Services**"), as further described in Exhibit S (Termination Assistance Services)

# Application Managed Services (AMS)

## Service Description

### 1.1. Application Managed Services (AMS) Scope

- The AMS apply to the Supported Applications listed in Attachment C-1 that are categorized into the following 7 portfolios :
  - Customer and Metering
  - Field Operations
  - Finance, Corporate & HR Human Resources
  - Generation & Sustainability
  - Grid & Pipelines
  - Platform
  - Others
- Contractor shall prioritize the AMS based on the Service Levels defined in Exhibit M (Service Levels).
- The Minor Enhancements Hours Pool defined in Section 2.2.2 will apply across the above seven (7) portfolios for Company's three (3) Affiliates ("**OpCos**") in Pennsylvania ("**PA"**), Rhode Island (**"RI"**) and Kentucky (**"KY**"). Contractor shall provide a monthly report on the consumption of minor enhancements hours, in accordance with Exhibit Q (Governance).

### 1.2. Application Managed Services (AMS) Description

The AMS shall consist of the core Services described in the table below ("**Core Services**") to be performed in accordance with Section 3.

| Ref | Core Services | Core Services Description |
|---|---|---|
| **1.** | **L2 & L3 Support** | • Level 2 ("**L2"**) support shall consist of tracking, monitoring, and responding to requests or Incidents that do not require modification, configuration, or customization of the Supported Applications listed in Attachment C-1.<br>• Level 3 ("**L3**") support will consist of modifying, configuring, and customizing the Supported Applications listed Attachment C-1 to correct/fix faults (Break-fix)<br>• The L2 and L3 support activities will only be performed based on the Incident and Request tickets logged in Company's IT Service Management system, ServiceNow (**"Company ITSM Tool"**). |
| **2.** | **Problem Management** | • Resolve repetitive occurring Incidents that cause failure within the Supported Applications listed in Attachment C-1 including finding a permanent fix to prevent reoccurrence.<br>• Problem Management activities will be performed based on the Problem Managed Request tickets received from Company's ITSM Tool. |

| Ref | Core Services | Core Services Description |
|---|---|---|
| | | • Problem Management Request tickets must be logged in Company's ITSM Tool. |
| **3.** | **Monitoring (Applications, Batch, Interfaces)** | • Regularly monitor the Supported Applications listed in Attachment C-1, batch jobs and/or interface connections utilizing Company's existing monitoring systems for successful cycle completion.<br>• Respond and resolve failures by coordinating with Company's appropriate teams.<br>• All Alerts are logged into Company ITSM Tool as Incidents. |
| **4.** | **Ad-hoc reporting / queries** | • Ad-hoc simple reports requested by Users that require no modification, configuration, or customization of the Supported Applications listed in Attachment C-1 and up to a maximum of 8 hours of effort per ad-hoc report.<br>• Ad-hoc reports requiring more than 8 hours of effort will be part of the Minor Enhancements backlog and addressed as part of the Minor Enhancements Hours Pool.<br>• Ad-hoc reports requests shall be logged in Company ITSM Tool<br>• Ad-hoc reports as a category will be defined in the service catalog that will be created during ServiceNow implementation in parallel to Transition phase |
| **5.** | **Service Request** | • Service Request is an approved standard request from a User for information, advice, a standard change or for access to an IT Service (e.g., request to change a password or to provide standard access for a new User) as defined in the Service Catalog.<br>• Respond and resolve the Service Request<br>• Requests requiring more than 8 hours of effort will be part of Minor Enhancements backlog and addressed as part of the Minor Enhancements Hours Pool. |
| **6.** | **Vendor Coordination** | • Facilitate support for Incidents related to Company's third-party software or products vendors (**"Company Vendors"**).<br>• These Incidents will be logged by Contractor with Company Vendors for the Supported Applications (as identified in Attachment C-1) as Tickets. |
| **7.** | **Minor Enhancements** | • Minor enhancements consist of modifying any Supported Applications listed in Attachment C-1 in response to new or changing business requirements, up to a maximum of 40 hours of effort (**"Minor Enhancements"**) for each enhancement |

| Ref | Core Services | Core Services Description |
|---|---|---|
| | | • Minor Enhancements requiring more than 40 hours of effort will be considered as projects/major enhancements. |
| 8. | **Production Services** | • Production support consists of ongoing operation of the Supported Applications listed in Attachment C-1, including both cyclic and non-cyclic activities, allowing effective system maintenance. This will be tracked in Company ITSM tool.<br>• Monitoring events will be generated for any application or interface issues, batch failure<br>• Event monitoring systems are assumed to be Dynatrace-based auto-generated tickets that are quick fix tickets that do not take more than half hour to close. |

**Table 1 - Core Services**

## Roles and Responsibilities

The following responsibility matrix describes the roles and responsibilities of Contractor and Company for AMS.

| Ref | AMS Responsibility Matrix | Contractor | Company |
|---|---|---|---|
| **Break Fix – L2 & L3 Incident Support for Supported Applications listed in Attachment C-1** | | **Contractor** | **Company** |
| 1. | Capture, document, and assign Incident including categorization and priority from the Service Desk (Exhibit-I) | X | |
| 2. | Capture, document, and assign Incident with categorization and priority when contacted from email (ticket shall be captured) | X | |
| 3. | Reassign Tickets incorrectly routed to Contractor to the appropriate Company queue | X | |
| 4. | Validate Incident categorization and priority, including the upgrade and downgrade of Tickets, in accordance with Company's defined service management process | X | |
| 5. | Investigate Incident, Service Request, Problem Request, and Application Change Request. | X | |
| 6. | Make an initial determination of the potential resolution | X | |
| 7. | Analyze, develop solutions to resolve Incidents and update the relevant knowledge article (for e.g., technical specs etc.). Peer-review solutions where knowledge is available. | X | |
| 8. | Provide effort estimate for break-fix (L3) Tickets | X | |
| 9. | Test fixes in pre-production environment | X | |
| 10. | Test fixes in post-production environment | X | |
| 11. | User verification testing in post-production environment | | X |
| 12. | Validate and sign off solution developed for production changes | | X |
| 13. | Restore service operations (within scope) following an Incident post unit testing | X | |
| 14. | Coordinate with applicable Company Vendors to resolve Incidents | X | |
| 15. | Escalate to Company for resolution when not resolved in time or unsuccessful co-ordination | X | |

| Ref | AMS Responsibility Matrix | Contractor | Company |
|---|---|---|---|
| 16. | Resolve Incident as per process defined in Exhibit -I<br>Eg - five (5) business days have passed, and the Contractor has made at least three (3) attempts to contact the End-User during working hours without receiving a response from such End-User | X | |
| 17. | Raise support tickets that may require Company Vendors (such as SAP, Oracle, Microsoft, Infor, Intergraph, etc.) support for Incident resolution that are not in Contractor's control (including but not limited to issues like lack of communication from Users) | X | |
| 18. | Provide or, where Incident resolution is not in Contractor's control, coordinate the final resolution | X | |
| 19. | Monitor and communicate in-scope Incident status | X | |
| 20. | Provide workaround if required to resolve Incident | X | |
| 21. | If a workaround is required, test and deploy workaround | X | |
| 22. | If workaround is not successful, as required, escalate Incident to a Problem ticket for further support to remediate the root cause | X | |
| 23. | Perform root-cause analysis for P1 & P2 Incidents. Provide the analysis to Company | X | |
| 24. | Maintain current documentation (technical, functional specifications and testing documentation) for Supported Applications listed in Attachment C-1, to incorporate new changes coming through projects performed by Contractor | X | |
| 25. | Support current documentation (technical, functional specifications and testing documentation) for Supported Applications listed in Attachment C-1, to incorporate new changes coming through projects performed by Company | | X |
| 26. | Provide feedback to Company on issues or Problems that cause inefficiencies or impact the execution of the AMS | X | |
| 27. | Review and approve Contractor-proposed changes to improve execution of AMS | | X |
| 28. | Implement approved changes in Company-owned processes to improve execution of AMS | | X |

| Ref | AMS Responsibility Matrix | Contractor | Company |
|---|---|---|---|
| 29. | Implement approved changes in Contractor-owned process to improve execution of AMS | X | |
| 30. | Update tickets and documentation for Incidents. Existing documentation should be adjusted as applicable for clarifications and/or changes made. | X | |
| 31. | Create or update knowledge articles for new, repetitive tickets that need user training | X | |
| **Batch Monitoring** | | | |
| 32. | Monitor batch jobs for successful completion | X | |
| 33. | Resolve or fix the failed jobs and communicate to business as appropriate | X | |
| 34. | Schedule a new job or update schedule change to an existing job | X | |
| 35. | Raise Problem ticket for any repetitive job failures | X | |
| **Service Request** | | | |
| 36. | Raise or submit a Service Request | | X |
| 37. | Review Service Request and assign priority | X | |
| 38. | Fulfill the Service Request per documented procedure | X | |
| **Ad-hoc Reporting Requests** | | | |
| 39. | Submit a Service Request for ad-hoc report via helpdesk or Company ITSM Tool | | X |
| 40. | Review Service Request and provide effort estimate to Company if the effort exceeds eight (8) hours, in which case the Service Request will be addressed as part of the Minor Enhancements Hours Pool | X | |
| 41. | Prioritize the Service Request in the backlog queue if there is no sufficient capacity to service ad hoc reporting Service Requests | | X |
| 42. | Approve or reject the effort if necessary, to progress the reporting request | | X |
| 43. | Provide estimated completion date and share status of the Service Request | X | |
| **Service Management** | | | |

| Ref | AMS Responsibility Matrix | Contractor | Company |
|---|---|---|---|
| 44. | Company will provide Contractor's onshore and offshore team with access to Company's existing paging solution for Ticketing alerts | | X |
| 45. | Classify Incident into agreed categories, including determining Incident priority, and assign. | X | |
| 46. | Raise change ticket, update ticket with all relevant documentation, route for approvals and represent the change in change review meeting | X | |
| 47. | Participate and provide inputs in change review process as part of the Change Approval Board ("**CAB"**) | X | |
| 48. | Approve or reject the change ticket | | X |
| 49. | Coordinate with other Company's or Company Vendor's teams, as required, to deploy the change | X | |
| 50. | Communicate the status of the change, until closure | X | |
| 51. | Prepare Service Levels (CSLs/KPIs) performance reports and publish monthly as per Exhibit-Q | X | |
| 52. | Provide Company ITSM Tool | | X |
| 53. | Implement any configurations in Company ITSM Tool to enable data extraction for Service Levels (CSLs/KPIs) performance monthly reporting | X | |
| 54. | Approve any configurations in Company ITSM Tool for enabling the data extraction required for Service Levels (CSLs/KPIs) performance monthly reporting | | X |
| 55. | Approve access in Company ITSM Tool to enable data extraction for Service Levels (CSLs/KPIs) performance monthly reporting | | X |
| 56. | Investigate Problem and complete root cause analysis | X | |
| 57. | Provide support for root cause analysis activities that involve applications in scope | X | |
| 58. | Define the actions and resolution steps needed to resolve the Problem and estimate the effort, time, and cost to implement the resolution. | X | |
| 59. | Review and sign off Problem resolution | | X |

| Ref | AMS Responsibility Matrix | Contractor | Company |
|---|---|---|---|
| 60. | Perform actions to resolve Problem | X | |
| 61. | Approve or reject Problem resolution | | X |
| 62. | Plan and conduct training and User communication | | X |
| 63. | Support to training materials and User communication materials | X | |
| **Customer Updates** | | | |
| 64. | Review release notes published by product vendors, assess impact to Company environment and share assessment report to Company | X | |
| 65. | Identify relevant regression test scripts, execute, and capture test results | X | |
| 66. | Provide sign off regression test results | | X |
| 67. | Resolve open defects or provide work around by working with product vendors and Company Business as appropriate | X | |
| **Corrective Maintenance – Problem** | | | |
| 68. | Problem – Review, prioritize and provide resolution or work around | X | |
| 69. | Monitor and communicate status of the Problem ticket | X | |
| 70. | Update/maintain system documentation (technical specifications and testing documentation) addressing the Problem | X | |
| **Preventative Maintenance** | | | |
| 71. | Review, provide inputs and fulfill preventive maintenance Service Request | X | |
| 72. | Prepare preventive maintenance calendar that covers application patching | X | |
| 73. | Identify and assess application patches for the Supported Applications listed in Exhibit-C1 and notify the Company of their availability as appropriate. | X | |
| 74. | Manage patch management process as per Change Management Process | X | |
| 75. | Approve patches | | X |

| Ref | AMS Responsibility Matrix | Contractor | Company |
|---|---|---|---|
| 76. | Apply/execute approved application patches logged as Service Requests in Company ITSM Tool | X | |
| 77. | Troubleshoot and remediate failed patch deployments | X | |
| 78. | Provide remediation plan for the failed patches | X | |
| 79. | Review and approve remediation plan or risks which cannot be mitigated (e.g., legacy environment, technical debt, etc.) | | X |
| 80. | Provide list of identified exception(s) for patches recommended to be excluded and/or delayed | X | |
| 81. | Approve exception(s) for any patch updates that are requested to be excluded and/or delayed by the Company or Company third party(ies) | | X |
| 82. | Document exceptions to patching in Company risk register | X | |
| 83. | Regression testing post application patches logged as Service Requests in Company ITSM Tool before deployment | X | |
| 84. | Conduct user acceptance testing | | X |
| **Company Vendors Coordination** | | | |
| 85. | For unresolved Incidents where resolution that are not in Contractor's control (including but not limited to issues like lack of communication from Users), assign to Level 3 if support is needed from Company Vendors | X | |
| 86. | Share subscription details to raise support tickets with Company Vendors. | | X |
| 87. | Raise support tickets that may require Company Vendors support (such as SAP, Oracle, Microsoft, etc.). | X | |
| 88. | Coordinate to receive necessary support from applicable Company Vendor to facilitate closure of Incident | X | |
| 89. | Vendor Operation Level Agreement (**"OLA"**) management | | X |
| **Non-Ticketing activities / tasks** | | | |
| 90. | Monthly patching / maintenance – Pre and post-checkouts | X | |

| Ref | AMS Responsibility Matrix | Contractor | Company |
|---|---|---|---|
| 91. | Process ID remediations | X | |
| 92. | Batch monitoring / Job monitoring | X | |
| 93. | Reporting activities | X | |
| 94. | Weekly, monthly and quarterly meetings | X | |
| 95. | Daily health checks of Gold tiered Supported Applications identified in Attachment C-1 | X | |
| 96. | Support all deployments to be performed by Company's Dev Teams | X | |
| **Minor Enhancements** | | | |
| 97. | Document Minor Enhancement's requirements | X | |
| 98. | Estimate effort to implement each Minor Enhancement | X | |
| 99. | Review and approve Minor Enhancement and prioritize in the backlog queue | | X |
| 100. | Implement Minor Enhancement including design, development and testing | X | |
| 101. | Accept/sign-off Minor Enhancement testing | | X |
| 102. | Promote Minor Enhancement to production | X | |
| **Production Services Monitor Application** | | | |
| 103. | Provide all hardware, software licenses for the tools currently used by Company and obtain all consents/authorizations required for Contractor to use such items for the provision of the AMS. | | X |
| 104. | Provide access to existing Dynatrace application monitoring enabled for Supported Applications listed in Attachment C-1 | | X |
| 105. | Review Supported Application processing logs | X | |
| 106. | Identify Supported Application exceptions | X | |
| 107. | Analyze Supported Application exceptions | X | |
| **Production Services Report & Communicate Application Performance** | | | |
| 108. | Collect Supported Application performance data | X | |

| Ref | AMS Responsibility Matrix | Contractor | Company |
|---|---|---|---|
| 109. | Collect Supported Application utilization data | X | |
| 110. | Collect Supported Application exception data | X | |
| 111. | Collect Supported Application Accounting data | X | |
| 112. | Analyze Supported Application data | X | |
| 113. | Publish Supported Application performance report | X | |

**Table 6 – Roles and Responsibilities**

# IMS – Cloud and Datacenter - Database Management

## Service Description

### 1.1 Scope Overview & RUs Baseline

The in-scope Cloud and Datacenter & Database Management Services and associated Resource Units (**"RUs"**) Baseline are as set forth below.

| Service | Sub Service | Baseline RUs |
|---|---|---|
| **Cloud & Datacentre Services** | • Operating System (OS) Administration<br>• Operating System (OS) Patch Management<br>• Provisioning and Deprovisioning Server Instances<br>• Availability Management and Monitoring<br>• Capacity Management<br>• Cloud Network Management<br>• Cloud Platform Engineering<br>• Storage and Backup Management<br>• Disaster Recovery | On-premise in-scope infrastructure :<br>• ESX Hosts & Nutanix Acropolis AHV Hypervisor: 324<br>• Windows Server: 2562<br>• Red Hat Linux Server: 1072<br>• CentOS Linux Server: 94<br>• Other Linux Server: 117<br>• Debian GNU/Linux Server: 20<br>• FreeBSD Server: 13<br>• SUSE Linux Server: 73<br>• Ubuntu Server: 33<br>• VMWare Photon Server: 32<br>• Oracle Linux Server: 21<br>• HPUX Server: 15<br>• Acano Server: 1<br>• Unknown Server: 10<br>• Storage [TB]: 7500<br>• Backup [TB]: 2500<br>Cloud Infrastructure (Azure):<br>VM's: 129<br>Storage Accounts: 448<br>Azure Kubernetes: 12<br>Azure PaaS Services: 762 |
| **Database Administration Services** | • Database Management/Administration (DBA)<br>– | In-scope Databases and servers:<br>• SQL Instance: 400<br>• SQL Server: 83<br>• SQL Database: 2498<br>• SQL Database (Azure): 229<br>• Oracle Database: 573<br>• Postgres Server: 9<br>• Postgres Database: 29<br>• Cosmos Database: 23<br>• SQL Elastic Pools: 8 |

**Table 1 - Scope & RUs Baseline**

## 1.2 Data Center and Office Space Management

Contractor will not provide data center hands and feet support. Company will (i) provide full physical support and approval level support for access to data center and office space, and (ii) be responsible for any associated escort activities. Contractor will coordinate Company Vendor's hands and feet support for operational activities such as replacing hardware and will provide detailed configuration for parts that need to be replaced.

# Roles and Responsibilities

## Operating System (OS) Administration, Patching, Privileged Access, and Hypervisor Management

Table 3 sets forth the roles and responsibilities of Company and Contractor for the OS administration services for the technologies identified in Table 1 (Scope & RUs Baseline), under "Baseline RUs" for the OS technologies identified in Table 1 (Scope & RUs Baseline), under "Baseline RUs" (**"OS Administration Services"**).

| | OS Administration | Contractor | Company |
|---|---|---|---|
| 1. | Provide Contractor authorized access to Company's Azure cloud environments, including the necessary account credentials for Contractor to access Company's account with Azure. | | X |
| 2. | Request administrator level access for Contractor administrators | X | |
| 3. | Approve administrator level access requests | | X |
| 4. | Maintain approved administrator level remote access (i.e., local admins) | X | |
| 5. | Resolve Windows/Linux/HPUX OS related Incidents | X | |
| 6. | Manage servers in accordance with the established processes | X | |
| 7. | Manage containers and images | X | |
| 8. | Manage OS-level configuration changes | X | |
| 9. | Execute system recovery | X | |
| 10. | Perform server health checks as part of OS management and/or after Incident resolution, make recommendations where applicable based on health check results | X | |
| 11. | Review and approve health check recommendations and approve configuration change requests and/or project requests | | X |
| 12. | Implement the approved health check recommendations | X | |
| 13. | Monitor relevant server resources as part of OS management and/or after system startup | X | |
| 14. | Perform infrastructure startup/shut down procedures | X | |
| 15. | Approve infra-application start-up / shut down procedures for in-scope infrastructure | | X |
| 16. | Update Runbooks, "how-to" and troubleshooting procedures | X | |
| 17. | Coordinate with on-site support/hands and feet for Incidents and/or Service Requests requiring physical intervention (e.g., hard reboot, check lights, check cable, media/external drive swap, etc.) | X | |
| 18. | Coordinate with on-site support/hands and feet to resolve tickets and Service Requests which require on-site intervention including updating and closing-out Service Requests and Incidents in Company ITSM Tool | X | |
| 19. | Provide onsite support to resolve tickets and Service Requests that cannot be resolved remotely | | X |

| | OS Administration | Contractor | Company |
|---|---|---|---|
| 20. | Reboot in accordance with authorized request for change by the server and application owners | X | |
| 21. | Provide admin access on OS for approved administrators | X | |
| 22. | Adhere to Company-provided secure password storage guidelines | X | |
| 23. | Conduct a review of access in accordance with Company's User access review procedures | X | |
| 24. | Request least privilege access for Contractor Personnel in relation to their respective roles | X | |
| 25. | Grant approval to the Contractor for granting OS access | | X |
| 26. | Provide admin access on OS for Company-approved administrators | X | |
| 27. | Define the roll on/roll off process for Contractor's system admins | | X |
| 28. | Manage roll on/roll off support for system admins in accordance with Company-provided process | X | |
| 29. | Provide access control list report when requested by Company | X | |
| 30. | Coordinate remediation of Problem tickets with Company or Company Vendors | X | |
| 31. | Act as a point of escalation between Contractor and Company Vendors | | X |
| 32. | Report operational risks identified for Services in scope of Contractor as per Schedule Q | X | |
| 33. | Perform availability (device up/down) monitoring of servers in-scope | X | |
| 34. | For Contractor Supported Applications, Contractor applications support team to conduct application regression testing post OS patching within the agreed timelines | X | |
| 35. | For Company managed applications, Company application support team to conduct application regression testing post OS patching | | X |
| **Hypervisor Configuration and Support** | | | |
| 36. | Provide Level 2 and Level 3 Support as defined in Exhibit I, Section 2.1.5 | X | |
| 37. | Provide support for virtualization of Windows and Linux servers using hypervisor technology | X | |
| 38. | Configure and maintain high availability (HA) servers and hypervisors to support virtual servers and virtual machines | X | |
| 39. | Configure the virtualization environment using VMware best practices. | X | |
| 40. | Configure and maintain HA clusters for virtual servers and virtual machines. | X | |
| 41. | Identify, install, configure, and update Security Patches for VMware ESX hosts | X | |
| 42. | Install, configure, and test patches and updates for VMware ESX hosts. | X | |
| 43. | Allocate physical or virtualized storage to virtual machines. | X | |
| 44. | Configure and maintain virtual center or other hypervisor management software approved by Company. | X | |

| | OS Administration | Contractor | Company |
|---|---|---|---|
| 45. | Verify virtual machines are configured for in accordance with performance specification. | X | |
| 46. | Automate and perform manual or other virtual server provisioning as required to maintain availability and performance - subject to Company's design and architecture. | X | |
| 47. | Monitor and manage virtual to real hardware utilizations to avoid performance degradation, over allocation and any associated underutilization | X | |
| 48. | Setting up Policies, related to security, resource allocation, backup and recovery, monitoring, compliance/audit, and network configuration | | X |
| 49. | Procuring licenses for VMware products | | X |

**Table 3. OS Administration Roles and Responsibilities.**

## Operating System (OS) Patch Management

Contractor will review patches, identify the ones applicable to Company's environment and secure Company's approval for deploying them to remediate vulnerabilities for the OS technologies identified in Table 1 (Scope & RUs Baseline), under "Baseline RUs", in accordance with Company Change Management process ("**OS Patch Management Services**").

OS patches will be applied on a monthly cycle, inclusive of maintenance updates for the applicable OS, and backlog and exceptions identified after Services Commencement Date as scheduled with Company´s approval in accordance with the Change Management Process.

The following responsibility matrix sets forth the roles and responsibilities of Company and Contractor for the OS Patch Management Services.

| | OS Patch Management | Contractor | Company |
|---|---|---|---|
| 1. | Execute distribution of approved OS patches/security updates | X | |
| 2. | Conduct integration tests for OS patches with the affected standard OS image prior to distribution and submitting an impact analysis to Company | X | |
| 3. | Manage patch management process as per Change Management Process | X | |
| 4. | Troubleshoot and remediate failed patch deployments | X | |
| 5. | Manage and support Company's existing patch management tools and pre-built automation | X | |
| 6. | Approve group and role administration of Contractor support personnel | | X |
| 7. | Define secure password storage strategy | | X |
| 8. | Provide a plan to remediate vulnerabilities identified after the Services Commencement Date | X | |
| 9. | Propose remediation plan for vulnerabilities or risks which cannot be mitigated. | X | |
| 10. | Review and approve remediation plan or risks which cannot be mitigated (e.g.., legacy environment, technical debt, etc.) | | X |
| 11. | Conduct re-installation/recovery of infrastructure applications on servers for break-fix Incidents | X | |
| 12. | Support re-installation/recovery of applications software on servers for break-fix Incidents for Company's productivity applications in-scope of the Contractor (i.e., Microsoft 365) | X | |
| 13. | Perform OS vulnerability remediation for vulnerabilities identified after the Services Commencement Date | X | |
| 14. | Provide list of identified exception(s) for patches/security updates recommended to be excluded and/or delayed | X | |
| 15. | Approve security exception(s) for any patches/security updates that are requested to be excluded and/or delayed by the Company or Company third party(ies) | | X |
| 16. | Provide a test environment to Contractor with remote access enabled for Contractor support teams to access and test patches, backups and restores, tool configurations, integrations and other services necessary to support the Services. | | X |

**Table 4. OS Patch Management Roles and Responsibilities.**

## Provisioning and Deprovisioning Server Instances

Table 5 sets forth the roles and responsibilities of the Company and the Contractor related to provisioning and deprovisioning server instances for the OS technologies identified in Table 1 (Scope & RUs Baseline), under "Baseline RUs" ("**Provisioning and Deprovisioning Server Instances Services**").

For physical servers and/or network devices, Contractor will coordinate with Company's hands and feet support to provision/deprovision the hardware.

| Ref | Provisioning and Deprovisioning Server Instances | Contractor | Company |
|---|---|---|---|
| 1. | Raise Service Request for the provisioning and deprovisioning of VM server instances in non-production and production environments | | X |
| 2. | Approve Service Request for provisioning and deprovisioning of VM instances | | X |
| 3. | Perform provisioning and deprovisioning of VM server instances in non-production and production environments | X | |
| 4. | Provide existing VM templates | | X |
| 5. | Maintain and manage VM templates or image pipelines as per Company's OS standards. | X | |
| 6. | Review images against NIST OS hardening standards and the Center for Internet Security (CIS) benchmark for Windows and Linux Operating Systems | X | |
| 7. | Update CMDB with the details of newly provisioned and de-provisioned server instances | X | |
| 8. | Enable/disable operational support for provisioned/deprovisioned for server instances | X | |
| 9. | Follow Company's decommissioning process to retire deprovisioned servers | X | |
| 10. | Manage security baseline and configurations for in-scope server | X | |
| 11. | Define standards and policies for the server hardening template for new workloads | | X |
| 12. | Manage server hardening template as per Company's defined standards | X | |
| 13. | Apply server hardening on new or existing workloads | X | |
| 14. | Perform OS image operational readiness test (ORT) | X | |
| 15. | Coordinate with application groups for user acceptance testing (UAT) | X | |
| 16. | Test images in pre-production environment | X | |
| 17. | Test images in post-production environment | | X |
| 18. | Validate and sign off image and UAT | | X |
| 19. | Manage, review, and report on servers' compliance as per Schedule Q | X | |
| 20. | Review and approve audit compliance of patches and hardening | | X |

| Ref | Provisioning and Deprovisioning Server Instances | Contractor | Company |
|---|---|---|---|
| 21. | Provide a review of the audit data and sign off that servers are in compliance | X | |
| 22. | Collect and report audit data on Company's request as per Schedule Q | X | |

**Table 5. Provisioning and Deprovision VM Instances Roles and Responsibilities.**

## Availability Management and Monitoring

Table 6 sets forth the roles and responsibilities of Company and Contractor for the monitoring of virtual machine (VM) and physical server elements (such as processor, memory, etc.) and configuration of certain alerts to notify certain Users or User Groups when certain conditions are reached, for the technologies identified in Table 1 (Scope & RUs Baseline), under "Baseline RUs" ("**Availability Management and Monitoring Services**").

| Ref | Availability Management and Monitoring | Contractor | Company |
|---|---|---|---|
| 1. | Own overall event management process | X | |
| 2. | Monitor server and instances for events following the event management process | X | |
| 3. | Monitor storage subsystems for events, following the event management process | X | |
| 4. | Define standards and policies for the monitoring thresholds, parameters, rules, and response | | X |
| 5. | Implement and manage thresholds, parameters, rules, and response procedures based on Company-defined standards | X | |

**Table 6. Availability Management and Monitoring roles and responsibilities.**

## Capacity Management

Table 7 sets forth the roles and responsibilities of Company and Contractor for the capacity management services for the technologies identified in Table 1 (Scope & RUs Baseline), under "Baseline RUs" ("**Capacity Management Services**").

| Ref. | Capacity Management | Contractor | Company |
|---|---|---|---|
| 1. | Develop and provide a capacity plan based on Company's business performance requirements and forecast monthly | | X |
| 2. | Execute the capacity plan based on quarterly plan approved by the Company | X | |
| 3. | Recommend and clean up wasted capacity | X | |
| 4. | Report capacity as per Schedule Q to Company to provide capacity plan | X | |
| 5. | Monitor resource utilization (e.g., CPU, memory, disk space for VMs, storage systems and physical servers) | X | |
| 6. | Manage the resolution procedures for any threshold breaches for infrastructure resources | X | |

| Ref. | Capacity Management | Contractor | Company |
|---|---|---|---|
| 7. | Recommend additional capacity requirements based on actual resource utilization and agreed thresholds with the Company | X | |
| 8. | Provide hardware replacement through OEM or Company vendor | | X |
| 9. | Perform capacity procurement and provisioning to meet Company business and technical requirements on a timely basis | | X |
| 10. | Follow the escalation matrix defined in Exhibit Q if threshold breach is observed | X | |
| 11. | Analyze the Service Levels defined in Exhibit M (Service Levels) for achievability and provide recommendations for corrective action as needed | X | |
| 12. | Report performance as per Schedule Q against the Service Levels targets | X | |

**Table 7. Capacity Management Roles and Responsibilities.**

## Cloud Network Management

Table 8 sets forth the roles and responsibilities of Company and Contractor for the cloud network management services that consist of management of virtual networks, subnets, and network service groups in the cloud for Azure ("**Cloud Network Management Services**").

| Ref | Cloud Network Management | Contractor | Company |
|---|---|---|---|
| | **General Responsibilities** | | |
| 1. | Manage virtual networks (e.g., Vcenter Networks, , VPC, Route tables, etc.) | X | |
| 2. | Manage IP addresses (dynamic and static) | X | |
| 3. | Define network schema to use for cloud | | X |
| 4. | Domain Name Service (DNS) Management: Create, modify, delete, backup records in accordance with the business requirements | X | |
| 5. | Manage point to site configurations | X | |
| 6. | Manage network security groups | X | |
| 7. | Administer, manage, and troubleshoot network connectivity within the data centers and cloud tenants | X | |
| 8. | Coordinate with Company's third-party network circuit contractors on any connectivity issues | X | |
| 9. | Troubleshoot network issues with third parties (e.g., Azure) | X | |
| 10. | Act as escalation point between Contractor and Company's third-party network circuit contractors | | X |
| 11. | Provide onsite support to resolve tickets and Service Requests that cannot be resolved remotely | | X |
| **Dynamic Host Configuration Protocol (DHCP) Management** | | | |

| Ref | Cloud Network Management | Contractor | Company |
|---|---|---|---|
| 13. | Add, modify, and remove DHCP networks | X | |
| 14. | Configure and decommission DHCP servers | X | |
| 15. | Configure Bootstrap Protocol (BOOTP) relay agents | X | |
| 16. | Manage DHCP service options as per requirements | X | |
| **Azure Environment (General Responsibilities)** | | | |
| 17. | Manage route tables | X | |
| 18. | Manage Virtual Networks (VNETS) and subnets | X | |
| 19. | Manage VNET service endpoints | X | |
| 20. | Manage Virtual Private Network (VPN) gateways | X | |
| 21. | Manage ExpressRoute | X | |
| 22. | Troubleshoot networking issues | X | |
| 23. | Create or modify tagging as required | X | |
| 24. | Manage service availability/monitoring alerts | X | |
| 25. | Coordinate with Cloud Service Providers (“CSPs”) for support issues | X | |
| **VDI Platform Management and Administration (General Responsibilities)** | | | |
| 26. | Administer Virtual Desktop Infrastructure (VDI) platform Azure Virtual Desktop (AVD) solution | X | |
| 27. | Manage access to Company’s subscribed VDI platform services and systems | X | |
| 28. | Deploy patches to, update, and configure the VDI platform, in compliance to agreed patching schedule | X | |
| 29. | Monitor performance of the VDI Platform (Incident alerts, usage reports as per Schedule Q, etc.) | X | |
| **File Share Administration and Management (General Responsibilities)** | | | |
| 30. | Create, modify, control, restore, and delete backup jobs | X | |
| 31. | Manage file shares (i.e., provision, deprovision, backup, recovery, access control lists) | X | |
| 32. | Manage content hosted on infrastructure and cloud | X | |

**Table 8. Cloud Network Management roles and responsibilities.**

## Cloud Platform Engineering

Table 9 sets forth the roles and responsibilities of Company and Contractor for the cloud platform engineering services for Azure, consisting of support to maintain the design and architecture of the cloud infrastructure and services, and advanced troubleshooting (“**Cloud Platform Engineering Services**”).

| Ref | Cloud Platform Engineering – Environment Support | Contractor | Company |
|---|---|---|---|
| 1. | Provide cloud architecture design, build and support standards | | X |
| 2. | Maintain cloud architecture and design approved by the Company | X | |
| 3. | Raise requests for configuration changes to the Cloud environment | X | |
| 4. | Approve requests for configuration changes to the Cloud environment | | X |
| 5. | Modify cloud environments as per change requests or Service Requests | X | |
| 6. | Configure monitoring agents and define thresholds according to Company´s standards | X | |
| 7. | Update applicable cloud platform image, approval workflows, and service catalog | X | |
| 8. | Update documentation in accordance with the change management process for design and configuration | X | |
| 9. | Approve design and configuration documentation | | X |
| 10. | Update scripts/tools for server automation/auto scaling as needed | X | |
| 11. | Provide cloud architecture design, build and support standards | | X |
| 12. | Maintain cloud architecture and design approved by the Company | X | |
| 13. | Raise requests for configuration changes to the cloud environment | X | |
| 14. | Approve requests for configuration changes to the cloud environment | | X |
| 15. | Modify cloud environments as per change requests or Service Requests | X | |
| 16. | Configure monitoring agents and define thresholds according to Company´s standards | X | |

**Table 9. Cloud Platform Engineering – Environment Support Roles and Responsibilities.**

## Storage and Backup Management

Table 10 and Table 11 set forth the roles and responsibilities of Company and Contractor for backup monitoring and re-initiating the failed backups, simple file level restores, first level troubleshooting of failed backups, backup configuration, monitoring status of running backups, troubleshooting of backup errors in server backup tools for Dell EMC DataDomain and Pure Cohesity ("**Backup Management and Recovery Management Services**").

The core Services under Backup and Recovery Management Services are:

- Backup and restore management
- Archive administration

| | Backup and Recovery (Storage and Backup Management) | Contractor | Company |
|---|---|---|---|
| 1. | Define standards and policies for backup and restore | | X |
| 2. | Establish schedule, implement backup, and restore processes to maintain continued availability of business-critical data | X | |

| | Backup and Recovery (Storage and Backup Management) | Contractor | Company |
|---|---|---|---|
| 3. | Prepare operating system, databases and applications for backup agent installs | X | |
| 4. | Confirm the backup tool compatibility and the support from the tool's OEM | X | |
| 5. | Perform initial backup and restore test, for identified servers during initial build and Operational Readiness Test (ORT) | X | |
| 6. | Perform testing of restore as per agreed testing frequency | X | |
| 7. | Provide recommendations regarding backup and recovery procedures that can improve levels of protection, efficiencies, and cost reductions | X | |
| 8. | Perform backups on systems per schedule and implement Company retention policy | X | |
| 9. | Monitor backup/restore process | X | |
| 10. | Verify the backup/restore status and take appropriate action based on the status (success/fail) | X | |
| 11. | Upgrade the backup software to latest supported version on the backup servers and clients | X | |

**Table 10 Backup and Recovery Roles and Responsibilities.**

Table 11 sets forth the roles and responsibilities of Company and Contractor for the management and monitoring of datacenter storage, including managing snapshots and data replication across storage devices ("IMS In-Scope Hardware") ("**Storage Management Services**").

| | Storage Management (Storage and Backup Management) | Contractor | Company |
|---|---|---|---|
| 1. | Monitor availability, capacity, performance, and utilization of storage systems | X | |
| 2. | Provide storage forecasts leveraging baseline and trend analysis as per Schedule Q | X | |
| 3. | Provide storage requirements based on business application releases, new project requirements, and acquisitions | | X |
| 4. | Maintain storage space according to Company requirements and forecasts | X | |
| 5. | Create, edit, restore, delete snapshots | X | |
| 6. | Manage the Network Area Storage (NAS) Network | X | |
| 7. | Coordinate with hardware vendors for hardware related Problems or Incidents | X | |
| 8. | Manage escalations for hardware vendor Problems or Incidents | | X |
| 9. | Configure and execute replication between storage devices | X | |
| 10. | Perform firmware upgrades including upgrades of backup solution, patch backup agents and software | X | |

**Table 11. Storage Management Roles and Responsibilities.**

## Database Management/Database Administration (DBA)

Subject to any refinements and clarifications agreed during Transition, Table 12 sets forth the roles and responsibilities of Company and Contractor for the database management/database administration services for the databases identified in Table 1 (Scope & RUs Baseline), under "Baseline RUs" ("**Database Management/Database Administration Services**" or "**DBA Services"**).

| Ref | Database Administration and Database Management | Contractor | Company |
|---|---|---|---|
| **Database Administration** | | | |
| 1. | Maintain DB inventory and keep CMDB up to date | X | |
| 2. | Manage and maintain licenses | | X |
| 3. | Install database license(s) in adherence with Change Management Process | X | |
| 4. | Report license install using report from Company ITSM Tool as per Schedule Q | X | |
| 5. | Track licenses and consumption | | X |
| 6. | Report licenses, consumption, and compliance to stakeholders | | X |
| 7. | Manage and maintain database licenses and maintenance contracts | | X |
| 8. | Purchase licenses and vendor support for IT asset management tool | | X |
| 9. | Coordinate and escalate IT asset management tool related issues to Company platform vendor | | X |
| 10. | Execute license optimization plan (e.g., software removal, user cleanup, infrastructure consolidation, contract renegotiations, procurement) | | X |
| 11. | Establish control and governance protocols to manage software | | X |
| 12. | Respond to ad-hoc software licensing inquiries and requests from end users and stakeholders for the in-scope publishers | | X |
| 13. | Provide the approved software list | | X |
| 14. | Confirm with budget owner if renewal needed and license quantity | | X |
| 15. | Request software quote from reseller or software publisher | | X |
| 16. | Create purchase requisition and purchase order | | X |
| 17. | Document software renewal processes | | X |
| 18. | Maintain renewal transactions within the software asset management tool | | X |
| 19. | Log the life cycle of in scope assets (e.g., receipt, inventory, installation, maintenance to disposal) within the asset management tool | | X |
| 20. | Update the asset database and provide required information related to additions, Changes and decommissions of in scope assets | | X |
| 21. | Dispose of IT assets in a secure and safe manner and in alignment with existing Company IT asset disposal process | | X |

| Ref | Database Administration and Database Management | Contractor | Company |
|---|---|---|---|
| 22. | Define standards and policies for the asset details to be captured and updated in the asset database | | X |
| 23. | Manage asset database as per defined Company standards, policies, processes, and procedures | | X |
| 24. | Provide tool to perform the automated discovery of in scope assets | | X |
| 25. | Perform monthly validation of discovery data discovered from the discovery tool with existing asset inventory in asset management database and perform updates in the asset management database as required | | X |
| 26. | Provide monthly hardware inventory report as per Exhibit Q | X | |
| 27. | Share stock management reports with the asset team for quarterly inventory reconciliation | | X |
| 28. | Conduct quarterly inventory reconciliation using stock management reports | | X |
| 29. | Affix an asset identifier tag to the asset following Company's standards, policies, processes, and procedures | | X |
| 30. | Stock management – Company's site contact to provide up to date details of stock inventory when stock is added or removed | | X |
| 31. | Update asset details for assets in stock in the asset database | | X |
| 32. | Perform quarterly review of the hardware records in the CMDB | | X |
| 33. | Maintain stock levels and restock end user devices and peripherals at the Company locations | | X |
| 34. | Set up initial passwords/profiles for database administrators per Company defined standards | X | |
| 35. | Maintain and update runbooks | X | |
| 36. | Perform patching as per the patching schedule cadence after publishing the schedule calendar | X | |
| 37. | Get patching calendar approval from all the respective IT parties at the beginning of the year | X | |
| 38. | Work with Company to get approval on the patching calendar | X | |
| 39. | Manage life cycle of databases including data archival, purging (with Company approval) (e.g. creation of a new database, management of the database, decommission database, archival of data, purging data, return disk to disk pool (on premise)) | X | |
| 40. | Manage database replication | X | |
| **Performance Maintenance** | | | |
| 41. | Apply configuration changes (e.g., instance parameters) as requested and approved per Change Management process | X | |
| 42. | Clean up environment (e.g., log/trace file, purge, housekeeping) per Company's requirements — production environment only | X | |

| Ref | Database Administration and Database Management | Contractor | Company |
|---|---|---|---|
| 43. | Execute proactive database checklist (e.g., memory usage, database parameter configuration, database resources, input/output (I/O) distribution, etc.) per Company's requirement—production environment only | X | |
| 44. | Review optimizer parameters and suggest and make changes as necessary | X | |
| 45. | Approve reviewed parameters to make changes | | X |
| 46. | Monitor database plan deviations and enforce database plan management as needed | X | |
| 47. | Approve scheduled database startup/shutdown requirements | | X |
| 48. | Perform scheduled database startup/shutdown in accordance with Company requirements | X | |
| **Backup and Recovery for database** | | | |
| 49. | Define policies and standards for backup and recovery | | X |
| 50. | Implement backup processes/schedule and restore processes in alignment with Company requirements | X | |
| 51. | Export or import table/User data as needed to perform administrative functions | X | |
| 52. | Perform database backup/restore per Standard Operating Procedure (SOP) | X | |
| 53. | Monitor and manage database license concurrent usage limits | X | |
| 54. | Tag resources in cloud according to Company's tagging guidelines | X | |
| 55. | Optimize databases | X | |
| **Database Technical Monitoring and Reporting** | | | |
| 56. | Provide database metrics/indicators (e.g., availability, performance, operational, utilization) monthly | X | |
| 57. | Create and distribute monthly report as per Schedule Q on database performance and system utilization and capacity | X | |
| 58. | Monitor database processes and status (i.e., up/down) | X | |
| 59. | Monitor core database technical items (e.g., memory usage, database parameter configuration, database resources, I/O distribution, etc.) | X | |
| 60. | Perform table space, disk space, and temporary space management per requirements | X | |
| 61. | Perform database object structural management (e.g., tables, indices, etc.) per requirements | X | |
| 62. | Maintain physical database layout per requirements | X | |
| 63. | Monitor technical database patch releases from the vendors | X | |
| 64. | Apply and test applicable patch bundle in the test environment | X | |
| 65. | Perform evaluation of patch impact prior to deployment | X | |

| Ref | Database Administration and Database Management | Contractor | Company |
|---|---|---|---|
| 66. | Approve patch deployment to production environment | | X |
| 67. | Deploy patch in production environment, approved per Change Management Process | X | |
| 68. | Define patch and security policies as applicable to the database environment | | X |
| **Troubleshooting** | | | |
| 69. | Plan technical approach for applying required database fixes | X | |
| 70. | Apply technical corrections (i.e., bug fixes) provided by the database vendor as requested and approved per Change Management Process | X | |
| 71. | Coordinate the remediation of technical Incident tickets with the Company's database software vendors and drive to resolution | X | |
| 72. | Coordinate with the Company's database software vendors to support and drive resolution of Incidents | X | |
| 73. | Manage the Incident escalation with Company's database software vendor | | X |
| 74. | Approve communication to appropriate teams, groups, end users, and individuals through announcements or emails | | X |
| 75. | Perform standard execution of data refresh in lower environments as per change request | X | |
| 76. | Perform physical database Operational Readiness Testing (ORT), following completion of a major database event that would significantly impact Company's business | X | |
| **User Security and Compliance** | | | |
| 77. | Manage and maintain database admin password as per Company's policies | X | |
| 78. | Create database Users and provide appropriate privileges as per the requirements. | X | |
| 79. | Identify vulnerabilities on database/database servers. | X | |
| 80. | Approve deployment of vulnerability patches | | X |
| 81. | Deploy approved vulnerability patches per Change Management Process | X | |
| 82. | Remove vulnerabilities on database/database servers after getting fix from vendor | X | |
| 83. | Provide relevant evidence/artifacts to audit/compliance. | X | |
| **OEM Database Supplier Management** | | | |
| 84. | Maintain OEM support access and information (e.g., password to vendor website, contract numbers, etc.) | X | |
| 85. | Provide approval to administer provisioning in OEM support information (e.g., password to vendor website, contract numbers, etc.) | | X |
| 86. | Coordinate with OEMs to resolve technical database issues assigned to database vendors | X | |

| Ref | Database Administration and Database Management | Contractor | Company |
|---|---|---|---|
| **Engineering Support** | | | |
| 87. | Plan technical approach for applying required database fixes | X | |
| 88. | Apply technical corrections (i.e., bug fixes) provided by Company's database vendor | X | |
| 89. | Coordinate the remediation of escalated Incidents with the Company Vendors | X | |
| 90. | Escalate technical Incidents to the Company Vendors where needed | | X |
| 91. | Manage secure passwords as per Exhibit K | | X |
| 92. | Store database and admin passwords in a secure password storage tool provided by Company | X | |
| 93. | Review and document the replication configuration setup | X | |

**Table 12. Database Administration (DBA) Roles and Responsibilities.**

| Ref | Patch Management (Database) | Contractor | Company |
|---|---|---|---|
| 1. | Execute distribution of approved database patches/security updates | X | |
| 2. | Conduct tests for database patches prior deploying patches | X | |
| 3. | Manage patch management process as per Change Management Process | X | |
| 4. | Troubleshoot and remediate failed patch deployments | X | |
| 5. | Propose remediation plan for vulnerabilities or risks which cannot be mitigated. | X | |
| 6. | Review and approve remediation plan or risks which cannot be mitigated (e.g.., legacy environment, technical debt, etc.) | | X |
| 7. | Provide list of identified exception(s) for patches/security updates recommended to be excluded and/or delayed | X | |
| 8. | Approve security exception(s) for any patches/security updates that are requested to be excluded and/or delayed by the Company or Company third party(ies) | | X |
| 9. | Document exceptions to patching in Company risk register | X | |

**Table 13. Database Patch Management Roles and Responsibilities.**

## Disaster Recovery (DR)

Subject to any refinements and clarifications agreed during Transition, Table 14 sets forth the roles and responsibilities of Company and Contractor for the DR Services.

| Disaster Recovery | Contractor | Company |
|---|---|---|
| Participate in annual DR planning and tabletop exercises | X | |
| Approve the DR plan, design diagrams and related documents | | X |

**Table 14. Disaster Recovery Roles and Responsibilities**

# IMS – Network Data and Voice

## Scope of Services

The following scope of Services will be provided by Contractor, with support and participation from Company as detailed herein. Details regarding each Party's roles and responsibilities with respect to the below scope

| Service | Sub Service | Volumetric Assumptions* |
|---|---|---|
| Network Data | • 12*5 Network Data services supporting:<br>– Circuit Management<br>– Wide Area Network (WAN) and Local Area Network (LAN) routing and switching<br>– Load Balancers (physical and virtual)<br>– Wireless<br>• 24*7 Network Data monitoring | • Circuit Management: 0<br>• Routers: 866<br>• Switches: 2388<br>• Load Balancer: 75<br>• Cisco APIC (SDN): 15<br>• Wireless LAN Controller: 4<br>• Wireless Access Points: 1721<br>• Infoblox: 79 |
| Network Voice | • 12*5 Network Telephony services supporting PPL's voice technologies<br>• 24*7 Network Telephony monitoring | • Avaya servers: 60<br>• Avaya agents: 165<br>• CUCM/Unity/Express/Emergency Responder: 14<br>• Cisco Phones: 4642<br>• Cisco Call Center Express Agents: 166<br>• Cisco Analog Gateways: 174<br>• Cisco Video Rooms: 97<br>• Oracle Session Border Controller: 6<br>• Zoom Phones: 2843<br>• Zoom Video Rooms: 118<br>• Zoom Analog: 183<br>• Twilio Agents: 285 |

*Devices listed in this column are detailed in Exhibit U ("**IMS In-Scope Hardware**")

**Table 1**

## Summary of Key Services

A summary of the core services under the Network Services is as follows:

- Service operations using Information Technology Infrastructure Library (ITIL) processes
- Coordination for field services and Contractor related Incidents
- Capacity and configuration management for the devices identified in Table 1, under Volumetric Assumptions ("**Network Device(s)**")
- Network (data and voice) management:
  - Incident, Service Request, Change and Problem management
  - Infrastructure alert and events resolution
  - Infrastructure/platforms—operational administration, management, and maintenance
  - Patch management
  - Compliance management
  - Vulnerability remediation for vulnerabilities identified after the Commencement Date
  - Reporting (e.g. Utilization trends, Capacity, vulnerability remediation)
  - Monitoring of Network Devices
  - Contractor will provide L1.5 SOP based support for Zoom and Twillio systems. L2 and L3 support to be provided by respective OEMs.

Detailed in Table 3 are the Contractor and Company responsibilities for the Network Services.

| Ref | Description | Contractor | Company |
|---|---|---|---|
| 1. | Provide a test environment to Contractor with remote access enabled for Contractor support teams to access and test patches, backups and restores, tool configurations, integrations and other services necessary to support the Services. | | X |
| **Network Monitoring** | | | |
| 2. | Update existing and ongoing network documentation for logical network diagrams, circuit and interface mapping, IP addressing | X | |
| 3. | Update and maintain monitored Network Device list based on submitted changes (e.g., IP address, add/remove devices, add/remove interfaces, etc.) | X | |
| 4. | Enable access to Network Devices (e.g., SNMP agents, User accounts, port opening on firewalls, etc.) | X | |
| 5. | Load Network Devices into monitoring tools | X | |
| 6. | Validate discovered topology relationships and Network Device configuration against documentation | X | |
| 7. | Define and update monitoring requirements | X | |
| 8. | Review and approve monitoring requirements | | X |
| 9. | Monitor and detect availability and performance events for Network Devices | X | |
| 10. | Resolve network Incidents | X | |
| 11. | Perform third-party contractor management for all WAN services | | X |
| 12. | Provide/validate current infrastructure documentation | | X |
| 13. | Provide/validate current physical and logical network diagrams | | X |
| 14. | Provide/validate current circuit and interface mapping | | X |
| 15. | Maintain infrastructure documentation and diagrams | X | |
| 16. | Provide Network Device's business priority and service levels | | X |
| 17. | Provide IP addresses and SNMP read community strings | | X |
| Provide reports in accordance with Exhibit Q | | X | |
| **Network Administration** | | | |
| 18. | Process change/Service Requests for soft Moves, Adds, Changes, and Deletes (MACDs) as per Exhibit M (e.g.—enabling/disabling LAN ports, assigning VLANs, interface settings, etc.) | X | |
| 19. | Provide and manage access to Network Devices | X | |
| 20. | MACD routing tables and/or protocol prioritization | X | |

| | | | |
|---|---|---|---|
| 21. | Maintain agreed patch levels on equipment | X | |
| 22. | Review OEM patch releases and recommend level to maintain on equipment (within same version) | X | |
| 23. | Review patch release recommendations and approve | | X |
| 24. | Install approved patch releases as per Change Management process | X | |
| 25. | Troubleshoot and remediate failed patch deployments | X | |
| 26. | Propose remediation plan for vulnerabilities or risks which cannot be mitigated. | X | |
| 27. | Review and approve remediation plan for vulnerabilities or risks which cannot be mitigated (e.g., legacy environment, technical debt, etc.) | | X |
| 28. | Document exceptions to patching in Company risk register | X | |
| 29. | Provide list of identified exception(s) for patches/security updates recommended to be excluded and/or delayed | X | |
| 30. | Approve security exception(s) for any patches/security updates that are requested to be excluded and/or delayed by the Company or Company third party(ies) | | X |
| 31. | Maintain design of LAN including protocols and routing | X | |
| 32. | Manage IP ranges and Virtual Local Area Network (VLAN) numbers using global IP addressing scheme | X | |
| 33. | Support network protocols as per Company architecture standards and define access control lists for routers and switches | X | |
| 34. | Enable quality of service (QoS) configurations on routers as applicable | X | |
| 35. | Maintain the Network Devices and components within the CMDB | X | |
| 36. | Approve access to test environment | | X |
| 37. | Monitor and analyze network performance metrics of all Local Area Network (LAN) devices identified in Table , under “Volumetrics Assumptions”, including, but not limited to, routers, switches, wireless LAN controllers (WLCs), wireless access points (WAP), load balancers | X | |
| 38. | Manage Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP), and Internet Protocol (IP) address management and related tasks for Network Devices:<br>• Manage hardware (H/W) and Operating System (OS) for DHCP/NTP/IP address management servers<br>• Perform DHCP, IP address management and NTP related activities as per incident, change, or Service Request (SR)<br>• Monitor DHCP, IP address management and NTP services for network uptime | X | |
| 39. | Manage the WLC and Wi-Fi related backend platform identified in Table 1, under “Volumetrics Assumptions”:<br>• Add/modify/delete WAPs within the network as per SR<br>• Troubleshoot wi-fi related Incidents | X | |

| | | | |
|---|---|---|---|
| | • Monitor WAPs using management software | | |
| 40. | Manage performance tuning based requests and accelerations:<br>• Configure load balancers for optimal application delivery<br>• Maintain configuration of network cache environment to distribute content across network as designed<br>• Perform load balancing and load sharing related tasks as per Incident and change requirement<br>• Performance tuning | X | |
| **Operational Support** | | | |
| 41. | Provide accurate network documentation including designs, diagrams, and procedures | | X |
| 42. | Maintain network documentation including designs, diagrams, processes, and procedures | X | |
| 43. | Escalate Incidents as necessary based on pre-defined criteria—elapsed times, Incident priority, and complexity, to Original Equipment Manufacturer(s) (OEMs), Company, vendors, or third parties | X | |
| 44. | Coordinate and triage Incident response and resolution with WAN circuit provider as necessary | X | |
| 45. | Interface with and dispatch hardware maintenance providers for resolution of hardware/software issue | X | |
| 46. | Develop and maintain network hardware and software maintenance strategy | | X |
| 47. | Manage the network hardware and software maintenance strategy developed by Company | X | |
| 48. | Manage and maintain licenses and maintenance contracts | | X |
| 49. | Provide hardware replacement through OEM or Company vendor | | X |
| 50. | Update knowledge base with known errors/resolutions, technical documentation, and procedures | X | |
| 51. | Control access to Network Devices | X | |
| 52. | Log access to Network Devices | X | |
| **Configuration Management** | | | |
| 53. | Perform configuration management activities of Network Devices (e.g., routers, wireless access points, wireless controllers, load balancers and switches) by:<br>• Monitoring configuration changes<br>• Backing up configurations<br>• Restoring applicable Network Device configurations in a test environment<br>• Audit the configurations against the template at agreed frequency | X | |
| 54. | Investigate, reconcile, and escalate as appropriate auto-detected changes to network topology and configurations | X | |

| | | | |
|---|---|---|---|
| 55. | Provide configuration template | | X |
| **Capacity Management** | | | |
| 56. | Collect network bandwidth capacity statistics | X | |
| 57. | Analyze, track, and report on network capacity issues and solution recommendations | X | |
| 58. | Analyze capacity trends and generate executive-level findings as agreed | X | |
| 59. | Summarize capacity recommendations for annual IT planning process | X | |
| 60. | Propose network changes for optimal utilization | X | |
| 61. | Approve proposed network changes | | X |
| 62. | Make recommendations regarding bandwidth consumption and trends, particularly with regards to expansion of Company network | X | |
| **Release Management** | | | |
| 63. | Collect Network Device related hardware and software information | X | |
| 64. | Maintain and govern standard hardware and software levels within network infrastructure | X | |
| 65. | Analyze non-standard hardware and software within network and generate executive level finding | X | |
| 66. | Establish hardware refresh/upgrade strategy | | X |
| **Hands and Feet Support** | | | |
| 67. | Provide on-site persons for data centers, sites, and offices to provide for physical needs of environment (i.e., hard reboot, physical port tagging, check lights, check cable, etc.) | | X |
| 68. | Provide the hands and feet contact and escalation matrix for each location | | X |
| 69. | Update Configuration Management Database (CMDB) with hands and feet support and escalation matrix for each location and Configuration Item (CI) | | X |
| 70. | Maintain CMDB with hands and feet support and escalation matrix for each location and CI | X | |
| **Connectivity** | | | |
| 71. | Manage connectivity between the Company locations | | X |
| **Service Request Management** | | | |
| 72. | Provide and maintain a list of authorized personnel who can approve installs, moves, adds, changes (IMAC) | | X |
| 73. | Receive IMAC requests from authorized Users and validate the IMAC request for correctness and proper authorization | X | |
| 74. | Provide remote support for IMAC requests that cannot be resolved by the Level 1 Service Desk | X | |
| 75. | Provide onsite support for IMAC requests that cannot be resolved remotely | | X |

| | | | |
|---|---|---|---|
| 76. | Verify inventory for all hardware, software, parts, network, cabling, or any other component necessary to execute the IMAC is available | | X |
| 77. | Verify that services necessary to execute the IMAC are valid and available | | X |
| 78. | Verify that all hardware, software, parts, network, cabling, or any other services necessary to execute the IMAC will be available as of the date(s) scheduled for the IMAC | X | |
| 79. | Notify Company of inventory components that may need to be replenished | X | |
| 80. | Coordinate (setup meetings, provide list of material required to complete IMAC) and verify with Company that all hardware, software, parts, network, cabling, or any other services necessary to execute the job will be available as of the date(s) scheduled for the IMAC | X | |

**Table 3. Network roles and responsibilities.**

In Table 4 are the Contractor and Company responsibilities for the voice platform Services:

| Ref | Description | Contractor | Company |
|---|---|---|---|
| **Voice Management Platform** | | | |
| 1. | Manage voice management platform and associated endpoints:<br>• Maintain records of number-to-User mapping<br>• Maintain/manage voice systems identified in Table , under "Volumetric Assumptions"<br>• Perform daily health checks and routine maintenance to mitigate avoidable Incidents or outages. | X | |
| 2. | Create and/or update documentation as and when necessary | X | |
| 3. | Schedule OS/firmware patches as they are required/posted by the service | X | |
| 4. | Remediate vulnerabilities by applying patches released by Company's telephony solution provider. | X | |
| 5. | Maintain the document on the configuration standards | X | |
| 6. | Maintain Network Devices in the CMDB | X | |
| 7. | Plan a roadmap for telephony services | | X |
| 8. | Procure parts/licenses that are part of the telephony platforms | | X |
| 9. | Approve Service Requests | | X |
| 10. | Act as escalation point between Contractor and Company's Third-Party Contractors, when required | | X |
| 11. | Provide required licenses and support contracts with respective OEMs | | X |

**Table 4. Voice Platform Services roles and responsibilities.**

In Table 5 are the Contractor and Company responsibilities for the contact center platform Services:

| | Description | Contractor | Company |
|---|---|---|---|
| **Contact Center Platform Management** | | | |
| **General Responsibilities** | | | |
| 1. | Review and approve changes, configurations, maintenance plans, etc. | | X |
| 2. | Act as escalation point between Contractor and Company Third-Party Contractors during outages | | X |
| 3. | Procure parts/licenses that are part of the platform | | X |
| 4. | Contact center end-consumer support | | X |
| **Change Management** | | | |
| 5. | As required by Company guidance and lifecycle management, validate all infrastructure changes (upgrades, configuration, functional releases, bug fixes, Interactive Voice Response (IVR/) inbound/multi-channel routing rule changes, security patch updates etc.) are deployed in accordance with Company Change Management processes which includes expectations such as timely notifications, proper approvals, and complete testing | X | |
| 6. | Perform contact center maintenance, maintaining the design principles for the solution | X | |
| 7. | IP phones: Contractor will logically configure the phone for the agent (and handle issues with the logical configuration). Physical phone break/fix is out of scope | X | |
| 8. | In accordance with Company Change Management processes and procedures, conduct analysis of Network Device OS upgrades and implementation recommendations | X | |
| **Incident Management** | | | |
| 9. | Respond to reports of issues and outages from Company and take corrective action—adhering to all Company Incident management tools, processes, and procedures. | X | |
| 10. | Proactively resolve infrastructure and application Incidents detected via monitoring. | X | |
| 11. | Provide ongoing issue notification and updates to Company teams according to the MIM process | X | |
| 12. | Update and/or create content for knowledge management database based on resolution, to assist with future diagnosis/resolution | X | |
| 13. | As required, participate in Major Incident Management (MIM) process for critical Incidents in accordance with Exhibit I, Section 2.2 | X | |
| **Problem Management** | | | |
| 14. | Determine Incident root cause for agreed contact center infrastructure Incidents and provide root cause trending for agreed Incidents related to contact center infrastructure. | X | |
| 15. | Complete reviews of Problem reports and proactively identify issues requiring mitigation | X | |

| | Description | Contractor | Company |
|---|---|---|---|
| **Contact Center Platform Management** | | | |
| 16. | Analyze platform trend reports and proactively identify issues requiring mitigation and adhere to the Company Problem management processes and procedures | X | |
| **Configuration Management** | | | |
| 17. | Determine Incident root cause for agreed contact center platform application/Infrastructure Incidents and provide root cause trending for agreed Incidents related to contact center Infrastructure. | X | |
| 18. | Complete reviews of Problem reports and proactively identify issues requiring mitigation | X | |
| 19. | Analyze platform trend reports and proactively identify issues requiring mitigation and adhere to the Company Problem management processes and procedures | X | |
| **Continuous Improvement** | | | |
| 20. | Complete ongoing and regular contact center Infrastructure performance tuning | X | |
| 21. | Perform an annual end-to-end systems analysis and provide recommendations for Infrastructure improvements | X | |
| 22. | Review Incidents/Problems and recommend improvements | X | |
| **Monitoring** | | | |
| 23. | Resolve Incidents related to critical contact center components that are created by the monitoring tools | X | |
| 24. | Maintain logs in adherence with Company security standards, process, and procedures | X | |
| 25. | Conduct end-to-end monitoring of the system, set-up alerts on its components for availability and capacity | X | |
| 26. | Monitor critical infrastructure components and act upon alerts. | X | |
| 27. | Utilize Company standard or approved monitoring tools and procedures to identify, report, resolve, and escalate an issue | X | |
| 28. | Perform agreed solution health test and address Problems as they are identified | X | |
| 29. | Conduct daily contact center Infrastructure status check | X | |
| **Service Reporting** | | | |
| 30. | Provide service reports on an as agreed basis. Such reports should include, but are not limited to, availability, Incidents, Problems, and Changes., | X | |
| 31. | Prepare and conduct monthly operational reviews with Company to include, but not limited to, performance metrics, service level compliance, change history, root cause analysis, Incidents, and trending | X | |
| **Release Management** | | | |

| | Description | Contractor | Company |
|---|---|---|---|
| **Contact Center Platform Management** | | | |
| 32. | Adhere to all Company release management processes, procedures, and documentation requirements | X | |
| 33. | Complete post release validation testing | X | |
| 34. | Coordinate deployment of Infrastructure components | X | |
| 35. | Coordinate Infrastructure releases with client teams to validate impacts to other applications and testing are addressed. | X | |
| **Environment Management** | | | |
| 36. | Maintain contact center platform software levels across all environments, at Company's direction and/or based on vendor recommendations. | X | |

**Table 5. Contact Center Platform Services roles and responsibilities.**

# End User Management

## Service Description

The Parties are entering into this Exhibit F under which Contractor will manage Company's End User functions, as detailed below.

The following scope of Services will be provided by Contractor, with support and participation from Company as detailed herein. Details regarding each Party's roles and responsibilities with respect to the below scope:

| Service | Sub Service | Volumetric Assumptions |
|---|---|---|
| End User Management | 16*5 End User services supporting:<br>• VDI (VMWare Horizon)<br>• VDI (Azure Virtual Desktop)<br>• Mobile Device Management<br><br>9*5 End User services supporting:<br>• Windows Desktop<br>• Application Packaging | • VDI (VMWare Horizon): 2210<br>• Citrix VDI: 500<br>• Citrix Published Applications: 120<br>• VDI (Azure Virtual Desktop): 2263<br>• Mobile Device Management: 6972<br>• Windows Desktop: 9953<br>• MacBook: 100<br>• Application Packaging: 4 |

**Table 1**

Table 2 summarizes Contractor's coverage approach to End User Management Services.

| Services | Coverage |
|---|---|
| End User Management Services | 9X5 with on call for P1 and P2 |

**Table 2. Coverage of Unified Endpoint Management Services.**

# Roles and Responsibilities

## 1.1 End User Management Services

Table 2 describes Company and Contractor roles and responsibilities related to unified endpoint management.

| Ref | End User Management Services | Contractor | Company |
|---|---|---|---|
| **1.** | Provide a test environment to Contractor with remote access enabled for Contractor support teams to access and test patches, backups and restores, tool configurations, integrations and other services necessary to support the Services. | | **X** |
| **2.** | Provide 2 test devices for each OS variant of Mobile Device Management (MDM) | | **X** |
| **End User Management – Image Management** | | | |
| 3. | Raise and approve Service Requests for standard workstation image updates | | X |
| 4. | Update the imaging process to align with Company's choice of platform | X | |
| 5. | Receive approved Service Requests from authorized Company Personnel for standard workstation image updates | X | |
| 6. | Ensure that the updated image is tested and applicable to the target supported hardware models | X | |
| 7. | | | |
| 8. | Provide core applications and installation instructions required to be included in the standard workstation image updates for Company supported applications | | X |
| 9. | Provide core applications and installation instructions required to be included in the standard workstation image updates for applications in Contractor supported applications | X | |
| 10. | Maintain installation instructions for standard workstation image | X | |
| 11. | Confirm adequate licenses to cover all core applications used in the standard workstation image | | X |
| 12. | Provide report on license consumption in accordance with Exhibit Q | X | |
| 13. | Work closely with the Company to identify a set of mandatory security configurations and base productivity applications that are required in standard workstation image | X | |
| 14. | Conduct maintenance, updates, and integration testing for standard workstation image and its base software components including:<br>• Incorporating Microsoft feature updates<br>• Hardware driver, utility updates, and OEM suite updates | X | |

| Ref | End User Management Services | Contractor | Company |
|---|---|---|---|
| 15. | Provide onsite support for resolving issues that cannot be resolved remotely | | X |
| 16. | Provide an updated list of authorized application owners and test Users | | X |
| 17. | Deploy updated standard workstation image to authorized application owners and test Users for user acceptance testing<br>• Work with Company to ring-fence the UAT and/or roll-out of the update image | X | |
| 18. | Perform testing, including coordination with Contractor application support team, for approved Service Requests related to standard workstation image updates | X | |
| 19. | Approve Service Requests for standard workstation image updates | | X |
| 20. | Validate standard workstation image updates meet end user functionality requirements | | X |
| 21. | | | X |
| 22. | Establish lab and sandbox for testing purposes | | X |
| 23. | Certify updated standard workstation image for deployment through approved deployment processes | | X |
| 24. | Approve updated standard workstation image for deployment through approved deployment tool and IT Change Management processes | | X |
| 25. | Release updated standard workstation image for deployment through approved deployment processes<br>• Contractor shall adhere to Company's Change Management process to roll-out certified image | X | |
| 26. | Manage and maintain licenses and maintenance contracts | | X |
| 27. | Apply the hardware and software maintenance strategy regarding Change Management Process developed by Company | X | |
| **Endpoint Management – Patch Management** | | | |
| 28. | Monitor, identify, and review criticality of patches for supported operating systems | X | |
| 29. | Propose schedule for distribution of patches following IT Change Management processes (regular and zero-day patches) | X | |
| 30. | Review and approve schedule for distribution of patches following IT Change Management processes | | X |
| 31. | Provide an updated list of test Users | | X |
| 32. | Conduct patch testing on test machines with standard workstation image prior to distribution and submit an impact analysis to the Company | X | |

| Ref | End User Management Services | Contractor | Company |
|---|---|---|---|
| 33. | Deploy patches to authorized application owners and test Users for UAT | X | |
| 34. | Document exceptions to patching in Company risk register | X | |
| 35. | Validate patch update is successful through UAT or other method | | X |
| 36. | Conduct patch deployment distributions to production Users upon Company approval following IT Change Management processes | X | |
| 37. | Approve patch deployment risks | | X |
| 38. | Sign-off on UAT reports | | X |
| 39. | Conduct patch deployment distributions to production Users upon Company approval following IT Change Management processes | X | |
| 40. | Prepare and submit patching compliance report (normal and zero-day patches) within agreed timelines | X | |
| **Endpoint Management—Software Packaging** | | | |
| 41. | Identify the existing applications that are for packaging | | X |
| 42. | Provide repository of applications to be packaged and maintain the updated versions for in-house applications | | X |
| 43. | Provide the frequency of packaging per each application | | X |
| 44. | Maintain n-1 version of the packaged application | X | |
| 45. | Contractor shall identify and report to Company any standard application packages that are out of date and need to be updated | X | |
| 46. | Identify and report to Contractor any non-standard or custom application packages that are out of date and need to be updated for which Contractor is not providing Services | | X |
| 47. | Raise and approve Service Requests for new software packaging | | X |
| 48. | Raise Service Request for software packaging for updated identified by standard monitoring tools | X | |
| 49. | Receive approved Service Request(s) from authorized Company Personnel for software packaging | X | |
| 50. | Identify and provide application owner of the software to be packaged for Company supported applications | | X |
| 51. | Provide application owner of the software to be packaged for Contractor supported applications | X | |
| 52. | Create and document, in Company's ITSM, the mapping between End User Management application packages and the Company's service owner, including the location of the executable file and licenses | X | |
| 53. | Provide software installation instructions with the installer's location and license information for Company supported applications | | X |

| Ref | End User Management Services | Contractor | Company |
|---|---|---|---|
| 54. | Provide software installation instructions with the installer's location and license information for Contractor supported applications | X | |
| 55. | Confirm adequate licenses are secured for applications to be packaged | | X |
| 56. | Report on inadequate licenses using Company ITSM | X | |
| 57. | Provide report on number of application packages deployed monthly in accordance with Exhibit Q | X | |
| 58. | Provide a list of test users and target production users | | X |
| 59. | Create package and conduct integration tests | X | |
| 60. | Conduct package conflict detection and resolution as needed during the packaging process | X | |
| 61. | Conduct application package remediation for issues discovered during the packaging process | X | |
| 62. | Conduct peer reviews and release User acceptance tests | X | |
| 63. | Develop and maintain UAT scripts for Company supported applications | | X |
| 64. | Develop and maintain UAT scripts for Contractor Supported Applications | X | |
| 65. | Deploy software package for UAT with authorized application owner(s)/test Users | X | |
| 66. | Review UAT and approve requests for software packaging | | X |
| 67. | Create deployment package on software distribution tool for distribution through approved deployment processes | X | |
| 68. | Approve deployment package through approved deployment and IT Change Management processes | | X |
| 69. | Release deployment package to production through approved deployment processes | X | |
| 70. | Approve retiring older application versions | | X |
| 71. | Retire older application versions from the software distribution tool | X | |
| 72. | Maintain and update the application tracker | X | |
| **Endpoint Management—Software Distribution** | | | |
| 73. | Propose timing for package distributions based on the priority of the related Incident or Service Request | X | |
| 74. | Develop role-based or persona-based set of applications working closely with Company to deploy a set of standard tools automatically | X | |
| 75. | Review and approve package distribution timing | | X |

| Ref | End User Management Services | Contractor | Company |
|---|---|---|---|
| 76. | Schedule authorized packages for distribution | X | |
| 77. | Build and maintain systems collections for targeted package deployments | X | |
| 78. | Conduct deployment distributions and troubleshooting to standard supported devices upon receipt of client approval following IT Change Management processes | X | |
| 79. | Prepare and submit deployment report as per Exhibit Q | X | |
| **Device Management—Engineering Support** | | | |
| 80. | Qualify escalated Problem records as endpoint management tickets (e.g., global, systemic, or chronic issues for workstation software, or widespread and time-sensitive issues) | X | |
| 81. | Provide support for addressing and managing Problems associated with the standard workstation image and base software components | X | |
| 82. | Provide necessary operational support to maintain the existing EUM tools | X | |
| 83. | Coordinate the remediation of Problems for endpoint management tickets with the Company, or the Company Third-Party Contractors, for resolution | X | |
| 84. | Act as a point of escalation between Contractor and the Company's Third Party Contractors | | X |

**Table 2Unified Endpoint Management Roles and Responsibilities.**

Table 3 includes Company and Contractor roles and responsibilities related to device management.

| Ref | Error! Reference source not found.**Device Management Services** | Contractor | Company |
|---|---|---|---|
| **Device Management—Infrastructure Design for Mobile Devices and Workstations** | | | |
| 1. | Document, maintain, administer, and manage the mobile server infrastructure | X | |
| 2. | Document, maintain, and administer processes and procedures for provision and de-provision of mobile devices | X | |
| 3. | Document, maintain, administer, and manage infrastructure for mobile device upgrades | X | |
| 4. | Develop and design Company policies regarding devices and notify Contractor | | X |
| 5. | Document, maintain, configure, administer, and support policy enforcement of Company policies regarding devices | X | |
| **Device Management—Infrastructure Support** | | | |
| 6. | Provide operational support for device management | X | |
| 7. | Use IT service management (ITSM) process approved by the Company for all Incident, Problem, and Change Management as well as the related processes | X | |
| 8. | Work with Company Personnel to draft communication to announce planned activities or outages that affect Services | X | |
| 9. | Send communication to End Users related to planned activities, outages that will affect Services | | X |
| 10. | Implement and maintain Company policies across End User devices; Contractor shall adhere to the current governance process | X | |
| 11. | Configure infrastructure tools and platforms to deploy policies, compliance baselines, adhering to company standards | X | |
| 12. | Review and assess security vulnerability alerts relating to device security patches | X | |
| 13. | Review and approve vulnerability remediation plan presented by the Contractor | | X |
| 14. | Remediate vulnerabilities related to security patches approved by the Company | X | |
| 15. | Investigate alerts generated by application monitoring (e.g., CPU, memory, disk, network spikes, memory leaks, or business logic response is slow) | X | |
| 16. | Determine, establish, and carry out capacity management and performance monitoring | X | |
| 17. | Review and maintain User ID account management procedures; Contractor shall adhere to Company's existing process to manage User IDs | X | |
| 18. | Perform software upgrades, including the installation of service packs, patches, and hotfixes, and provide functional and system testing of patches and fixes before implementation – including internal and Commercial off-the-shelf software (COTS) tools. | X | |

| Ref | Error! Reference source not found.**Device Management Services** | Contractor | Company |
|---|---|---|---|
| 19. | COTS application shall undergo security assessment in accordance with the relevant Company policies and standards provided to the Contractor by Company | X | |
| 20. | Contribute to and review the scripts that Service Desk and deskside support teams use to carry out administration operations and troubleshooting; Contractor shall adhere to Company's existing process for reporting | X | |
| 21. | Communicate end-of-support dates and new product release information to Company | X | |
| 22. | Push software to devices | X | |
| 23. | Maintain/update enrollment procedure for end User mobile devices | X | |
| 24. | Conduct periodic reviews and updates of the run books, work instruction documentation, and operational procedures; Knowledge Management will be performed via ServiceNow | X | |

**Table 3 Enterprise Mobility Management Infrastructure Support Services Roles and Responsibilities**

# Messaging and Collaboration

## Service Description:

The following Services will be provided by Contractor, with support and participation from Company as detailed herein. Details regarding each Party's roles and responsibilities with respect to the below Services:

| Service | Sub Service | Volumetric Assumptions |
|---|---|---|
| Messaging and Collaboration | 9*5 Messaging and Collaboration services supporting:<br>• M365 (Exchange, Sharepoint, Onedrive, Teams)<br>• M365 Tenant administration<br>• M365 Exchange online support<br>• Exchange (on premise)<br>• Microsoft SharePoint administration and management<br>• Microsoft Teams support<br>• OneDrive support<br>• Group Policy Object Management | M365 Exchange users: 10650<br>M365 Sharepoint sites: 100<br>M365 Onedrive users: 6600<br>M365 Teams users: 6600<br>Microsoft Sharepoint (on premise): |

**Table 1**

Table 2 summarizes Contractor's coverage approach to Messaging and Collaboration Services.

| Services | Coverage |
|---|---|
| Messaging and Collaboration | 16X5 with on call for P1 and P2 Incidents |

**Table 2. Coverage of Messaging and Collaboration Services.**

# Roles and Responsibilities

Table 3 and **Error! Reference source not found.Error! Reference source not found.** describe Company and Contractor roles and responsibilities related to M365 Managed Services. Table 4 describes Company and Contractor roles and responsibilities related to on premise Microsoft Exchange.

| Ref | M365 Managed Services | Contractor | Company |
|---|---|---|---|
| **M365 Tenant Administration** | | | |
| **General** | | | |
| 1 | Company will have riginal Equipment Manu acturer ( EM) support agreement or in scope ervices | | X |
| 2 | Communicate new and upcoming M 65 eatures and unctionality | X | |
| 3 | Proactively evaluate new eatures with the Company or the betterment o the overall tenant operations or the End sers | X | |
| 4 | pprove enablement o new M 65 eatures and upgrades | | X |
| 5. | mplementation o M 65 eatures and upgrades | X | |
| 6. | dd and veri y domains | X | |
| 7 | Manage multi actor authentication or M 65 | X | |
| 8. | En orce password policies | X | |
| 9. | Manage security groups rom the M 65 admin center | X | |
| . | Manage admin roles | X | |
| . | pprove admin roles | | X |
| . | Provide erviceNow nowledge articles | X | |
| . | Manage object attributes visible in the M 65 administration portal | X | |
| . | esolve ncidents, ervice equests, Change requests, and address Problem tic ets in accordance with established processes, agreed Key Per ormance ndicators and ervice evels | X | |
| 5. | Monitor and trac M 65 service interruption | X | |
| 6. | Provide continuous improvement or governance in day to day operations | X | |
| . | Conduct reviews o and update the runboo s, nowledge base, and operational procedures | X | |
| 8. | Conduct enterprise wide ser communication | | X |
| 9. | Manage subscriptions and plans | | X |
| . | Troubleshoot recipient resolution ailures | X | |
| . | Troubleshoot shared older access | X | |
| . | Troubleshoot ree busy publishing | X | |

| Ref | M365 Managed Services | Contractor | Company |
|---|---|---|---|
| . | Troubleshoot message delivery | X | |
| . | Troubleshoot image attachment rendering | X | |
| 5. | Create modi y delete ser mailboxes | X | |
| 6. | Create modi y delete resource mailboxes | X | |
| . | Create modi y delete shared mailboxes | X | |
| 8. | Enable disable mailbox eatures | X | |
| 9. | Enable disable archive mailboxes | X | |
| . | Enable con igure mailbox orwarding | X | |
| . | estore ser mailboxes per Company's retention period | X | |
| . | Create modi y delete distribution groups | X | |
| . | Create modi y delete membership to distribution groups | X | |
| . | Manage ser mailbox permissions and delegations (send as, orwarding, send on behal ) | X | |
| 5. | Per orm email address changes | X | |
| 6. | Create modi y delete mail contacts | X | |
| . | Correct recipient in ormation in Global ccess ist (G ) | X | |
| 8. | Per orm ingle tem ecovery ( ) | X | |
| 9. | Manage ser level blac list whitelist | X | |
| . | Create mailbox size reports; Contractor shall review this with the Company per the current process | X | |
| . | Create mailbox quota reports; Contractor shall review this with the Company per the current process | X | |
| . | Manage service health reports and planned maintenance | X | |
| . | ssist with troubleshooting utloo connectivity issues | X | |
| . | ssist with troubleshooting Mobile ice apps connectivity issues | X | |
| 5. | ssist with troubleshooting utloo eb ccess connectivity issues | X | |
| 6. | ssist with troubleshooting P P connectivity issues | X | |
| . | ssist with and provide necessary M 65 Exchange con iguration o instant message access protocol ( M P) and simple mail trans er protocol ( MTP) connectivity issues | X | |
| 8. | ssist with troubleshooting ctive ync issues | X | |
| 9. | ssist with troubleshooting archive access | X | |

| Ref | M365 Managed Services | Contractor | Company |
|---|---|---|---|
| 5 . | Troubleshoot public older permissions | X | |
| 5 . | Troubleshoot public older creation | X | |
| 5 . | Create delete hosted domains; Company will review/reject/approve the changes proposed by the Contractor | | X |
| 5 . | Create delete hosted domains; Contractor shall test and execute change by ollowing Company's Change Management process | X | |
| 5 . | Create modi y delete remote domains; Company will review/reject/approve the changes proposed by the Contractor | | X |
| 55. | Create modi y delete remote domains; Contractor shall test and execute change by ollowing Company's Change Management process | X | |
| 56. | Create modi y delete accepted domains; Company will review/reject/approve the changes proposed by the Contractor | | X |
| 5 . | Create modi y delete accepted domains; Contractor shall test and execute change by ollowing Company's Change Management process | X | |
| 58. | Create modi y delete transport rules; Company will review/reject/approve the changes proposed by the Contractor | | X |
| 59. | Create modi y delete transport rules; Contractor shall test and execute change by ollowing Company's Change Management process | X | |
| 6 . | Troubleshoot object synchronization; Company will review/reject/approve the changes proposed by the Contractor | | X |
| 6 . | Troubleshoot object synchronization; Contractor shall test and execute change by ollowing Company's Change Management process | X | |
| 6 . | Create modi y delete ctive ync device policies; Company will review/reject/approve the changes proposed by the Contractor | | X |
| 6 . | Create modi y delete ctive ync device policies; Contractor shall test and execute change by ollowing Company's Change Management process | X | |
| 6 . | Create ctive ync devices reports; Company will review/reject/approve the changes proposed by the Contractor | | X |
| 65. | Create ctive ync devices reports; Contractor shall test and execute change by ollowing Company's Change Management process | X | |
| 66. | nvestigate mail low related issues or spam quarantine whitelist and blac listed mail | X | |
| 6 . | elease quarantine blac list spam mail | X | |
| 68. | Per orm Exchange nline policy con iguration | X | |
| 69. | Per orm Exchange nline connector con iguration | X | |
| . | Create Exchange nline report or mail low | X | |
| . | eview, approve, and sign o on policies lows | | X |

| Ref | M365 Managed Services | Contractor | Company |
|---|---|---|---|
| . | dd and remove sers in Exchange nline litigation hold pursuant to Company direction; Contractor shall work with Company stakeholders to execute these activities | X | |
| . | mplement archiving policies | X | |
| . | De ine legal hold policy | | X |
| 5. | Manage monitor legal hold pursuant to Company direction | X | |
| 6. | Troubleshoot eDiscovery search | X | |
| . | Modi y journal rules | X | |
| 8. | eview and approve guidelines or e Discovery, legal hold, journaling, audit, etc. | | X |
| 9. | En orce guidelines, as applicable to Contractor's ervices, or e Discovery, legal hold, journaling, audit, etc., that are provided by the Company | X | |
| 8 . | Create pdate harePoint sites as per requirements rom sta eholders ( 5 tic et a month) | X | |
| 8 . | ssign pdate oles and Permissions to harePoint sites as per requests rom sta eholders | X | |
| 8 . | Troubleshoot issues identi ied by sers | X | |
| 8 . | Create and share harePoint usage related training documents ( – times a year) | X | |
| 8 . | Create update delete site collection | X | |
| 85. | Create site collection usage reports | X | |
| 86. | ssign roles and permissions to manage term sets | X | |
| 8 . | Design and approve external sharing o harePoint nline environment | | X |
| 88. | Manage external sharing or harePoint nline environment | X | |
| 89. | et up n ormation ights Management ( M) in harePoint nline | X | |
| 9 . | pload and install orm templates | X | |
| 9 . | esolve issues with bloc ed ile types | X | |
| 9 . | Con igure usage analysis and processing | X | |
| 9 . | Con igure trusted ile locations | X | |
| 9 . | Manage harePoint recycle bin | X | |
| 95. | dd edit delete harePoint audiences | X | |
| 96. | eview and approve policies or records management, archival, sites quota, etc. | | X |
| 9 . | Troubleshoot organizational chart in personal pro ile | X | |

| Ref | M365 Managed Services | Contractor | Company |
|---|---|---|---|
| 98. | Troubleshoot application per ormance and unctionality issues | X | |
| 99. | Manage ser permissions to send email to channels | X | |
| . | Manage custom cloud storage | X | |
| . | Manage organization wide settings or messaging in Microso t Teams | X | |
| . | Create reports or Microso t Teams usage | X | |
| . | esolve permission related issues | X | |
| . | Manage account devices or ur ace Hubs and Microso t Teams ooms | X | |
| 5. | De ine retention policies and standards | | X |
| 6. | Manage retention policies and standards | X | |
| . | Create modi y delete retention policies | X | |
| 8. | Create modi y delete retention tags | X | |
| 9. | Per orm annual compliance review and assessment and provide report in accordance with Exhibit Q | X | |
| . | Manage account administration | X | |
| . | Manage integrated external apps | | X |
| . | et individual calls and meetings pre erences | | X |
| . | pprove organization wide license assignment | | X |
| . | Create sa e attachment policy | X | |
| 5. | De ine the policies or un nown malware in attachment (o , monitor, bloc , replace or dynamic delivery) | | X |
| 6. | Manage policies or un nown malware in attachment (o , monitor, bloc , replace or dynamic delivery) | X | |
| . | pply a e ttachment or recipients | X | |
| 8. | edirect attachment(s) when detected | X | |
| 9. | Create sa e lin policy | X | |
| . | dd s in sa e lin policy | X | |
| . | pply sa e lin or recipients | X | |
| 122. | Support integration with Company speci ied systems (e.g. racle HCM, racle People o t), n Prem, ctive Directory, Mail elay Forwarding, zure Entra ctive Directory ( D), Exterro (legal hold discovery application) | X | |
| . | Maintain on boarding o boarding scripts | X | |
| . | Modi y bloc ed s | X | |

| Ref | M365 Managed Services | Contractor | Company |
|---|---|---|---|
| 5. | Troubleshoot neDrive access issues | X | |
| 6. | Con igure secure sharing in accordance with Company policies and standards | X | |
| . | Enable neDrive pro iles in accordance with Company retention policies | X | |
| 8. | Coordinate ncidents raised via Microso t nline support premier support | X | |
| 9. | Monitor and trac ncidents raised to Microso t or M 65 issue a ecting the Company environment | X | |
| . | ssist with policy issues | X | |
| 131. | Act as a point of escalation between Contractor and Company Vendors | | X |
| . | Per orm vendor management | | X |

**Table 3. M365 Tenant Administration Roles and Responsibilities.**

| Ref | Exchange Managed Service | Contractor | Company |
|---|---|---|---|
| . | De ine hardware and con iguration architecture | | X |
| . | Manage server con iguration | X | |
| . | Manage accounts, permissions and roles | X | |
| . | Email policy management | X | |
| 5. | Manage retention policy as de ined by Company | X | |
| 6. | Monitor servers or per ormance and availability | X | |
| . | Provide onsite support to resolve tic ets and ervice equests that cannot be resolved remotely | | X |
| 8. | Manage patch management process as per Change Management Process | X | |
| 9. | Execute deployment of approved Exchange patches/security updates | X | |
| . | Conduct tests for Exchange patches/security updates prior deploying patches | X | |
| . | Troubleshoot and remediate ailed patch security updates deployments | X | |
| . | Propose remediation plan or vulnerabilities or ris s which cannot be mitigated. | X | |
| . | eview and approve remediation plan or ris s which cannot be mitigated (e.g., legacy environment, technical debt, etc.) | | X |
| . | Provide list o identi ied exception(s) or patches security updates recommended to be excluded and or delayed | X | |

| | | | |
|---|---|---|---|
| 5. | pprove security exception(s) or any patches security updates that are requested to be excluded and or delayed by the Company or Company third party(ies) | | X |
| 6. | Document exceptions to patching in Company ris register | X | |
| . | pprove updates and patches | | X |
| 8. | esolve ncidents related to Microso t Exchange | X | |
| 9. | Generate agreed reports as per Exhibit Q | X | |
| . | Monitor and trac ncidents raised to Microso t or Exchange issue a ecting the Company environment | X | |
| . | ssist with policy issues | X | |
| 22. | Act as a point of escalation between Contractor and Company Vendors | X | |
| . | Per orm vendor management | | X |
| 24. | Manage mailboxes on legal hold according to the Company's policy | X | |

**Table 4 Microsoft Exchange Administration Roles and Responsibilities**

# Service Description

The Cross-Functional Services consist of:

- Enterprise service desk,
- Service management, and
- Information Technology Service Management (ITSM) - Company's tool for ITSM is ServiceNow ("**Company ITSM Tool**"),

## 1.1 Enterprise Service Desk

### 1.1.1 Service Desk

Service Desk Services consist of coordinating and responding to Incidents, Problems, and Service Requests made by Company, and End Users, which may include Company Vendors.

Service Desk Services will be provided 24X7.

- Provide ownership of tickets and Service Requests in support of Company End Users and Service Recipients (e.g., logging, tracking, resolution, follow up, advocating on behalf of User, advising User of progress toward resolution, and reporting).

Incidents and Service Requests shall be resolved either by Contractor's Service Desk staff or, if necessary, will be referred/escalated for resolution.

The scope of services under Service Desk may be summarized as follows:

| Service | Sub Service | Volumetric Assumptions |
|---|---|---|
| Service Desk Services | • 24*7 Service Desk Services to Company as a central contact point for Company Users<br>• 24*7 Remote Technology Services (RTS) for Level 1.5 (as defined below) support to assist Company Users in remote resolution<br>• Company Users can reach the Service Desk via phone, chat, email, and a Web self-service-portal (over ServiceNow). | • 6600 IT Service desk tickets monthly<br>– 1980 Service Desk Email monthly<br>– 330 IT Service Desk Chats monthly<br>– 330 IT Service Desk Web monthly<br>– 3960 IT Service Desk voice calls monthly<br>• 1320 RTS tickets monthly |

### 1.1.2 Roles and Responsibilities

Table 1 sets forth the roles and responsibilities of Contractor and Company for the Service Desk Services.

| Service Desk: Service Operation Functions | Contractor | Company |
|---|---|---|
| Provide and maintain automated call distribution (ACD) capabilities for routing, handling, and reporting inbound and outbound telephone calls to and from the Service Desk. The ACD will be activated and comprehensively documented during Transition/mobilization phase, and comprise:<br>1. The device, firmware, and software components required to provide the ACD functionality.<br>2. The capability to review and design changes to the ACD call tree as required to meet changing business needs.<br>3. A customizable greeting to all callers.<br>4. A voice bulletin board feature that presents a customized voice message to all callers updating them on currently known outages and issues. This will be heard prior to the caller making a selection.<br>**5.** The ability to embed recorded messages at various positions within the call tree, including instructions for Incident self-reso ution (e.g., “to reset an active directory password, go to < >”). | X | |
| Review and approve changes to ACD and customized voice messages | | X |
| Provide Incident and Service Request support to the Company supported End-User base across the Company environment | X | |
| Ensure that ticket routing, resolver groups, and operational responsibilities are clearly defined and documented within the Incident Management and Service Request Management (IM-SRM) process | | X |
| Perform End-User password resets in compliance with Company security requirements. Inform Users about how to reset their passwords using the Company-provided ACD prompts, web portals, or chat channels. In cases where agents are unable to reset passwords, collaborate with other resolver(s), such as internal Company teams or Company Vendors teams, to:<br>• Adjust processes to enable service desk agent resets.<br>• Assist in implementing self-help procedures. | X | |

| Service Desk: Service Operation Functions | Contractor | Company |
|---|---|---|
| • Implement an alternative method of password resets that offers a similar experience to service desk agent resets.<br>• Incorporate authentication and secure communication measures into the documented process. | | |
| Verify license compliance prior to install and or reinstall | X | |
| Support phone, chat, email, portal, and Company enabled self-help options (and support new and emerging market technologies, as mutually agreed) for all End-Users to interact with Level 1 | X | |
| Provide support to self-help web portal, Frequently Asked Questions (FAQs), and knowledge management for proactive communication | X | |
| Manage ACD/voice response unit (VRU), queue balancing, resource planning, survey, and related operational systems | X | |
| Record service desk calls and interactions and retain them in accordance with Company policies related to record retention. | X | |
| Provide Company ITSM Tool licenses | | X |
| Provide Contractor with access to Company ITSM Tool to handle software requests. | | X |
| Provide process to request End-User software. | | X |
| Provide one (1) toll free number. Company owns/has responsibility for toll free solution. | | X |
| Provide toll-free/internal extensions for Company support and route to AWS Connect menu or a new AWS menu and structure if required. | | X |

**Table 1. Service Desk - Service Operation Functions Roles and Responsibilities**

Table 2 sets forth the roles and responsibilities of Contractor and Company for Service Desk self-help support.

| Service Desk: Self-Help Support | Contractor | Company |
|---|---|---|
| Define self-help support services requirements and policies | | X |
| Maintain/update self-help support Contractor procedures that adhere to Company policies (documentation developed during transition) | X | |
| Review and approve self-help support services procedures | | X |
| Assist service owners in publishing self-help solutions/articles in portal | X | |
| Monitor and review the effectiveness of self-help support services capabilities and usage and provide feedback with recommendations as per Exhibit Q | X | |
| Review self-help recommendations | | X |
| Maintain, document (textual and graphical as appropriate), promote, and provide support for self-service tools (e.g., password management) | X | |

| Service Desk: Self-Help Support | Contractor | Company |
|---|---|---|
| Provide Users with access to self-help tools for Problem resolution, such as FAQs and quick tips. Confirm that knowledge base articles are appropriately categorized into End-User facing and technical categories | X | |
| Develop and provide recommendations for improvements to self-help support services capabilities | X | |
| Review and approve recommendations for improvements to self-help support services capabilities | | X |
| Implement approved recommendations to enhance self-help support services capabilities. The implementation by the Service Desk will be limited to areas within its control and accessible resources. Certain recommendations may necessitate collaboration with other teams, such as the automation team or ServiceNow platform support team for portal enhancements, involving both Contractor and Company | X | |

**Table 2. Service Desk Self-Help Support Roles and Responsibilities**

Table 3 sets forth the roles and responsibilities of Contractor and Company for Service Desk Incident Management.

| Service Desk: Incident Management | Contractor | Company |
|---|---|---|
| Provide a single point of contact for Incidents and Service Requests responsible for:<br>• Logging and assigning a ticket number in Company ITSM Tool;<br>• Capturing the appropriate ticket;<br>• Provide operational support for all in-scope Services<br>• Maintain documentation of all supported items in the Service Desk knowledge base | X | |
| Provide operational support for all Service Desk related service catalog requests per a mutually agreed upon service catalog management process. | X | |
| Provide operational support for in-scope software, including operating systems, third-party software | X | |
| Resolve Incidents by the first agent contacted whenever possible | X | |
| Link multiple contacts pertaining to the same Incident to the associated Incident record<br>Document handling of parent-child tickets in the tool (i.e., which ticket to tag as parent, which properties are to be inherited by child tickets, etc.) | X | |
| Link multiple Incidents pertaining to the same Service Request to the associated Service Request<br>Document handling of parent-child tickets in the tool (i.e., which ticket to tag as parent, which properties are to be inherited by child tickets, etc.) | X | |
| Answer questions on use or features for all Managed Services related to standard hardware and software systems | X | |
| Transfer Incidents to the appropriate Level 2 support work queue when Level 2 support is required. Level 1 support Incidents transferred to Level 2 support will be monitored and reported. | X | |
| Manage all service queues for service desk | X | |

| Service Desk: Incident Management | Contractor | Company |
|---|---|---|
| Raise exemptions and exclusions for project-related impact on service desk performance for review | X | |
| Review exemptions/exclusions for project-related impact on service desk performance (e.g., tickets excluded from calculation) and resolve per Exhibit M | | X |
| Oversee and maintain responsibility of the monitoring, controlling and timely resolution of Incidents | X | |
| Escalate urgent and business critical or VIP Incidents in accordance with the policies and procedures manual | X | |
| Provide list of VIP Users and process for VIP Users to be signed off on by Company during Transition | | X |
| Resolve Incidents in Company ITSM Tool after confirming, communicating, and documenting resolution with End-User; confirm all contacts are logged and captured, including status inquiries for tickets and attempts to contact for ticket closure (including date/time, contact channel used, messages left) | X | |
| Escalate break/fix hardware support with Company Vendors and support groups | X | |
| Track and report the progress of resolution efforts and the status of Incidents:<br>• Review the proposed resolution time, for each occurrence exceeding the average<br>• Engage in efforts to continuously reduce the average effort time of Incidents; and<br>• Log each Incident and Service Request into Company ITSM Tool and assume ownership of assigning or escalating all Incidents and/or Service Requests that are not assigned to any other Company or Company Vendors support team; Service Desk to closely work with Company ITSM team regarding:<br>(a) streamlined process to prevent tickets from falling through the cracks, agree how to handle tickets with no takers<br>(b) alignment on the reporting scope: service desk to report only those created/handled by the desk (including those tickets service desk passed on to other teams); cross-functional reporting team to cover the holistic view (including tickets which were auto-routed to other teams and did not pass through Service Desk) | X | |
| Review reports and approve or decline recommendations | | X |
| Work directly in the Company ITSM Tool to document, track, and manage the Incident resolution processes | X | |
| Resolve tickets when:<br>• The underlying cause of the Incident has been repaired, or a temporary resolution has been implemented, or further troubleshooting activities have verified that the Incident has been resolved<br>• The End-User has confirmed resolution of the Incident, or five (5) business days have passed, and the Contractor has made at least three (3) attempts to contact the End-User during working hours without receiving a response from such End-User<br>• Normal operations have been restored<br>• Auto-ticket closure threshold: align with the ticketing tool team on the threshold before auto-ticket closure | X | |
| Close tickets that have been formally completed and documented as resolved by the End-User (auto-ticket closure will follow defined process) | X | |

| Service Desk: Incident Management | Contractor | Johnson Company |
|---|---|---|
| Upon receiving a Service Request, open a ticket and assign the Service Request to the appropriate resolver; coordinate the execution of the Service Request:<br>• Contacting the End-User to schedule an agreed time for the attempted resolution of the Service Request to occur;<br>• Routing the Service Request to the appropriate member or team (confirm that there is a catalog workflow on the ticketing tool to eliminate manual routing);<br>• Contacting End-User to verify that resolution of the Service Request occurred on schedule and that End-User is satisfied;<br>• Performing documented tasks for soft IMACs, when required; and<br>• Rescheduling the attempted resolution of a Service Request when necessary | X | |
| Provide reports to facilitate the closure of open IMAC Service Requests, and confirm these reports are accurately categorized and tagged as 'IMAC' in Company ITSM Tool for efficient tracking and reporting | X | |
| Manage all tickets logged into Company ITSM Tool, consisting of:<br>• Tracking all tickets from opening to closure;<br>• Monitoring the aging of all tickets, invoking any ticket escalation schemes based on processes developed during Transition;<br>• Confirming ticket entries in Company ITSM Tool include all troubleshooting and resolution data (including use of scripts and knowledge artifacts, and any print screens or attachments that would assist in understanding the issues or provide additional error information);<br>• Confirming documentation of resolution in Company ITSM Tool is sufficient to enable End-User to utilize the ticket record for self-help in the event of Incident recurrence;<br>• Confirming all contacts are logged and captured, including status inquiries for tickets and attempts to contact for ticket closure (including date/time, contact channel used, messages left);<br>• Upon resolution, validating with End-User that the Incident is resolved through email or other agreed-upon methods. Establishing a clear process for resolution validation, incorporating that five (5) business days have passed, and the Contractor has made at least three (3) attempts to contact the End-User during working hours without receiving a response from such End-User or scenarios where End-User does not respond. Confirming alignment on the methods and procedures for effective resolution validation; and<br>• Reporting individually and in aggregate on all ticket data and escalations | X | |
| Escalate open IMAC Service Requests that have exceeded timed thresholds, and implement an aging and inactivity escalation process that:<br>• Identifies classes or types of Incidents, and associated tickets, which will be escalated at specified ages or periods of inactivity based on Company guidelines;<br>• Includes tickets routed to all resolution entities, including Company, Company Vendors and other third-party support teams. Engaging with the Cross-Functional Services reporting team to include all aging or inactive requests, even those not processed through Service Desk (e.g., those processed via catalog workflow, self-service portal (SSP), etc.); and<br>• Establishes an escalation matrix to formalize escalation procedures. | X | |
| Provide status updates to End-User for open Service Requests and assist them in reviewing ticket status and historical tickets. Implement processes that allow End-Users to escalate Incidents when they believe (i) the correct priority level was not assigned, (ii) the Incident was not closed in a timely manner, or (iii) the issue was closed but not satisfactorily resolved | X | |

| Service Desk: Incident Management | Contractor | Company | |
|---|---|---|---|
| Confirm that status updates are appropriately recorded in the ticketing tool within an agreed-upon field, allowing Company's End-Users to view current ticket status through self-help options. | X | | |

**Table 3. Service Desk Incident Management Roles and Responsibilities**

Table 4 sets forth the roles and responsibilities of Contractor and Company for remote technology support.

| Service Desk Remote Technology Support: Tasks, Activities and Responsibilities | Contractor | Company |
|---|---|---|
| Define policies for the use of service desk remote control tools | | X |
| Maintain service desk remote device and software management services procedures | X | |
| Review and approve remote device and software management services procedures | | X |
| Resolve Incidents using remote-control capability and when possible, implement corrective actions; if resolution is not possible, escalate per the escalation procedures | X | |
| Utilize remote control tools to manage and update software, and to maintain configuration and inventory information | X | |
| Perform remote takeover of End-User devices following Company's remote ta eover policy | X | |
| Perform any required backup and restores procedures on End-User machine data / email in accordance with Company-provided guidelines | X | |
| Provide onsite support for Incidents that cannot be resolved remotely | | X |

**Table 4. Service Desk Remote Technology Support Roles and Responsibilities.**

Table 5 sets forth the roles and responsibilities of Contractor and Company for Software install/re-install support for Service Desk remote technology support.

| Service Desk Remote Technology Support: Software Install/Re-Install Support | Contractor | Company |
|---|---|---|
| Provide access to software repositories or libraries | | X |
| Provide list of authorized software for support and/or installation on approved devices | | X |
| Request from End-User the ability to take remote control over the device | X | |
| Accept or deny request by remote technician to take remote control over the device | | X |
| Provide remote support for authorized software related Incident(s) and Service Request(s) that cannot be resolved by Level 1 IT Service Desk support | X | |
| Approve access for remote support team to the software distribution tool | | X |
| Use the software distribution tool console to schedule installations on the User's device, as needed | X | |

| Service Desk Remote Technology Support: Software Install/Re-Install Support | Contractor | Company |
|---|---|---|
| In the event software must be replaced to conduct a repair, restore the environment to the previous state including configuration | X | |
| Define and provide standards and policies related to backup and restore procedures on end User devices | | X |
| Guide User on how to access, backup and restore data on end User device using OneDrive in accordance with the Company standards and policies | X | |
| Communicate ticket status to End-User for the tickets assigned to remote support team | X | |
| Confirm resolution with End-User and update ticket logs before setting ticket to resolved status | X | |
| Re-assign as needed, Incident(s) and request(s) to alternate resolver groups, including onsite support teams | X | |

**Table 5. Remote Technology Support: Software Install/Re-Install Support Roles and Responsibilities.**

Table 6 sets forth the roles and responsibilities of Contractor and Company for remote installations, moves, adds, and changes for single User Install, Move, Add, Changes (IMACs) as part of the Service Request process.

| Service Desk Remote Technology Support: Remote Installations, Moves, Adds and Changes (Single User IMACs As Part of Service Request Process) | Contractor | Company |
|---|---|---|
| Raise Service Request for remote IMACs | | X |
| Provide business approval for software installation Service Request (part of Service Request workflow approval process) | | X |
| Approve Service Requests where software license approval is required for software installation (part of Service Request workflow approval process) | | X |
| Request from End-User the ability to take remote control over the device | X | |
| Accept or deny request by remote technician to take remote control over the device | | X |
| Provide and maintain a list of authorized Company Personnel who can approve IMAC | | X |
| Receive IMAC requests from authorized Users and validate the IMAC request for correctness and proper authorization | X | |
| Provide remote support for IMAC requests that cannot be resolved by the Level 1 support | X | |
| Verify that software or any other services necessary to execute the IMAC will be available as of the date(s) scheduled for the IMAC | X | |
| Perform required back-up and/or restore procedures in accordance with Company standards and policies | X | |
| Un-install and re-install in-scope approved software or other related services as necessary to execute the IMAC | X | |
| Install software including new software in accordance with Change Management guidelines | X | |

| Service Desk Remote Technology Support: Remote Installations, Moves, Adds and Changes (Single User IMACs As Part of Service Request Process) | Contractor | Company |
|---|---|---|
| Guide Users on how to access, backup and restore data on end User device using OneDrive in accordance with Company standards and policies | X | |
| Set-up security, file access and other administrative procedures associated with the IMAC, in accordance with the agreed procedures | X | |
| Communicate IMAC ticket status to end Users | X | |
| Confirm resolution with an end User and update ticket logs before setting ticket to resolved status | X | |
| Re-assign as needed, Incident(s) and request(s) to alternate resolver groups, including onsite support teams | X | |

**Table 6. Service Desk Remote Technology Support. Remote Installations, Moves, Adds, and Changes for Single User IMACs Roles and Responsibilities.**

Table 7 sets forth the roles and responsibilities of Contractor and Company for device configuration and optimization.

| Service Desk Remote Technology Support: Device Configuration/Optimization Support | Contractor | Company |
|---|---|---|
| Request from End-User the ability to take remote control over the device | X | |
| Accept or deny request by remote technician to take remote control over the device | | X |
| Provide operations and support for device configuration issues/requests following the standard configuration guidelines | X | |
| Provide operations and support for new configurations and settings as defined by the desktop management and endpoint management team | X | |
| Communicate ticket status to authorized Users | X | |
| Confirm resolution with End-User and update ticket logs before setting ticket to resolved status | X | |
| Re-assign, as needed, Incident(s) and request(s) to alternate resolver groups, including onsite support teams | X | |

**Table 7. Service Desk Remote Technology Support for Device Configuration and Optimization Roles and Responsibilities.**

Table 8 sets forth the roles and responsibilities of Contractor and Company for continuous improvement.

| Continuous Improvement | Contractor | Company |
|---|---|---|
| Based on monitoring statistics and analysis, recommend improvement options | X | |
| Review and approve recommendations | | X |
| Provide monthly operational metrics based on Automatic Call Distribution (ACD)/ Interactive Voice Response (IVR) call volumes as per Exhibit Q | X | |

| Continuous Improvement | Contractor | Company |
|---|---|---|
| Perform reporting for call trends, top drivers, root cause, Service Levels specified in Exhibit M (Service Levels), etc., making recommendations to improve service as per Exhibit Q | X | |
| Set and achieve goals for continuous improvement of the Services via technology, process, or other changes | X | |
| Establish a service desk quality assurance program with metrics and a scoreboard to drive continuous improvement and review with Company monthly; align and calibrate the quality parameters used with those defined by the Company | X | |
| Maintain established Service Levels specified in Exhibit M (Service Levels) through performance of quality assurance evaluations conducted through call monitoring, call recording and ticket review of Service Desk analysts | X | |
| Perform service delivery oversight with Contractor, review service delivery reports and provide feedback on overall Service Desk Services | | X |
| Approve recommendations and update roadmap for funding of improvements | | X |
| Identify opportunities to improve the Level 1 and Level 1.5 capabilities for the Service Desk | X | |
| Develop and maintain all training documentation related to the Service Desk Services to be stored in Company-approved knowledge base | X | |
| Establish Service Level feedback process to allow for timely feedback to supervisors, agent evaluation, correction and, if required, training to prevent issues in support | X | |
| Conduct ongoing training and development for agents providing Service Desk Services, incorporating Company cultural and business operations awareness, as well as Service Desk feedback, consisting of:<br>• Conducting initial (i.e., onboarding) and annual training in accordance with Company-provided requirements;<br>• Coordinating with Company to obtain training materials specific to Company processes, technology, and Company Vendors and incorporate such training materials into the Service Desk annual training;<br>• Providing training programs for agents providing Service Desk Services that address the most frequent Incidents and Problems experienced by any part of the Service Desk to improve the overall services provided to Company;<br>• Promptly notifying Company upon discovering that the Service Desk is receiving calls concerning Company specific processes and technology for which Contractor has not conducted training for Service Desk personnel;<br>• Providing training as needed to address inadequate competencies that may be identified by either Contractor or Company (including through call monitoring or ticket review); and<br>• Providing, prior to the applicable introduction date, training to support changes in the Company environment that may result from the introduction of new projects / technologies | X | |
| Support self-help web portal, FAQs, and knowledge management for proactive communication | X | |
| Manage ACD/ Voice Response Unit (VRU), queue balancing, resource planning, survey, and related operational systems | X | |

| Continuous Improvement | Contractor | Company |
|---|---|---|
| Record service desk calls and interactions and retain them in accordance with Company policies related to record retention | X | |

**Table 8. Continuous Improvement Roles and Responsibilities**

## 1.2 Service Management

### 1.2.1 Continuous Service Improvement

Continuous improvement for service management, also known as CSI, is a core principle in the ITIL framework that focuses on constantly refining IT services to better align with business needs. It is a cycle of analyzing how things are currently done, identifying areas for improvement, implementing changes, and then measuring the effectiveness of those changes. Contractor will partner with Company to drive continuous service improvement across all in-scope Services.

### 1.2.2 Roles and Responsibilities

| | Contractor | Company |
|---|---|---|
| Monitor Incident management process effectiveness and adherence to Company policies and procedures | X | |
| Report on Incident management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Identify root causes of Incident-related Service Level failures and propose preventive/corrective actions through Problem management process, where appropriate, for in-scope Con iguration tems (“C s”) | X | |
| Provide management oversight and reporting of User escalation | X | |
| Manage Incident-related User escalations | X | |
| Monitor aged tickets and drive backlog reduction | X | |
| Maintain Incident management process documentation | X | |
| Propose Incident management process and policy improvement initiatives through continuous process improvement | X | |
| Monitor and improve Company’s customer experience re ated to ncident reso ution | X | |
| Monitor and report on the health of the Incident management process across all Managed Services as per Exhibit Q | X | |
| Partner with Company to drive continuous service improvement | X | |

Table 9 sets forth the roles and responsibilities of Contractor and Company for Incident Management. For clarity, the scope of Incident Management is limited to the Incidents related to the Supported Applications identified in Attachment C-1 (Supported Applications) and the technologies identified in Ex ibit (“ M in-cope Hardware”) ( erea ter “ upported pp ications and Tec no ogies”).

| Incident Management | Contractor | Company |
|---|---|---|
| Review, approve, and guide Incident management policies, procedures, and standards including Company ITSM Tool configurations | | X |
| Manage and govern the Incident management process operationally including maintenance of the process documentation | X | |
| Monitor health of the Incident management process and drive continuous service improvements | X | |
| Coordinate resolution of multi-tower Incidents as required | X | |
| Manage and maintain the Incident management process governance across in scope Services | X | |
| Provide escalation matrix for Company Vendors and act as escalation point between Contractor and Company Vendors | | X |
| Maintain escalation matrices | X | |
| Participate in the Incident management process governance as per the governance model described in Exhibit Q (Governance) | | X |

| Incident Management | Contractor | Company |
|---|---|---|
| Inform within two (2) working days of receiving a notification of audit (internal and external), excluding US holidays. | | X |
| Maintain Incident-related Service Levels as per Exhibit M | X | |
| Monitor Incident management process effectiveness and adherence to Company policies and procedures | X | |
| Report on Incident management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Identify root causes of Incident-related Service Level failures and propose preventive/corrective actions through Problem management process, where appropriate, for in-scope Con iguration tems (“C s”) | X | |
| Provide management oversight and reporting of User escalation | X | |
| Manage Incident-related User escalations | X | |
| Monitor aged tickets and drive backlog reduction | X | |
| Maintain Incident management process documentation | X | |
| Propose Incident management process and policy improvement initiatives through continuous process improvement | X | |
| Monitor and improve Company’s customer experience re ated to ncident reso ution | X | |
| Monitor and report on the health of the Incident management process across all Managed Services as per Exhibit Q | X | |
| Partner with Company to drive continuous service improvement | X | |

**Table 9. Incident Management Services Roles and Responsibilities.**

| Conduct post-Incident reviews for critical Incidents, document successes, areas for improvement, lessons learned and oot Cause na ysis (“ C ”) t roug rob em management process, when applicable. | X | |
|---|---|---|
| Monitor critical Incident management process health across all Managed Services | X | |
| Propose critical Incident management process and policy improvement initiatives through continuous process improvement. | X | |
| Establish and maintain a prioritization matrix and escalation matrix. | X | |

Table 10 sets forth the roles and responsibilities of Contractor and Company for the Critical Incident Management (“C M”).

| Critical Incident Management | Contractor | Company |
|---|---|---|
| Schedule, chair, and drive bridge calls to facilitate investigation and resolution of critical Incidents (P1 and selected P2). | X | |
| Participate in CIM bridge as needed (e.g. to confirm the Incident has been resolved) | | X |
| Manage and coordinate the resolution of critical Incidents related to CIs which are not in Contractor Scope | | X |
| Send out critical Incident (P1 and selected P2) communications to agreed Company stakeholders | X | |
| Participate in post-Incident reviews | | X |
| Review and approve such process improvement initiatives, communications, etc. | | X |
| Implement and communicate such process improvements when approved by Company as agreed | X | |
| Conduct post-Incident reviews for critical Incidents, document successes, areas for improvement, lessons learned and oot Cause na ysis (“ C ”) t roug rob em management process, when applicable. | X | |
| Monitor critical Incident management process health across all Managed Services | X | |
| Propose critical Incident management process and policy improvement initiatives through continuous process improvement. | X | |
| Establish and maintain a prioritization matrix and escalation matrix. | X | |

**Table 10. Critical Incident Management Services Roles and Responsibilities.**

| Set the Problem management-driven Incident ticket reduction targets to drive and track t e Contractor’s progress against targets periodica y | X | |
|---|---|---|
| Provide analysis on recurring Incidents | X | |
| Maintain Problem management process documentation | X | |
| Monitor Problem management process effectiveness and adherence to Company policies and procedures | X | |
| Report on Problem management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Partner with Company to drive continuous service improvement | X | |
| Operationally manage and coordinate RCA creation, delivery, reporting, and implementation of preventive/corrective actions for the Problem records | X | |
| Propose Problem management process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

**Table 11. Problem Management Services Roles and Responsibilities**

| | | |
|---|---|---|
| Set the Problem management-driven Incident ticket reduction targets to drive and track t e Contractor's progress against targets periodica y | X | |
| Provide analysis on recurring Incidents | X | |
| Maintain Problem management process documentation | X | |
| Monitor Problem management process effectiveness and adherence to Company policies and procedures | X | |
| Report on Problem management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Partner with Company to drive continuous service improvement | X | |
| Operationally manage and coordinate RCA creation, delivery, reporting, and implementation of preventive/corrective actions for the Problem records | X | |
| Propose Problem management process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

Table 11 sets forth the roles and responsibilities of Contractor and Company for Problem Management. For clarity, the scope of Problem Management is limited to Problems related to the Supported Applications and Technologies.

| Problem Management | Contractor | Company |
|---|---|---|
| Review, approve, and guide Problem management policies and standards including Company ITSM Tool configurations | | X |
| Manage and govern the Problem management process operationally, including maintenance of the process documentation | X | |
| Initiate creation of a Problem management plan and track progress against the plan. | X | |
| Coordinate RCA delivery and implementation of preventive or corrective actions | X | |
| Review and approve the RCA and the preventive or corrective actions | | X |
| Provide a fit for purpose known error database (KEDB) | | X |
| Manage and maintain KEDB | X | |
| Identify proactive Problem records based on Incident trend analysis | X | |
| Accept risks where preventive or corrective actions cannot be identified due to technology or Company IT environment constraints or when Company chooses not to implement the identified preventive or corrective action for any other reason subject to written explanation of such risks and their implications | | X |
| Review and approve Problem management process improvement initiatives | | X |

| Problem Management | Contractor | Company |
|---|---|---|
| Monitor Problem management process effectiveness and adherence to Company policies and procedures | X | |
| Report on Problem management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Manage and maintain the Problem management process governance across in-scope Services | X | |
| Participate in the Problem management process governance as per the governance model described in Exhibit Q (Governance) | | X |
| Act as escalation point between Contractor and Company Vendors | | X |
| Set the Problem management-driven Incident ticket reduction targets to drive and track t e Contractor's progress against targets periodica y | X | |
| Provide analysis on recurring Incidents | X | |
| Maintain Problem management process documentation | X | |
| Monitor Problem management process effectiveness and adherence to Company policies and procedures | X | |
| Report on Problem management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Partner with Company to drive continuous service improvement | X | |
| Operationally manage and coordinate RCA creation, delivery, reporting, and implementation of preventive/corrective actions for the Problem records | X | |
| Propose Problem management process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

**Table 11. Problem Management Services Roles and Responsibilities**

| Monitor Service Request fulfilment process effectiveness and adherence to Company policies and procedures | X | |
|---|---|---|
| Report on Service Request fulfilment process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Partner with Company to drive continuous service improvement | X | |
| Monitor and track each Service Request from opening to closing | X | |
| Monitor Service Request backlog, including aging tickets | X | |
| Report on Service Request backlog, including aging tickets as per Exhibit Q | X | |

| | | |
|---|---|---|
| Monitor and improve customer experience related to Service Request delivery | X | |
| Propose process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

Table 12 sets forth the roles and responsibilities of Contractor and Company for the Service Request Fulfillment. For clarity, the scope of Service Request Fulfilment is limited to the Service Requests related to the Supported Applications and Technologies.

| Monitor Service Request fulfilment process effectiveness and adherence to Company policies and procedures | X | |
|---|---|---|
| Report on Service Request fulfilment process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Partner with Company to drive continuous service improvement | X | |
| Monitor and track each Service Request from opening to closing | X | |
| Monitor Service Request backlog, including aging tickets | X | |
| Report on Service Request backlog, including aging tickets as per Exhibit Q | X | |
| Monitor and improve customer experience related to Service Request delivery | X | |
| Propose process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

Table 12. Service Request Fulfilment Services Roles and Responsibilities.

| Service Request Fulfilment | Contractor | Company |
|---|---|---|
| Review, approve, and guide Service Request fulfilment policies and standards including Company ITSM Tool configurations | | X |
| Submit Service Requests using Company ITSM Too ’s Service Request catalog, including approval and fulfillment workflow | | X |
| Manage and govern the Service Request fulfilment management process operationally, including maintenance of the process documentation | X | |
| Propose Service Request fulfilment management process improvement initiatives through continuous process improvement | X | |
| Review and approve Service Request fulfilment management process improvement initiatives | | X |
| Provide approval for fulfilment of Service Requests, where relevant | | X |
| Monitor and report on Service Request fulfilment management process effectiveness and adherence to Company policies and procedures | X | |

| Service Request Fulfilment | Contractor | Company |
|---|---|---|
| Review and approve proposed improvements to Service Request workflow design | | X |
| Monitor unfulfilled requests and manage requests via Service Request fulfilment management; monitor and report Service Request backlog, including aging tickets | X | |
| Manage and maintain the Service Request fulfilment management process governance for in-scope Services | X | |
| Participate in the Service Request fulfilment management process governance as per the governance model described in Exhibit Q (Governance) | | X |
| Provide escalation matrix for Company Vendors and act as escalation point between Contractor and Company Vendors | | X |
| Monitor Service Request fulfilment process effectiveness and adherence to Company policies and procedures | X | |
| Report on Service Request fulfilment process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Partner with Company to drive continuous service improvement | X | |
| Monitor and track each Service Request from opening to closing | X | |
| Monitor Service Request backlog, including aging tickets | X | |
| Report on Service Request backlog, including aging tickets as per Exhibit Q | X | |
| Monitor and improve customer experience related to Service Request delivery | X | |
| Propose process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

**Table 12. Service Request Fulfilment Services Roles and Responsibilities.**

| Maintain change management process documentation | X | |
|---|---|---|
| Schedule and chair the Change Advisory Board (CAB) meetings | X | |
| Publish forward schedule of approved changes | X | |
| Provide change communication | X | |
| Review and approve change communication | | X |
| Conduct impact assessments for in-scope changes | X | |
| Conduct post-implementation review for all failed and backed out changes for all in-scope CIs | X | |
| Review results of post-implementation review for failed and backed out changes | | X |

| | | |
|---|---|---|
| Provide input for determining approach to resolve failed and backed out changes | | X |
| Monitor change management process effectiveness and adherence to Company policies and procedures | X | |
| Report on change management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Propose change management process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

**Table 13. Change Management Services Roles and Responsibilities.**

| | | |
|---|---|---|
| Maintain change management process documentation | X | |
| Schedule and chair the Change Advisory Board (CAB) meetings | X | |
| Publish forward schedule of approved changes | X | |
| Provide change communication | X | |
| Review and approve change communication | | X |
| Conduct impact assessments for in-scope changes | X | |
| Conduct post-implementation review for all failed and backed out changes for all in-scope CIs | X | |
| Review results of post-implementation review for failed and backed out changes | | X |
| Provide input for determining approach to resolve failed and backed out changes | | X |
| Monitor change management process effectiveness and adherence to Company policies and procedures | X | |
| Report on change management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Propose change management process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

Table 13 sets forth the roles and responsibilities of Contractor and Company for Change Management. Company will manage change requests related to retained scope and represent them at the Change Advisory Board (“C ”).

| Change Management | Contractor | Company |
|---|---|---|
| Review, approve, and guide change management policies and standards including Company ITSM Tool configurations | | X |

| Change Management | Contractor | Company |
|---|---|---|
| Manage and govern the change management process operationally, including maintenance of the process documentation | X | |
| Provide tooling capability to raise changes from and link changes to Incident and Problems | | X |
| Assess the changes for technical impact on the Services | X | |
| Scheduling and chair CAB meetings | X | |
| Coordinate with Company Vendors for any impact on Company Vendors' services | X | |
| Act as point of escalation for Company Vendors during the changes, if required | | X |
| Approve changes | | X |
| Define the change approval process | | X |
| articipate in Company's defined change approval process | X | |
| Publish forward schedule of approved Changes | X | |
| Conduct post-implementation review for all failed and backed-out changes | X | |
| Participate in post-implementation review of failed and backed-out changes, as applicable | | X |
| Coordinate impact assessment and implement Contractor changes | X | |
| Propose change management process and policy improvement initiatives through continuous process improvement | X | |
| Review and approve the proposed improvements | | X |
| Implement the approved improvement initiatives | X | |
| Manage and maintain change management process governance across in-scope Services | X | |
| Participate in the change management process governance as per the governance model described in Exhibit Q (Governance) | | X |
| Maintain change management process documentation | X | |
| Schedule and chair the Change Advisory Board (CAB) meetings | X | |
| Publish forward schedule of approved changes | X | |
| Provide change communication | X | |
| Review and approve change communication | | X |
| Conduct impact assessments for in-scope changes | X | |
| Conduct post-implementation review for all failed and backed out changes for all in-scope CIs | X | |
| Review results of post-implementation review for failed and backed out changes | | X |

| Change Management | Contractor | Company |
|---|---|---|
| Provide input for determining approach to resolve failed and backed out changes | | X |
| Monitor change management process effectiveness and adherence to Company policies and procedures | X | |
| Report on change management process effectiveness and adherence to Company policies and procedures as per Exhibit Q | X | |
| Propose change management process and policy improvement initiatives through continuous process improvement | X | |
| Approve proposed improvements | | X |

**Table 13. Change Management Services Roles and Responsibilities.**

| Maintain Service Levels process documentation | X | |
|---|---|---|
| Monitor and measure agreed Cross-Functional Services metrics | X | |
| Report on agreed Cross-Functional Services metrics as per Exhibit Q | X | |
| Monitor and measure the Service Levels specified in Exhibit M (Service Levels) | X | |
| Update Cross-Functional Services metrics, as needed, to effectively measure continuous improvement towards Company's strategic priorities | X | |
| Manage and maintain the SLM process governance | X | |

Table 14 sets forth the roles and responsibilities of Contractor and Company for Service Level Management

| Maintain Service Levels process documentation | X | |
|---|---|---|
| Monitor and measure agreed Cross-Functional Services metrics | X | |
| Report on agreed Cross-Functional Services metrics as per Exhibit Q | X | |
| Monitor and measure the Service Levels specified in Exhibit M (Service Levels) | X | |
| Update Cross-Functional Services metrics, as needed, to effectively measure continuous improvement towards Company's strategic priorities | X | |
| Manage and maintain the SLM process governance | X | |

**Table 14. Service Level Management Roles and Responsibilities.**

| Service Level Management | Contractor | Company |
|---|---|---|
| Review, approve, and guide service level management (SLM) policies and standards including Company ITSM Tool configurations | | X |
| Manage and govern the Service Levels management process operationally, including maintenance of the process documentation | X | |
| Report on the Service Levels defined in Exhibit M (Service Levels) as per Exhibit Q | X | |
| Support service delivery performance review meetings by providing reports and inputs as described in Exhibit Q (Governance) | X | |
| Manage and maintain the Service Levels management process governance across in-scope Services | X | |
| Participate in the Service Levels management process governance as per the governance model described in Exhibit Q (Governance) | | X |
| Provide escalation matrix for Company Vendors and act as escalation point between Contractor and Company Vendors | | X |
| Maintain Service Levels process documentation | X | |
| Monitor and measure agreed Cross-Functional Services metrics | X | |
| Report on agreed Cross-Functional Services metrics as per Exhibit Q | X | |
| Monitor and measure the Service Levels specified in Exhibit M (Service Levels) | X | |
| Update Cross-Functional Services metrics, as needed, to effectively measure continuous improvement towards Company's strategic priorities | X | |
| Manage and maintain the SLM process governance | X | |

**Table 14. Service Level Management Roles and Responsibilities.**

| Maintain the knowledge management process documentation | X | |
|---|---|---|
| Periodically review and update knowledge articles for continued relevance | X | |
| Monitor the effective use of knowledge articles in resolving Incidents | X | |
| Propose knowledge management process improvement initiatives through continuous process improvement | X | |
| Manage and maintain knowledge management process governance | X | |

Table 15 sets forth the roles and responsibilities of Contractor and Company for Knowledge Management. For clarity, Knowledge Management is limited to the knowledge articles related to the Supported Applications and Technologies.

| Knowledge Management | Contractor | Company |
|---|---|---|
| Review, approve, and guide knowledge management policies and standards including Company ITSM Tool configurations | | X |

| Knowledge Management | Contractor | Company |
|---|---|---|
| Manage and govern the knowledge management process operationally including maintenance of the process documentation | X | |
| Publish knowledge articles | X | |
| Manage and maintain the knowledge management process governance across in-scope Services | X | |
| Participate in the knowledge management process governance as per the governance model described in Exhibit Q (Governance) | | X |
| Maintain the knowledge management process documentation | X | |
| Periodically review and update knowledge articles for continued relevance | X | |
| Monitor the effective use of knowledge articles in resolving Incidents | X | |
| Propose knowledge management process improvement initiatives through continuous process improvement | X | |
| Manage and maintain knowledge management process governance | X | |

**Table 15. Knowledge Management Roles and Responsibilities**

| Maintain service catalog management process documentation | X | |
|---|---|---|
| Provide inputs to catalog item creation/amendment, as required. Inputs are created through proactive analysis and identification of potential catalog items including suggested service level targets, if appropriate | X | |
| Identify service catalog improvement opportunities | X | |
| Periodically review the usage of the service catalog items | X | |
| Propose service catalog management process and policy improvement initiatives through continuous process improvement | X | |
| Manage and maintain service catalog management process governance | X | |

Table 16 sets forth the roles and responsibilities of Contractor and Company for Catalog Management. For clarity, Service Catalog Management Services is limited to the Service Catalogs related to the Supported Applications and Technologies.

| Service Catalog Management | Contractor | Company |
|---|---|---|
| Review, approve, and guide service catalog management policies and standards including Company ITSM Tool configurations | | X |
| Manage and govern the catalog management process operationally including maintenance of the process documentation | X | |
| Perform proactive analysis and identification of potential catalog items and define those as inputs for creation or amendment | X | |

| Service Catalog Management | Contractor | Company |
|---|---|---|
| Periodically review the usage and relevance of the catalog items, recommending decommissioning where required | X | |
| Provide inputs to catalog item creation or amendment, as required | X | |
| Review and approve improvement initiatives | | X |
| Implement service catalog improvements in Company ITSM Tool, including creation of new catalog items as needed. | X | |
| Participate in the catalog management process governance as per the governance model described in Exhibit Q (Governance) | | X |
| Provide escalation matrix for Company Vendors and act as escalation point between Contractor and Company Vendors | | X |
| Maintain service catalog management process documentation | X | |
| Provide inputs to catalog item creation/amendment, as required. Inputs are created through proactive analysis and identification of potential catalog items including suggested service level targets, if appropriate | X | |
| Identify service catalog improvement opportunities | X | |
| Periodically review the usage of the service catalog items | X | |
| Propose service catalog management process and policy improvement initiatives through continuous process improvement | X | |
| Manage and maintain service catalog management process governance | X | |

**Table 16. Service Catalog Management Roles and Responsibilities.**

| Maintain configuration management process documentation | X | |
|---|---|---|
| Maintain configuration management database (CMDB) | X | |
| Define Contractor's access ru es or CMD | X | |
| Propose configuration management process and policy improvement initiatives through continuous process improvement | X | |
| Review and approve CMDB access rules and proposed configuration management process and policy improvement initiatives | | X |

Table 17 sets forth the roles and responsibilities of Contractor and Company for Service Asset and Configuration Management.

| Service Asset and Configuration Management | Contractor | Company |
|---|---|---|
| Review, approve, and guide configuration management policies and standards including Company ITSM Tool configurations | | X |
| Manage and govern the service asset and configuration management process operationally including maintenance of the process documentation | X | |

| Service Asset and Configuration Management | Contractor | Company |
|---|---|---|
| Drive adherence to configuration management policies, processes, procedures, and standards | X | |
| Define CMDB data model for in-scope CIs types | | X |
| Define Contractor access rules for CMDB | | X |
| Manage and maintain access rules for CMDB | X | |
| Define CMDB audit procedures | | X |
| Manage and maintain CMDB audit procedures | X | |
| Manage and maintain CMDB as per the agreed process | X | |
| Update CMDB as per the agreed process | X | |
| Provide relationship between business services/process with the technology CIs | | X |
| Manage and maintain between business services/process with the technology CIs | X | |
| Manage and maintain the service asset and configuration management process governance across in-scope Services | X | |
| Participate in the service asset and configuration management process governance as per governance model described in Exhibit Q (Governance) | | X |
| Provide escalation matrix for Company Vendors and act as escalation point between Contractor and Company Vendors | | X |
| Maintain configuration management process documentation | X | |
| Maintain configuration management database (CMDB) | X | |
| Define Contractor's access ru es or CMD | X | |
| Propose configuration management process and policy improvement initiatives through continuous process improvement | X | |
| Review and approve CMDB access rules and proposed configuration management process and policy improvement initiatives | | X |

**Table 17. Service Asset and Configuration Management Roles and Responsibilities.**

# IMS – SAP Basis Management

## Services Description

### 1.1 Scope overview

The SAP Basis Management Services consist of Level 2 support for the SAP components and volumetrics specified in Section 2.2.

- Contractor shall provide the SAP Basis Management Services for the monthly ticket volumes listed in section 2.3.

### 1.2 SAP Basis Volumetrics

| SAP Component | System Type | OS | Database | Sandbox | Dev | QA | Training | Patch Test | Prod | HA | DR |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SAP ECC | SAP ECC 6.0 EHP8 | Win/RHEL | HANA 2.0 SP06 | S6N | D6N | Q6N | L6N | U6N | P6N | 1 | 1 |
| SAP CRM | CRM 7.0 EHP4 | Win/RHEL | HANA 2.0 SP06 | SCN | DCN | QCN | LCN | UCN | PCN | 1 | 1 |
| SAP BW | BW 7.5 | Win/RHEL | HANA 2.0 SP06 | SBN | DBN | QBN | | UBN | PBN | 1 | 1 |
| SAP PO | 7.5 JAVA | Win/RHEL | HANA 2.0 SP06 | SON | DON | QON | | UON | PON | 1 | 1 |
| SAP Solman ABAP | 7.2 ABAP | Win/RHEL | HANA 2.0 SP06 | | DSN | | | | PSN | 1 | 1 |
| SAP Solman JAVA | 7.2 JAVA | Win/RHEL | HANA 2.0 SP06 | | DSJ | | | | PSJ | 1 | 1 |
| SAP Portal | 7.5 JAVA | Win/RHEL | HANA 2.0 SP06 | SEN | DEN | QEN | | UEN | PEN | 1 | 1 |
| UCES | - | RHEL | HANA 2.0 SP06 | SUN | DUN | QUN | LUN | | PUN | 1 | 1 |

**Table 1. SAP Basis Volumetrics.**

### 1.3 SAP Basis monthly ticket volumes

| Type of Tickets (Monthly) | |
|---|---|
| Incidents | 125 |

| Type of Tickets (Monthly) | |
|---|---|
| Service Requests (4 hours maximum) | 28 |
| Problem | 2 |
| Change Requests | 7 |

**Table 2 SAP Basis Monthly Ticket Volumes.**

## 1.4 Support and Shift coverage

The following support and shift coverage applies to the SAP Basis Management Services.

| Services | Coverage |
|---|---|
| SAP Basis M**anagement** Services | 9X5 with on-call for P1 and P2 Incidents |

**Table 3. Coverage of SAP Basis Services.**

# Roles and Responsibilities

Table 4 sets forth the roles and responsibilities of Company and Contractor for the SAP Basis Management Services.

| Ref | SAP Basis Services | Contractor | Company |
|---|---|---|---|
| **SAP Basis Service Operations** | | | |
| **General** | | | |
| 1. | Communication to Company stakeholders related to SAP Basis Management Services | | X |
| 2. | Provide S-user ID and access to raise SAP Online Service System (OSS) messages | | X |
| 3. | Basic maintenance of SAP router & configuration | X | |
| 4. | Maintain connection which provides access to external vendor (SAP) | X | |
| 5. | Maintain runbooks, knowledge base, and operational procedures | X | |
| 6. | Act as a point of escalation between Contractor and Company' Vendors | | X |
| 7. | Perform vendor management | | X |
| 8. | SAP license management | | X |
| 9. | Provide maintenance agreements for all SAP applications, databases, and operating systems | | X |
| **SAP Configuration** | | | |
| 10. | Batch job scheduling for housekeeping activities (e.g. data archiving, cleanup activities, database maintenance) | X | |
| 11. | Approve proposed batch job schedule | | X |
| 12. | Execute scheduled batch jobs for housekeeping activities | X | |
| 13. | Functional background jobs scheduling in SAP | | X |
| 14. | Review and approval of SAP clients | | X |
| 15. | Setup of approved additional SAP clients | X | |
| 16. | Define weekly/monthly/quarterly transport window | | X |
| 17. | Transport input per approved change request | X | |
| 18. | Maintain system refresh schedule and approval | | X |
| 19. | Perform system refresh in accordance with agreed and approved schedule | X | |
| 20. | Deployment of SAP Basis OSS notes | X | |
| **Maintenance and Configuration Change** | | | |
| 21. | Provide schedule for planned outages as per Exhibit I | | X |
| 22. | Approve outages not part of existing outage schedule | | X |
| 23. | Outage planning and execution | X | |

| Ref | SAP Basis Services | Contractor | Company |
|---|---|---|---|
| **Incident, Problem, Change, Service Request Management, Monitoring, and Alerting** | | | |
| 24. | Follow ITSM processes as per Exhibit I to resolve Incidents, Service Requests, Change requests, and address Problem tickets | X | |
| 25. | P1/P2 Incident notification to Company and Basis support team using Company notification tool | | X |
| 26. | Recommend hotfix, patches, kernel patches, and security update changes | X | |
| 27. | Approve hotfix, patches, kernel patches, and security updates changes | | X |
| 28. | Apply hotfix, patches, kernel patches, and security updates following Change Management Process | X | |
| **Backup, Recovery, HA, and Disaster Recovery (DR)** | | | |
| 29. | Manage HANA database backup configuration, monitoring, and recovery | X | |
| 30. | Participate in annual disaster recovery test | X | |
| 31. | Notify Contractor of annual disaster recovery test schedule | | X |
| 32. | Provide Disaster Recovery strategy and approach and approve modification to recovery documentation | | X |
| 33. | Maintain Disaster Recovery (DR) plan documentation for SAP systems | X | |
| 34. | Perform SAP backup and recovery | X | |
| 35. | Provide reports for SAP backup and restore | X | |
| 36. | Recommend SAP backup schedule | X | |
| 37. | Approve SAP backup schedule | | X |
| 38. | Maintain SAP backup schedule | X | |
| **Other Administrative Activities** | | | |
| 39. | Access management for SAP HANA database | X | |
| 40. | Approve access for SAP HANA database | | X |
| 41. | Notify Company of SAP Basis resource and User account privilege changes (off-boarding, roles changes) | X | |
| 42. | Analyze Early Watch (EWA) sessions and make recommendations to Company | X | |
| 43. | Review and approve EWA recommendations | | X |
| 44. | Implement EWA approved recommendations | X | |
| 45. | Provide SAP HANA mini check recommendations | X | |
| 46. | Review and approve mini check recommendations | | X |
| 47. | Implement SAP HANA mini check approved recommendations | X | |

| Ref | SAP Basis Services | Contractor | Company |
|---|---|---|---|
| 48. | Generate agreed performance and usage reports to Company defined in Exhibit Q | X | |
| 49. | Configuration of operating system for printer and output management (e.g. Print Shop retained function) | | X |
| 50. | Monitor system performance | X | |

**Table 4. SAP Basis Services Roles and Responsibilities**

# Managed Security Services (MSS) Scope

## Service Description

### Cybersecurity Operations – SOC Operations

Contractor shall provide SOC services as set out in this section. The SOC services encompass staff augmentation support for the first phase and managed services for the second, with engineering and enhancement assistance throughout both the staff augmentation and managed services phases of delivery.

- **Phase-1 Staff Augmentation (Contract start date through November 2026):** Contractor shall provide two onshore and two offshore resources with SOC L2 analyst skills in a staff augmentation model to work with existing Company and third-party vendor team.
- **Phase-2 Managed SOC Services** (**Dec 2026 through end of contract**): 24x7 Managed SOC Operations (Level 1 and Level 2) services consist of:

**Level 1 Threat Detection:**

- Contractor shall monitor the security information collected from Log Sources, and Events of Interest, that are in each case generated by Company 's Security Information and Event Management (SIEM) Solution in accordance with the Use Cases approved by Company.
- The SIEM Solution will automatically log Events of Interest into the IT Service Management (ITSM) tool and generate a ticket. The response time for the Service Levels set out in Exhibit M (Service Levels) does not commence until the ticket has been generated.
- Contractor shall follow the agreed processes in the Runbook* to analyze and classify the logged Events of Interest into Security Event categories according to the Severity Levels set out below, including identifying and removing false positives.

Severity Levels set out below are assigned to Security Events

| Severity Level | Definition |
|---|---|
| **P1 - Emergency** | Business process and system functionality have been severely impacted or halted. A successful attack has rendered the system(s) or system data unsafe, inoperable, or compromised. |
| **P2 - High** | Business process and system functionality have been seriously affected. Systems and/or system data are exposed to interruption, compromise, or loss. |
| **P3 - Medium** | Business process or system functionality may be moderately affected. A threat may exist against systems or system data. |
| **P4 - Low** | Systems and/or system data are not at risk. These events are required for purposes of auditing, forensics, and legal or regulatory compliance, and may also be useful for trend analysis or correlation. This Severity Level serves as the default for unclassified Security Events. |

**Level 2 Threat Detection:**

- Where an Event of Interest is classified as a Security Event, Contractor shall notify the Security Point of Contact (POC) in accordance with the communication protocols in the Runbook for the Severity Level of the Security Event. The escalation of Security Events to the Security POC will include relevant information such as log files, reported device, vulnerability exploited, attack type, and reputation of attack

source, in each case where available. Contractor's analysis of a Security Event will be based on the threat intelligence feeds made available by Company

- Contractor shall provide Company with additional details in the form of search data and trend details that lead to understanding attributes for the Security Event that may later be used in performing Root Cause Analysis to facilitate Company identifying the root cause of a Security Event. Contractor shall assist Company with development of recommended mitigation actions for the Security Event and will assign the Security Event ticket in the ITSM to the relevant teams for resolution (Infrastructure, Firewall, Desktop, etc.) in accordance with Company 's standards and policies.
- Contractor shall coordinate with the respective teams as they respond to the Security Event and monitor, track and update the Security Event ticket to closure. Company remains responsible for resolution of the Security Event and for closing the Security Event ticket.
- Contractor shall support Company's integration of new Log Sources into the SIEM Solution by providing configuration information, instructions on how to integrate with the SIEM Solution and responding to ad hoc questions.

**Major Event Management/ Crisis Management**

- Where Contractor identifies that a Security Event requires escalation to a Major Event in accordance with the Runbook, Contractor shall follow the process set out in the Runbook to invoke a Major Event. Contractor shall assist Company with coordinating the response to the Major Event in accordance with the Runbook and Company's Cybersecurity Incident Response Plan, including, where applicable, establishing a hotline, gathering data, creating logs, performing limited remediation tasks (e.g. the removal of malware), notifying and contacting Company's IT team (as defined in the Runbook), attending a Major Event coordination call, engaging Company's third party vendors whose software or infrastructure may be impacted by the Major Event, and assisting Company in initial stages of planning a response.

The Major Event Management services do not include resolution or remediation of the Major Event, detailed investigation into the Major Event (beyond what is performed under Level 2 Threat Detection), and forensic evidence gathering.

**Reporting**

- **Standard Reports:** Contractor shall provide the reports to Company at the frequency set out in the table below. The reports shall include the parameters agreed with Company during Transition phase of Phase-2. Reports as set forth in the Exhibit Q – Governance & Reports.

| Report Title | Report content | Format | Frequency of delivery (weekly, monthly etc) | Recipient |
|---|---|---|---|---|
| **Technical report** | Provides details on severity P1 and P2 Security Events | Word Document | On as needed basis | SOC\Computer Emergency Response Team (CERT) personnel |
| **Security Event Notification** | Provide reports on detected Security Event | Microsoft Form | On as needed basis | SOC\Computer Emergency Response Team (CERT) personnel |

| | | | | |
|---|---|---|---|---|
| **Service Level Report** | Report on service level performance in the previous reporting period. | Word Document, Excel Spreadsheet | Monthly | SOC\Computer Emergency Response Team (CERT) personnel |

**Table 1 SOC Operations Reports**

- **Custom Reports:** Contractor shall develop and deliver custom reports using Company's SIEM Solution at Company's request ("Custom Reports"). The development of Custom Reports that may include features related to the design, generation, and testing prior to introduction to the production environment. Upon receipt of a request for a Custom Report, Contractor will confirm if such Custom Report can be provided as part of the MSS Fixed Fees, the Minor Enhancements Hours Pool (if available), or if none of these options are available, through a Change Order in accordance with Exhibit Q (Governance) and the Agreement.

Tools: Unless otherwise agreed to in writing, the following tools will be used to provide Security Operations Center Services

| Relevant Solution | In-Scope System | License Provided |
|---|---|---|
| Security Information and Event Management (Non-CIP/ IT SIEM) | QRadar | Company |
| Security Orchestration, Automation, and Response (SOAR) | QRadar | Company |
| ITSM/ Ticketing tool | ServiceNow | Company |

**Table 2 In-Scope Systems for SOC Operations**

**Phase-1 Staff Augmentation Services:** Contractor shall provide the following resources to perform the Capacity Services for IT SOC Operations:

| # | Role Description | Role location | Part-time / Full-Time | FTEs |
|---|---|---|---|---|
| 1 | IT SOC Analyst-L2 | USA | Full-Time | 2 |
| 2 | IT SOC Analyst-L2 | India | Full-Time | 2 |

**Table 3 Staff Augmentation**

**Phase-2 Managed SOC Services:** The following volumetric table define the metrics for the Services, measured as per the frequency specified in the Metric:

| Area | Baseline Resource Unit/Metric | Volume |
|---|---|---|
| Security Information and Event Management (SIEM) | Number of Incidents per month | 500 |
| Security Orchestration, Automation, and Response (SOAR) | Number of new playbooks per quarter | 1 |
| SIEM Use cases | Number of new use cases per month | 1 |

## 2.1 Data & Technology Cybersecurity – Privileged Access Management (PAM)

Contractor shall provide Level 2 and Level 3 Support Services for managing and administering the privileged administrator identities and access. The PAM services consist of the following:

- Managing the Privileged Access for administrators leveraging Company provided PAM tool
- Managing the Privileged identity lifecycle including onboarding and offboarding of privileged identities leveraging Company provided tool sets
- Discovering privileged accounts by leveraging Company provided toolset
- Managing Incidents, Service Requests, Problems, and Changes for the Privileged Access Management services
- Administering and managing the Privileged Access toolset

Privileged Access Management Services are provided on an 8x5 basis, 24x7 P1/P2 on-call support for IT systems and 8x5 support with 24x7 P1/P2 on-call support for OT systems.

| Area | Tool Used | Baseline Resource Unit / Metric | Volume | Service Window |
|---|---|---|---|---|
| Privileged Access Management (PAM) | CyberArk | Number of Privileged Users | 1200 | 8x5 ET (with 24x7 On-call for P1 and P2) for IT systems<br>8x5 ET (with 24x7 on-call for P1 and P2) for OT systems |
| | | Number of accounts | 24662 | |
| | | Number of instances | 4 (2 for IT; 2 for OT | |
| | | Number of Tickets per month | 250 (100 Incidents, 150 Service requests) | |
| | | Number of accounts to be onboarded per month | 50 – Y1, Y2<br>25 – Y3, Y4, Y5 | |

**Table 5 Volumetrics for Privileged Access Management**

## 2.2 Data & Technology Cybersecurity – Access Management, Directory Services, and Certificate Management Services

Contractor shall provide access management, directory services and certificate management planning and support consisting of the following:

- Performing platform support and maintenance
- Resolving Incidents, service Requests, Problem and Changes for the in-scope services
- Manage authentication, authorization, single sign on policies
- Manage directory services schema, forests, domains, and group policies
- Manage certificate lifecycle for internal and external certificates
- Renew Certifying Authorities (CA) certificates and manage root/intermediate CA validity
- Providing monthly reports

Managed services are provided on an 8x5 basis plus 24x7 P1/P2 on-call support for IT systems

The following volumetric tables define the metrics for the Access Management Single Sign on, Directory Services and Certificate Management services, measured monthly:

Only low and medium complexity applications as defined in **Error! Reference source not found.**, that support standard connectors like SAML, OIDC, OAuth will be onboarded as a part of managed services. High complexity application onboarding (applications not supporting standard protocols or requiring web-agents) would be assessed for efforts and addressed as part of Project work.

| Complexity Type | Criteria | Example |
|---|---|---|
| **Low** | • Platform: Application uses standard platform (SAML/OAUTH based integrations)<br>• Connectors: Out of box (OOB) connectors deployed from Access Management tools with only URL configurations leveraging OOB integration protocols like SAML/OAUTH<br>• Access Control Model: Simple access control model utilizing only standard authentication and authorization mechanisms<br>• Collaboration: Low communication and touch point with application owners | • Standard SAML/OAUTH based integrations<br>• |
| **Medium** | • Platform: Application uses non-standard platform (e.g., OIDC based integrations)<br>• Connectors: OOB connectors deployment, Java Code Development for authentication and authorization processes<br>• Access Control Model: Medium complexity access control model mostly utilizing standard authentication and authorization mechanisms<br>• Collaboration: Medium communication and touch point with application owners | • Development of OIDC based integrations with minor Java Code development |
| **High** | • Platform: Legacy or complex platform (e.g., Webservices (SCIM), Apps requiring Data migrations, IDP-SP based integrations, out of support applications)<br>• Connectors: Custom Connector development and Java code development for authentication and authorization processes | • Custom Connectors development, API-based connectors, Webservices API development, Apps requiring Data migrations, out of support applications |

| | | |
|---|---|---|
| | • Access Control Model: High complexity access control model using roles and entitlements required for fine grained authorizations<br>• Collaboration: High communication and touch point with application owners | |

**Table 7 Application Complexity Criteria**

## Infrastructure Security – Cloud Security

Cloud Managed Security Services comprise management, and operation of Cloud Access Security Broker (CASB), Cloud Security Posture Management (CSPM) solution, and Secured Internet Access solution. The services consist of:

- Configuration and cloud security rules/ policy administration
- Policy creation, tuning, and management
- Alert/ incident monitoring, and resolution tracking
- Operational Runbook creation and execution
- Tool administration and health monitoring
- Change Management support
- Resolve Incident, Service Requests, Change and Problem Management tickets

- Executive reporting

The following volumetric tables define the metrics for the Cloud Managed Security Services, measured monthly:

| Area | Baseline Resource Unit/ Metric | Volume | Service Window |
|---|---|---|---|
| Cloud Security Posture Management | # of tickets per month | 50 tickets | 8x5 ET (with 24x7 On-call for P1 and P2) |
| Cloud Access Security Broker | # of users<br># of tickets per month | 9000 users<br>100 tickets | |
| Secure Internet Access | # of users<br># of tickets per month | 9000 users<br>100 tickets | |

**Table 10 Volumetrics for Cloud Security**

## Infrastructure Security – Firewall Management

Firewall Management service provides management and maintenance of Company 's firewalls in IT environment. For the firewalls listed in Exhibit U ("**Firewalls**"), the Firewall Management services consist of:

- **System Administration:** Perform required ongoing system administration activities for the Firewalls, and action any relevant outputs from the specific Firewalls, in accordance with the Runbook.
- **Availability and Health Monitoring:** Monitor the availability of the Firewalls and respond to alerts that a Firewall is unavailable in accordance with the Runbook.
- **Firewall Patch Management:** Review existing configuration of the Firewalls, propose and implement simple patches version updates or enhancements which are available from the third-party vendor, this also includes patching or upgrading the Firewalls (where available)., but excludes major upgrades or enhancements Contractor is only responsible for implementing patches on the Security Tools and can only implement patches made available by third party vendors. Contractor will implement the patches in accordance with either Company's operational change management or emergency change management procedure. Contractor shall advise Company of prioritization of patching but is not liable for any events, including Security Events, that occur as a result of delayed implementation of patching to the extent the delay is requested or caused by Company, or failure by a third-party vendor to provide a patch that

addresses vulnerabilities or new threats. Nonetheless, Contractor will be responsible to reasonably remediate the Security Event to the extent set forth in this Exhibit K.

- **Fault Management:** Remediate actions to resolve defects in the Firewalls detected during routine health check or from other sources, logged into the ITSM. Review of recurring faults and performing root cause analysis of defects as needed to help maintain availability of the Applications. Contractor may interact with Company's third-party vendors to troubleshoot existing issues or enhancements of the Firewalls. This includes coordination with the vendor for version and patch updates.
- **Reporting:** Contractor shall provide the standard reports described in Exhibit Q (Governance & Reports) to Company. These reports shall include the parameters and frequency agreed with Company during Transition.

The following firewalls are in scope for the Firewall Management services

| Area | Baseline Resource Unit/ Metric | Volume | Service Window |
|---|---|---|---|
| Firewall Management | Number of Firewalls | 214 | L1/ L2 - 8x5 ET<br>Engineering support – 8x5 (2 PM – 10 PM IST) + On-call for P1 and P2 |
| Firewall Management | Number of Tickets per month (including CRs and SRs) | 450 | L1/ L2 - 8x5 ET<br>Engineering support – 8x5 (2 PM – 10 PM IST) + On-call for P1 and P2 |
| Firewall rule review | Frequency of rule review | Annual review | 8x5 (2 PM – 10 PM IST) + On-call for P1 and P2 |

**Table 12 Volumetrics for Firewall Management**

## 2.3 Application Security

Application Security Testing (Static Application Security Testing (SAST); Software Composition Analysis (SCA); Dynamic Application Security Testing (DAST)) services include:

- **Scanning.** Contractor shall work with Company to define and perform testing of the applications for identification of security vulnerabilities. Such scanning may attempt to exploit vulnerabilities or to execute vulnerability checks that could affect the stability of a system. Company acknowledges and accepts such risk, and that except to the extent that Contractor is providing Services with respect to the applicable applications, Company is responsible to make appropriate support available to undertake remedial action if such risk eventuates. Scanning will include up to 2 user roles (Developer and Tester roles) within the application.
- **Scanning Environment.** Contractor shall only perform scans scheduled through Company Change Approval Board (CAB) or in non-production/sandbox environments.
- **Re-Scans:** Contractor and Company will agree and perform re-scans within the Monthly Baseline Volume for Application to be scanned specified in Attachment T-1-D MSS RUs.
- **Basic Reporting:** Contractor shall generate basic vulnerability standard reports after performing scans ("Basic Reports"). These Basic Reports are generated from the SAST, SCA, and DAST scanner directly by leveraging the reporting capability of the tool. Basic Reports are generated and shall be provided to Company on a monthly basis. Customization of the Basic Reports is not in scope for the Application Vulnerability Management Services. Contractor's basic reporting responsibility also include quarterly submission of tickets for vulnerability remediation or risk exception submission using Company's ITSM tool to ITSM resolver groups (or emails to 3rd party URL owners who are not using Company's ITSM tool) owning URLs discovered by vulnerability scanning to have out-of-compliance vulnerabilities as dictated by Company 's vulnerability management standard.

The following volumetric tables define the metrics for the Application Vulnerability Management Services, measured monthly:

| Area | Baseline Resource Unit/ Metric | Volume | Service Window |
|---|---|---|---|
| Phase – 1: During Migration and Modernization | Applications to be scanned for SAST, DAST, and SCA per month | M4 – 2; M5 & M6 – 5; M7-7; M8-M12 – 8; M13 – 14; M15-M23 – 15 apps; M24 – 8 | 8x5 (2 PM to 10 PM IST) |
| Phase – 2 Post Migration and Modernization | Applications to be scanned for SAST, DAST, and SCA per month | 10 Applications | Applications to be scanned for SAST, DAST, and SCA per month |

**Table 14 Volumetrics for Application Security**

## 2.4 Penetration Testing (PT)

Contractor shall perform a point-in-time "path of least resistance" penetration test covering OWASP Top 10 and vendor advisories of the web applications ("**Penetration Testing Applications**") and IP addresses identified by Company for penetration testing to identify security vulnerabilities in the application layer that may lead to unauthorized access to Company's network, systems and the data contained within. Using the defined attack paths as per the business logic, Contractor will attempt to search for, obtain access and exploit weaknesses in such In-Scope Penetration Testing Applications and IP Addresses to demonstrate that the vulnerability exists, show the business impact of the vulnerability and leverage the vulnerability to gain deeper access to Company's systems. The Penetration Testing scope includes:

- Infrastructure Penetration Testing of external IP addresses
- Web Application Penetration Testing of external URLs
- Remediation guidance and report submission
- Privilege Escalation

The testing scope will be limited to the below category, type and volumetrics considering all applications are medium sized with less than or equal to 50 dynamic pages per app and 2 user roles.

| Area | Baseline Resource Unit/ Metric | Volume | Service Window |
|---|---|---|---|
| Web Application PT | # of Apps to be tested per month | 2 Apps<br>Each month except the month Contractor performs the Internal Corporate Test (i.e., 11 of 12 months annually) | 8x5 (2 PM to 10 PM IST) |
| Infrastructure PT | # of external IP addresses to be tested per month | 200 IP addresses | 8x5 (2 PM to 10 PM IST) |
| Connectivity to OT networks | Once per year, test access to the OT Network from either the Corporate IT network or from direct internet connections to the OT network (e.g. Third-party remote access for maintenance) | 1 time annually | 8x5 (2 PM to 10 PM IST) |
| Internal Corporate Network | Once per year, test internal access for privilege escalation and lateral movement techniques and weaknesses.<br>Test scope will be limited to two Penetration Testing Applications and two unique credentials as the starting point. | Once per year, instead of the 2 Penetration Testing Applications PT above that month (not in addition to) | 8x5 (2 PM to 10 PM IST) |

**Table 16 Volumetrics for Penetration Testing**

| Area | Security Tool | License provided |
|---|---|---|
| Web and Infra PT | Burp Suite Pro | Company |
| Web and Infra PT | Multiple Open-Source Tools | Contractor |

**Table 17 Tools for Penetration Testing**

## 2.5 Security Engineering as a Service

Security Engineering as a Service include providing platform support and engineering services such as policy configurations, out of box integrations, health monitoring and fault management of in-scope security technologies.

The following volumetric table defines the metrics for the Security Engineering as a Service

| Area | Baseline Resource Unit/ Metric | Volume | Service Window |
|---|---|---|---|
| Security Engineering as a Service | # of tickets (including SRs, incidents) per month | 200 | 8x5 (2 PM to 10 PM IST) + On-call for P1 and P2 |

**Table 18 Volumetrics for Security Engineering as a Service**

## 2.6 Cybersecurity Strategy and Planning – Third Party Risk Management

Third Party Risk Management (TPRM) services include performing ongoing TPRM assessments, identifying and logging findings from the risk assessments, and providing monthly reports on the assessment findings to Company stakeholders.

The following volumetric table define the metrics for the TPRM Services, measured monthly

| Area | Baseline Resource Unit/ Metric | Volume | Service Window |
|---|---|---|---|
| Third Party Risk Management | # of Assessments per month<br># of Investigations per month | 5 Vendor assessments per month<br>2 Investigations per month | 8x5 (2 PM to 10 PM IST) |

**Table 20 Volumetrics for Third Party Risk Management**

## 2.7 Cybersecurity Strategy and Planning – Risk Assessments

Contractor shall provide the following support services to assist with IT Security Risk Management to Company. The IT Risk Management Services consist of the following activities in support of Company's Risk Management:

- Support Company in performing 3-4 IT Risk Assessments on an ongoing basis. IT Risk Assessments for the purpose of this SOW refers to reviewing the changes logged through Change Management Process and tagged to Contractor for review, impacting Company Cyber Security Posture against Company Risk Assessment framework and identifying any gaps in the change that are not aligned with Company Cybersecurity policies and procedures.
- Update risk register with cyber security risks
- Provide monthly reports on the status of the risks

The following volumetric table define the metrics for the IT Security Risk Assessment Services, measured monthly

| Area | Baseline Resource Unit/ Metric | Volume | Service Window |
|---|---|---|---|
| IT Security Risk Assessment (SRA) | Risk Assessments per month | 4 Risk Assessments per month | 8x5 (2 PM to 10 PM IST) |

**Table 22 Volumetrics for Risk Assessment**

# Roles and Responsibilities

## 3.0 SOC Operations

Table 26 Staff Augmentation Roles and Responsibilities. Table 26 outlines the Staff Augmentation Roles and Responsibilities of Company and Contractor. Table 27 outlines the SOC Operations Roles and Responsibilities of Company and Contractor.

**Phase-1 Staff Augmentation Service**

| Item | IT SOC Operations | Contractor | Company |
|---|---|---|---|
| **Staff Augmentation** | | | |
| 1. | Request for resources across staff augmentation security services providing appropriate agreed upon lead time through demand planning and capacity management | | X |
| 2. | Source and identify the required personnel once the requirements are triggered by Company | X | |
| 3. | Onboard the new Personnel and integrate into the team | X | |
| 4. | Manage the Personnel on a day-to-day basis, including monitoring their performance, providing feedback, and handling any issues that may arise. | X | |
| 5. | Assign Day-day-operations tasks to the Security Personnel onboarded | | X |
| 6. | Manage Shift, deliverables, of Managed Capacity services | | X |
| 7. | Responsible for day-to-day operations, ongoing service management, preparing the shift plan, any SLA / SLO that have been agreed to with Company business teams | | X |
| 8. | Provide resources including but not limited to, playbook, runbook, guides, etc. required to support the day-to-day operations in alignment with current SOC operations and deployed capabilities. | | x |

**Table 26 Staff Augmentation Roles and Responsibilities.**

**Phase-2: Managed SOC Services:**

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| **Security Monitoring and Incident Management** | | | |
| 1. | Provide, maintain and update Cyber Incident Response Plan (“**CIRP**”) | | X |
| 2. | Development and provision of Runbook | X | |
| 3. | Maintain and update Runbook as required due to various changes including Use Case development, and integration of new Log Sources and devices. | X | |
| 4. | Participate in implementation of CIRP in accordance with the Runbook | X | |
| 5. | Provide Company approved data retention standard for logging | | X |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| 6. | Provide external threat intelligence feeds to Contractor | | X |
| 7. | Integration of threat intelligence feeds into SIEM | X | |
| **Level 1 - Threat Detection** | | | |
| 8. | Monitor the SIEM Solution for Events of Interest | X | |
| 9. | Log Events of Interest flagged in the SIEM solution into the ITSM solution | X | |
| 10. | Analyze and categorize Events of Interest in the ITSM solution in accordance with agreed Severity Levels and the Runbook. Remove false positives and false negatives | X | |
| 11. | Provide input on identifying false positives and false negatives | | X |
| 12. | Escalate security incidents in accordance with Company's CIRP and Runbooks | X | |
| **Level 2 – Threat Detection** | | | |
| 13. | Investigate Security Events including log analysis, coordinate response activities with system owners, communicate updates and track resolution | X | |
| 14. | Assign activities to Company's IT teams to resolve the Security Event | X | |
| 15. | Implement resolution activities for Contractor in-scope systems | X | |
| 16. | Coordinate response activities between Company's IT teams and track activities until completed in accordance with the Runbook. | X | |
| 17. | Provide support for remediation of incidents on unmanaged devices | | X |
| 18. | End user technical support for issues not related to security (e.g., real-time troubleshooting) | | X |
| **Major Event Management** | | | |
| 19. | Confirm whether a Security Event meets the criteria to be escalated as a Major Event in accordance with the Runbook | X | |
| 20. | Notify Company of a potential Major Event using the notification processes set out in the Runbook | X | |
| 21. | Implement the CIRP | | X |
| 22. | Assist with implementation of the CIRP | X | |
| 23. | Implementation of remediation and recovery from Major Event | | X |
| **SOAR Support and Operations Management** | | | |
| 24. | Identify use cases for automation using SOAR playbooks. | X | |
| 25. | Approve the use cases selected for automation. | | X |
| 26. | Develop, test, deploy, monitor, and optimize the playbooks. | X | |
| 27. | Approve the finalized playbooks. | | X |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| 28. | Integrate, enhance, and update both playbooks and process documentation. | X | |
| 29. | Provide licenses, API keys, and documentation for both third-party and internal tools. | | X |
| 30. | Execute new integrations with IBM QRADAR SOAR and oversee the monitoring of existing API integrations. | X | |
| 31. | Resolve or escalate issues that fall outside the SOAR application. | | X |
| 32. | Adhere to the Change/Release Management process. | X | |
| 33. | Approve changes in line with the Change/Release Management process. | | X |
| 34. | Administer SOAR, including managing console access, licenses, and other administrative functions. | X | |
| **Engineering and Enhancements** | | | |
| 35. | **Use Cases** | | |
| 36. | Define new Use Cases for the SIEM Solution | X | |
| 37. | Approve new Use Cases for deployment | | X |
| 38. | Develop, deploy, monitor and adjust new Use Cases | X | |
| 39. | Provide metrics in reports or dashboards, in a mutually agreed format | X | |
| 40. | **Integrations** | | |
| 41. | Support Company's integration of new Log Sources into the SIEM solution by providing configuration information, instructing on how to integrate with the SIEM and responding to ad hoc questions. | X | |
| 42. | Review and approve new Log source recommendations by Contractor | | X |
| 43. | Implement new Log Sources into the SIEM solution | X | |
| 44. | **Enhancements and other changes** | | |
| 45. | Raise Change | X | |
| 46. | Analyze and review the Change | X | |
| 47. | Propose time and cost estimate for the Change | X | |
| 48. | Accept proposed time and effort estimate for the Change | | X |
| 49. | Communicate, develop and implement Change | X | |
| 50. | Approve Change | | X |
| 51. | Review post Change implementation | X | |
| 52. | Manage Change closure and notification | X | |
| 53. | Update Runbooks with Changes | X | |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| 54. | Roll back if needed | X | |
| **Reporting (Refer Exhibit Q – Governance and Reports)** | | | |
| 55. | Provide scheduled statistical Reports (e.g., number of events, trending analysis, etc.) | X | |
| 56. | Provide list of stakeholders to whom the reports will be distributed by Contractor | | X |
| 57. | Request custom report | | X |
| 58. | Propose time and effort estimate for the custom reporting | X | |
| 59. | Accept proposed time and effort estimate for the custom report | | X |
| 60. | Generate custom reports as agreed in accordance with Change Management | X | |
| **SIEM Support and Operations Management** | | | |
| | **Availability and Health Monitoring** | | |
| 61. | Approve initial access to QRADAR software to monitor availability for SIEM Solution | | X |
| 62. | Ongoing access requirements and platform maintenance | X | |
| 63. | Monitor alerts from the SIEM solution related to availability | X | |
| 64. | Where availability is impacted, perform activities set out in the Run Book to react to the alert | X | |
| | **Patch Management for the SIEM Solution** | | |
| 65. | Identify, analyze and prioritize patches | X | |
| 66. | Conduct testing for each patch | X | |
| 67. | Follow Change/Release Management process | X | |
| 68. | Approve Changes in accordance with the Change/Release Management process | | X |
| 69. | Deploy the patches | X | |
| | **Log Source Tracking** | | |
| 70. | Add new log sources to SIEM | X | |
| 71. | Monitor Log Sources reporting into SIEM Solution and identify Log Sources that fail to report in accordance with the Runbooks | X | |
| 72. | Perform initial troubleshooting to identify the cause of the failure to report | X | |
| 73. | Raise a ticket in the ITSM system for resolution of the identified cause of the failure to report | X | |
| 74. | Coordinate remediation actions to resolve identified issue with Log Sources with Company ’s IT teams | X | |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| | **Fault Management** | | |
| 75. | Identify and classify faults in the SIEM Solution (application) and SIEM infrastructure (where the SIEM is hosted) and in scope Log Sources | X | |
| 76. | Notify Company of faults using the ITSM and escalation process in the Runbook | X | |
| 77. | Investigate and diagnose faults in the SIEM application and infrastructure | X | |
| 78. | Resolve/escalate faults outside the SIEM infrastructure and application and Log Sources beyond Level 2 troubleshooting | | X |
| 79. | Resolve/escalate faults in the SIEM infrastructure and application | X | |
| 80. | Perform Root Cause Analysis and problem resolution in the SIEM infrastructure and application | X | |
| 81. | Coordinate with product manufacturer or third-party vendor for issue resolution in the SIEM infrastructure and application | X | |
| 82. | Notify end users about the availability on service restoration in accordance with agreed processes | | X |
| | **Backup and Restore Management** | | |
| 83. | Perform backup operation of SIEM configurations and data | X | |
| 84. | Verify backup operation | X | |
| 85. | Perform restoration from the backup | X | |
| 86. | Provide software to perform backup and location/facility to store backup data | | X |
| | **Disaster Recovery** | | |
| 87. | Develop and maintain Disaster Recovery Plan | | X |
| 88. | Provide input into and approve application of Disaster Recovery Plan to the Security Monitoring and Incident Management services | X | |
| 89. | Build and maintain Disaster Recovery infrastructure | | X |
| 90. | Participate SOC support to IT Disaster Recovery planning and exercises | X | |
| 91. | Follow the Disaster Recovery Plan if implemented | X | |
| | **General Support** | | |
| 92. | SIEM administration, including granting resources access to the console/removing access after PPL approval | X | |
| 93. | Provide physical or virtual support for any hardware maintenance, replacements, racking and stacking, cabling, etc. | | X |
| 94. | Enable appropriate access to Company -owned tools including any necessary licences | | X |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| 95. | Provide documentation regarding network devices, servers, and applications for integration with SIEM | | X |
| 96. | Provide virtual or physical hardware and storage for the SIEM | | X |
| 97. | Provide connectivity for SIEM and log sources | | X |
| 98. | Provide license and OEM (Original Equipment Manufacturer) for SIEM Solution and obtain additional licensing (if required) | | X |
| 99. | Provide OEM Maintenance agreements for SIEM Solution | | X |
| 100. | Pay for any third-party software changes, including upgrades | | X |
| 101. | Escalated Forensics and Incident Response services | | X |
| 102. | Asset management | | X |
| 103. | Execution and/or change management of product migrations or re-platforming | | X |

**Table 27 SOC Operations Roles and Responsibilities.**

## General Service Management for PAM/Access Management - Single Sign on/Directory Services/Certificate Management

Table 28 General Service Management for PAM/Access Mgmt/Dir Services/Cert Management roles and responsibilities outlines the roles and responsibilities of Company and Contractor.

| Item | General Service Management | Contractor | Company |
|---|---|---|---|
| | **General** | | |
| 1. | Execute and participate in the Service Management process across in-scope Services such as Incident Management, Major Incident Management, Service Requests, Problem Management, Change Management, Service Level Management. | X | |
| 2. | Comply with Service Management process, policies, notification and escalation procedures. | X | |
| 3. | Propose process and policy improvements. | X | |
| 4. | Review and approve such process improvement initiatives. | | X |
| 5. | Implement and communicate approved process improvements. | X | |
| 6. | Produce periodic reports mutually agreed between the Contractor and the Company | X | |
| 7. | Publish contact lists of Company teams, including major incident distribution list, Company third party vendors and other stakeholders. | | X |
| | **Incident Management** | | |

| Item | General Service Management | Contractor | Company |
|---|---|---|---|
| 8. | Report Incidents by opening a Ticket in accordance with Company's process as set forth in the Incident Management Standard Operating Procedure ("SOP") | | X |
| 9. | Resolve Incidents relating to the In-Scope IAM tools – CyberArk/Myapps - Entra ID/AD/Azure AD/Certificate Management tools | X | |
| 10. | Notify the applicable software vendor of a Product defect and coordinate correction/resolution as appropriate | X | |
| 11. | Schedule the installation of the Product defect corrections into production | X | |
| 12. | Update user, system, operations documentation, and knowledge management database as necessary, including lessons learned for future improvement | X | |
| 13. | Perform Incident analysis, diagnosis, and resolution consistent with the Service Levels | X | |
| | **Major Incident Management** | | |
| 14. | Identify that the incident meets the criteria to be escalated as a Major Event in accordance with the Standard Operating Procedure | X | |
| 15. | Notify Company of a potential Major Event using the notification processes set out in the Procedures Manual | X | |
| 16. | Coordinate with the Service Desk team for creating a bridge and sending notifications to all parties involved for troubleshooting, resolution of the Major incident and send End User communications | X | |
| 17. | Launch Major incident Management ("MIM") process as per Company established MIM process and coordinate with end user communication team to notify required stakeholders of the Major incident | X | |
| 18. | Implementation of remediation and recovery from Major Event for in scope services | X | |
| 19. | Implementation of the Cyber Incident Response Plan ("CIRP") in case of a Breach | | X |
| 20. | Assist with implementation of the CIRP | X | |
| | **Service Request Management** | | |
| 21. | Create service request within the ITSM tool | X | |
| 22. | Assign priority for service request | X | |
| 23. | Provide approvals for service request | | X |
| 24. | Deploy changes pertaining to service requests (as applicable) as per the release schedule | X | |
| 25. | Update service request status throughout ITSM tool | X | |
| | **Problem Management** | | |
| 26. | Implement and maintain a problem management process designed to manage In-Scope tools defects/failures | X | |

| Item | General Service Management | Contractor | Company |
|---|---|---|---|
| 27. | Perform problem identification and resolution consistent with the Service Levels. Develop short–term work-around as feasible and make this information available to the Service Desk | X | |
| 28. | Conduct and document a root cause analysis such as identification of the source of the problem) for high priority tickets | X | |
| 29. | Communicate root cause, work-around or process improvement plan to the applicable End Users and/or Service Desk; notify Company if a broadcast message to a large number of End Users is needed | X | |
| 30. | Participate with functional testing as applicable in support of In-Scope tools, database, or systems corrections to known or reasonably anticipated problems consistent with the problem management activities | X | |
| 31. | Recommend process improvements and implement agreed improvements that are identified in the root cause analysis | X | |
| 32. | Document problems and lessons learned for future improvement in the Company designated knowledge base | X | |
| 33. | Provide oversight and approval of root cause analysis. Also provide governance over RCA recommendations. | | X |
| | **Preventative Maintenance** | | |
| 34. | Recommend performance tuning improvements for In-Scope tools to improve the efficiency and reliability of programs or to minimize ongoing maintenance efforts | X | |
| 35. | Implement approved performance tuning improvements as agreed for In-Scope tools to improve the efficiency and reliability of programs or to minimize ongoing maintenance efforts | X | |
| 36. | Provide estimates of the effort for preventative maintenance | X | |
| 37. | Monitor and analyze Tickets to identify potential trends and problems | X | |
| 38. | Assess software patches for In-Scope tools and notify Company of their availability as appropriate | X | |
| 39. | Provide processes and/or reports to help identify areas where preventive maintenance might be performed to improve In-Scope tools efficiency and implement changes for improvement of the performance of the tools. | X | |
| 40. | At Company' request, assess the performance of tools or a modification prior to production installation of improvement processes as part of a plan that would be subject to the approval of Contractor and Company | X | |
| 41. | Utilize the Company pre-production environments when necessary to perform analysis to avoid potential issues or problems | X | |
| 42. | Identify and recommend solutions to job failures. When possible, remediate failures through work around, configuration parameter change, or other change that does not involve modification to In-Scope tools code | X | |
| 43. | Review and approve preventative and patch maintenance requests | | X |
| | **Disaster Recovery** | | |

| Item | General Service Management | Contractor | Company |
|---|---|---|---|
| 44. | Declare DR event for in-scope Services within Company environments | | X |
| 45. | Create Disaster Recovery Plan (DRP) for the in-scope systems | | X |
| 46. | Maintain Disaster Recovery Plan (DRP) for the in-scope systems | X | |
| 47. | Participate in Company' Disaster Recovery planning and test (tabletop exercises annually) | X | |
| 48. | Oversee the implementation of DR tests that pertains to Contractor scope of Services | X | |
| 49. | Execute the DR Plan as it pertains to Contractor's scope of Services | X | |
| 50. | Provide feedback on DR tests to system owners for Contractor scope of Services | X | |
| 51. | Verify the disaster recovery environment for Contractor Services | X | |
| | **Service Level Management (Refer Exhibit M – Service Level Methodology)** | | |
| 52. | Manage and maintain the service level management and reporting process across in-scope Services. | X | |
| 53. | Comply with service level management and reporting process, policies, notification and escalation procedures. | X | |
| 54. | Propose process and policy improvements through continual process improvement. | X | |
| 55. | Review and approve such process improvement initiatives. | | X |
| 56. | Implement and communicate such process improvements. | X | |
| 57. | Produce periodic Service Level reports. | X | |
| 58. | Monitor, measure, and collate service level performance data for in-scope infrastructure and applications and report the findings to the Company. | X | |
| 59. | Schedule and facilitate monthly reviews of target vs actual service levels. | X | |
| 60. | Identify actions and track to closure service levels below target when applicable. | X | |

**Table 28 General Service Management for PAM/Access Mgmt/Dir Services/Cert Management roles and responsibilities**

## Privileged Access Management Support

Table 30 outlines the roles and responsibilities of Company and Contractor.

| Item | Privileged Access Management | Contractor | Company |
|---|---|---|---|
| | **Privileged Access Management Support** | | |
| 1. | Provide information required to configure PAM account management policies including but not limited to approval requirements, password policies, and user access lists | | X |
| 2. | Create and modify account management PAM policies | X | |
| 3. | Configure and maintain password rotation policies | X | |
| 4. | Provide and approve changes to PAM password management policies | | X |
| 5. | Perform daily review of PAM account management errors and troubleshoot connectivity to managed systems | X | |
| 6. | Provide SSL certificates | | X |
| 7. | Maintain SSL certificates for PAM components | X | |
| 8. | Perform troubleshooting of issues with systems integrated with PAM including LDAPs (Lightweight Directory Access Protocols), mail servers, SIEM tool | X | |
| 9. | Provide support for troubleshooting issues with integrated applications and systems | X | |
| 10. | Coordinate with infrastructure support team and teams supporting the integrated systems for resolution of issues pertaining to integrations | X | |
| 11. | Submit ITSM requests for granting or revoking privileged user access to PAM | X | |
| 12. | Create, modify, and delete PAM Safes for granting end user access to privileged accounts | X | |
| 13. | Add, move, and delete accounts from PAM Safes for end user access to privileged accounts | X | |
| 14. | Prepare and submit applicable compliance control evidence as necessary per Company compliance requirements | X | |
| 15. | Deploy CyberArk Credential Provider (CP) agents | | X |
| 16. | Manage Just in Time provisioning policies for granting access to Contractor resources for support activities | X | |
| | **Privileged Administrators Onboarding** | | |
| 17. | Schedule and facilitate quarterly planning session to identify and prioritize accounts and systems for onboarding on to the PAM platform for systems leveraging out-of-the-box capabilities of PAM | X | |
| 18. | Participate in quarterly planning session and provide list of prioritized accounts and systems for onboarding | X | |
| 19. | Provide necessary information required to onboard accounts and systems into PAM (including but not limited to account names, server IP's, related services, and tasks) | X | |
| 20. | Provide access to test data to test account management policies | | X |
| 21. | Perform system and integration testing of account management policies | X | |
| 22. | Perform user acceptance testing of account management policies for accounts not managed by Contractor | | X |

| Item | Privileged Access Management | Contractor | Company |
|---|---|---|---|
| 23. | Participate and supervise user acceptance testing of account management policies for accounts | | X |
| 24. | Perform validation of privileged accounts, systems, applications, and service accounts post onboarding | X | |
| 25. | Define new PAM Policy requirements | | X |
| 26. | Validate PAM Policy Change requirements | X | |
| 27. | Approve PAM Policy Changes | | X |
| 28. | Implement and test approved PAM Policy Changes | X | |
| 29. | Roll back PAM Policy change if needed | X | |
| 30. | Provide existing Runbooks for PAM support | | X |
| 31. | Update, maintain, and create any new Runbooks | X | |
| 32. | Define escalation matrix in case of PAM incident | | X |
| 33. | Follow escalation matrix to highlight any major PAM incidents back to Company | X | |

**Table 30. PAM roles and responsibilities.**

## 3.1 Access Management, Directory Services and Certificate Management Support

Table 31 outlines the roles and responsibilities of Company and Contractor.

| Item | Access Management, Directory Services and Certificate Management | Contractor | Company |
|---|---|---|---|
| | **Access Management** | | |
| 1. | Provide list of Authentication and Authorization policies | | X |
| 2. | Troubleshoot issues related to User Access for integrated applications | X | |
| 3. | Resolve User Data issues pertaining to profile data | X | |
| 4. | Troubleshoot issues related to the group or access within the Access Management application or User Authentication repository | X | |
| 5. | Maintain integration guidelines for application integration with Access Management solution using (Simple Access Markup Language (SAML), OpenID Connect (OIDC), OpenAuthorization 2.0(Oauth2) agent based, and identity gateway integration methods | X | |
| 6. | Troubleshoot and fix issues related to application integrations using SAML, OIDC, OAuth2, agent based, and identity gateway integration methods | X | |
| 7. | Analyze incident trends on a monthly basis and suggest measures to improve Access Management Solution to reduce the volume of incidents | X | |
| 8. | Provide inputs to Contractor for deriving the list of access management rules | | X |
| 9. | Troubleshoot issues related to the identities within the Access Management environment Resolving User Data issues pertaining to Profile data being maintained by the Access Management and Multifactor Authentication (MFA) tool | X | |

| Item | Access Management, Directory Services and Certificate Management | Contractor | Company |
|---|---|---|---|
| 10. | Troubleshoot issues related to the group or access within the Access management environment | X | |
| 11. | Resolve issues with respect to policy violations for Access policies | X | |
| 12. | Troubleshoot and resolve issues with configuration for multi-factor authentication | X | |
| 13. | Resolve issues with configuration MFA policies | X | |
| 14. | Provide Minor Enhancements support for Access Management applications | X | |
| | **Access Management Onboarding** | | |
| 15. | Schedule and facilitate ongoing planning session to identify and prioritize In-Scope Applications for onboarding | X | |
| 16. | Participate in quarterly planning session and provide list of prioritized applications for onboarding according to agreed-on in-scope application complexity | | X |
| 17. | Schedule and facilitate meetings with application owners and stakeholders for In-Scope Applications for onboarding | X | |
| 18. | Provide list of necessary information required to onboard applications to the appropriate application owners and the Company stakeholders | X | |
| 19. | Provide necessary information required to onboard applications into Access Management tool (including but not limited to application URLs, Type of application, application attributes that need to be passed as part of authentication token, application server information, etc.) | | X |
| 20. | Onboarding of applications to Access Management Solution including activities such as build, test, and deploy | X | |
| 21. | Perform system and integration testing of integrated applications | X | |
| 22. | Coordinate and schedule user acceptance testing with the Company stakeholders | X | |
| 23. | Perform user acceptance testing | | X |
| 24. | Production deployment | X | |
| 25. | Perform validation of user access post-onboarding of applications | | X |
| 26. | Application support to application owners and contacts (onboarding kickoff, Frequently Asked Questions (FAQs), testing/validation) | X | |
| | **Certificate Management** | | |
| 27. | Root Certifying Authority (CA) certificate renewal | X | |
| 28. | Root CA certificate installation | | X |
| 29. | Review usage statistics for Certificate Management Solution to assess impact of increased usage on system performance on monthly basis | X | |
| 30. | Log requests for issuance of new certificates | X | |
| 31. | Maintain certificate book of records | X | |
| 32. | Validate new certificate issuance requests | X | |
| 33. | Approve or deny certificate requests | | X |
| 34. | Provide list of ‘owners’ responsible for issued certificates | | X |

| Item | Access Management, Directory Services and Certificate Management | Contractor | Company |
|---|---|---|---|
| 35. | Maintain list of 'owners' responsible for issued certificates | X | |
| 36. | Identify the application, user, and location of the newly discovered certificates | X | |
| 37. | Discovery of certificates leveraging Public Key Infrastructure (PKI) tool out-of-box capabilities | X | |
| 38. | Maintain certificate lifecycle for internal certificates leveraging PKI internal infrastructure | X | |
| 39. | Maintain certificate lifecycle for external certificates | X | |
| 40. | Coordinate with infrastructure and application teams for certificate installation on end devices | X | |
| 41. | Coordinate resolutions related to certificate installations on end user devices | X | |
| 42. | Monitor root and intermediate Certificate Authority (CA) validity times and ensure new certificates are generated before expiry | X | |
| 43. | Renew CA certificates assigned for root CA and issuing CAs | X | |
| 44. | Provide and maintain guidance material on how to obtain a certificate for end-users, applications, and services. | X | |
| 45. | Leverage PKI tool certificate discovery feature for onboarding of new certificates | X | |
| 46. | Identify all certificates with compliance issues across Company systems, including certificates expiring in 30/60/90 days | X | |
| 47. | Follow up with individual asset owners (listed in order of priority) and notify them that:<br>• The certificate is expiring in 30/60/90 days<br>• The certificate has an insufficient key size or cipher algorithm<br>• The certificate is already expired | X | |
| 48. | Provide asset owners with certificate request form and associated training materials and job aid to enable certificate remediation | X | |
| 49. | Provide support to application teams (if required) for certificate installation | X | |
| 50. | Remediate unmanaged or expired certificates | X | |
| 51. | Migrate certificates from one CA to another as required | X | |
| 52. | Analyze PKI related incidents, trends on a monthly basis and suggest measures to improve PKI Services Management solution to reduce the volume of incidents | X | |
| 53. | Resolve End User related issues as per agreed upon SLAs as set forth in Exhibit M – Service Level Methodology | X | |
| 54. | PKI service health check after patching | X | |
| | **Directory Services** | | |
| 55. | Provide regular reporting on environment performance against applicable service levels | X | |
| 56. | Perform Incident, Problem, and Change management as per agreed KPIs | X | |
| 57. | Perform problem management and root cause analysis | X | |

| Item | Access Management, Directory Services and Certificate Management | Contractor | Company |
|---|---|---|---|
| 58. | Troubleshoot issues related to the group or access within the company's directory | X | |
| 59. | Create new forests and domains within Active Directory | | X |
| 60. | Manage Active Directory forests, domains, and domain controllers | X | |
| 61. | Review and approve trust relationships | | X |
| 62. | Manage and maintain trust relationships with all domains | X | |
| 63. | New Schema design | | X |
| 64. | Promote and demote domain controllers | X | |
| 65. | Execute changes and modifications to schema | X | |
| 66. | Maintain security and integrity of schema | X | |
| 67. | Policy monitoring and compliance | X | |
| 68. | Organization Unit (OU)administration | X | |
| 69. | Ensure overall security and integrity of all managed OU hierarchies | X | |
| 70. | Coordinate with infrastructure support team for manual creation/deletion/management of objects, i.e., groups, workstations, servers, printers, etc. in the OU hierarchy | X | |
| 71. | Manage Directory Services (includes trusts, replication topology, etc.), OU hierarchies with standard sub-OUs, groups, and appropriate security permissions | X | |
| 72. | Manage and maintain Group Policy Objects (GPOs), Pre-Prod, Staging, and Prod GPOs | X | |
| 73. | Monitoring and reporting associated with domain reliability and security | X | |
| 74. | Monitor changes to domain root and domain controllers OU to ensure unauthorized changes do not occur | X | |
| 75. | Manage AD domains and trusts, OU management/delegation, manage group policies | X | |
| 76. | Publish resource objects from their OU hierarchy in the Active Directory as applicable | X | |
| 77. | Provide support for tickets related to user groups sync and Active Directory sync | X | |
| 78. | Troubleshoot issues related to Directory Schema | X | |
| 79. | Maintain roles and permissions in Active Directory | X | |
| 80. | Monitor and troubleshoot Active Directory Connect synchronization job failure issues | X | |
| 81. | Monitor Directory synchronization | X | |
| 82. | Analyze Directory Services management related incidents, trends on a monthly basis and suggest measures to improve Directory Services management solution to reduce the volume of incidents | X | |
| 83. | Execute approved technical changes for defect fixes | X | |
| | **Governance** | | |

| Item | Access Management, Directory Services and Certificate Management | Contractor | Company |
|---|---|---|---|
| 84. | Perform service strategic direction, oversight, and governance | | X |
| 85. | Manage joint organizational change management communications to Company and coordination | | X |
| 86. | Own, license, and manage OEM Vendor relationships for access management, certificate management, and directory services tools such as Microsoft | | X |

**Table 31. Access Management, Directory Services and Certificate Management roles and responsibilities.**

## Cloud Security

Table 32 outlines the roles and responsibilities of Company and Contractor.

| Item | Cloud Security | Contractor | Company |
|---|---|---|---|
| **Cloud Access Security Broker (CASB) Policy and Alert Management** | | | |
| 1. | **Configuration Baselining** | | |
| 2. | Auto discover or collect information on applications, platforms, device types, and locations on an ongoing basis (monthly if not automated) | X | |
| 3. | Validate information on applications, platforms, device types and locations | | X |
| 4. | Update CASB policy and rule baselines | X | |
| 5. | Review and approve CASB policies updated by Contractor | | X |
| 6. | Generate compliance violation / deviation reports | X | |
| **7.** | Review compliance violation / deviation reports | | X |
| 8. | Review and update of baselines as per on-going trend | X | |
| | **Policy Management** | | |
| 9. | Development and definition of Company use policy for CASB monitored applications/platforms/systems/devices | | X |
| 10. | Create/modify/tune/delete custom CASB policies subject to Company approval | X | |
| 11. | Test and monitor new/modified policies | X | |
| 12. | Grant approval to deploy policies | | X |
| 13. | Deploy and validate approved policies | X | |
| 14. | Provide documentation of policy updates | X | |
| 15. | Modify policy to add/remove/modify exception | X | |
| 16. | Approve policy exceptions | | X |
| 17. | Validate deployed policies | | X |
| 18. | Provide recommendations for CASB compliance and standards to be adhered to | X | |
| **Use Cases** | | | |

| Item | Cloud Security | Contractor | Company |
|---|---|---|---|
| 19. | Define new Use Cases for the CASB Solution | X | |
| 20. | Approve new Use Cases for deployment | | X |
| 21. | Develop, deploy, monitor and adjust new Use Cases | X | |
| 22. | Provide metrics in reports or dashboards, in a mutually agreed format | X | |
| **Alert Monitoring** | | | |
| 23. | Updating the in-scope Systems, platform types, locations and IP addresses | X | |
| 24. | Align the appropriate baseline with type of Systems prior to policy deployment | X | |
| 25. | Monitoring CASB alerts and Analysis | X | |
| 26. | Policy violation/deviation identification and Analysis | X | |
| 27. | Qualify the alerts based on severity, priority, pattern, occurrence and impact | X | |
| 28. | Notify stakeholders of the result of the alert Analysis | X | |
| 29. | Implement resolution activities | | X |
| **CASB Platform Support** | | | |
| | **CASB Integrations** | | |
| 30. | Configuration (Discovery, Application Programming Interface (API), agent distribution integration (existing 3rd party solutions like AD, SIEM, Data Loss Prevention (DLP)), and customization (views, feature enhancements) | X | |
| 31. | Support the Company's integration of new Log Sources (applications/platforms/systems/devices) into the CASB Solution by providing configuration information, instructions on how to integrate with the CASB Solution and responding to ad hoc questions | X | |
| 32. | Implement new Log Sources into the CASB Solution | | X |
| | **CASB Solution Management** | | |
| 33. | DLP dictionary and rules creation, maintenance and management | X | |
| 34. | Deploying target system agents | X | |
| 35. | Maintain inventory/list of agents deployed | X | |
| 36. | Periodic review of addition/deletion/modification of agents | X | |
| 37. | Tracking the agents' status (running/stopped) from CASB Solution management console | X | |
| | **Performance, Availability and Health Monitoring (as applicable)** | | |
| 38. | Implement performance, health and availability monitoring features as per vendor recommendations for given solution (out of the box functionality) | X | |
| 39. | Monitor alerts from the solution monitoring feature set | X | |

| Item | Cloud Security | Contractor | Company |
|---|---|---|---|
| 40. | Where Service is impacted, perform activities set out in the Runbook to react to the alert | X | |
| | **Performance Optimization** | | |
| 41. | Analyze application and configuration settings, policies & signature, historical performance data & provide recommendations | X | |
| 42. | Discuss and finalize recommendations with Company | X | |
| 43. | Fine tune the CASB Solution infrastructure parameters such as application and database settings | X | |
| 44. | Analyze performance data post-implementation | X | |
| 45. | Prepare and share performance optimization report | X | |
| **Secure Internet Access - Zscaler Internet Access (ZIA)** | | | |
| 46. | Manage and administer configuration/ policies on Zscaler Internet Access | X | |
| 47. | Create new URL policies, whitelist, blacklist websites, custom URL categories | X | |
| 48. | Modification of existing URL policies | X | |
| 49. | Adding websites in bypass i.e., SSL bypass etc. | X | |
| 50. | Troubleshooting for incident management through ZIA/Zscaler Digital Experience) ZDX functions | X | |
| 51. | Reviewing and troubleshooting existing URL policies for any defects | X | |
| 52. | Fine tuning of URL policies | X | |
| 53. | Re-ordering of URL policies | X | |
| 54. | Troubleshooting ZIA cloud connectivity issues | X | |
| 55. | Coordinating with vendor Technical Assistance Center (TAC) team for any troubleshooting | X | |
| 56. | Troubleshooting on end user systems and data center servers with respective Company support teams. | X | |
| 57. | Provide service report on weekly and monthly basis including service, change, incident and problem management tickets handled | X | |
| **Cloud Security Posture Management (CSPM)** | | | |
| 58. | Maintain process, procedures, documentation (including approach and strategy) | X | |
| 59. | Approve scope for CSPM monitoring | | X |
| 60. | Provide access to Company cloud infrastructure and CSPM solution | | X |
| 61. | Obtain permissions/consents from third party infrastructure providers for CSPM monitoring | | X |
| 62. | Provide complete and accurate list of cloud infrastructure to be monitored | | X |

| Item | Cloud Security | Contractor | Company |
|---|---|---|---|
| 63. | Define and configure CSPM monitoring to be run | X | |
| 64. | Manage and administer policies on CSPM | X | |
| 65. | Monitor the CSPM policy compliance violations | X | |
| 66. | Identify and remove false positives per process agreed in CSPM runbook and exceptions notified by Company and logged in CSPM runbook | X | |
| 67. | Establish appropriate risk to Company assets from identified vulnerabilities, and appropriately risk rank, in alignment with Company CSPM framework | X | |
| 68. | Investigate CSPM alerts related to cloud configuration compliance issues | X | |
| 69. | Provide remediation recommendations to address vulnerabilities and compliance issues | X | |
| 70. | Define and customize queries to support alert investigation | X | |
| 71. | Execute remediation of vulnerabilities identified in the Reports | | X |
| 72. | (When unable remediation a vulnerability) Initiate exception request | | X |
| 73. | Manage exception request/approval process | | X |
| 74. | Provide subject matter expertise (input and advice) when needed during the exception request/approval process | X | |
| 75. | Monitor Company approved vulnerability and compliance issue exceptions / Delineate vulnerabilities and compliance issues during reporting that have approved and active exceptions | X | |
| 76. | Make configuration changes to avoid recurring false positives and enhance the accuracy of the CSPM monitoring | X | |
| 77. | Recommend proper firewall rules /Intrusion Detection System (IDS)- Intrusion Protection System (IPS) exclusions to allow scan traffic between the CSPM tool and ensure access to the In-Scope Infrastructure (including where third party hosted) | X | |
| 78. | Implement proper firewall rules /IDS-IPS exclusions to allow scan traffic between the CSPM tool and ensure access to the In-Scope Infrastructure (including where third party hosted) | X | |
| **General Support** | | | |
| 79. | Enable appropriate access to Company-owned tools (e.g. integrations flows) including any necessary licenses | | X |
| 80. | Provide documentation regarding network devices, servers and applications for integration with CASB, Secure Internet Access, and CSPM solutions | | X |
| 81. | Provide license and OEM Support for CASB, Secure Internet Access, and CSPM solutions and obtain additional licensing (if required) | | X |
| 82. | Pay for any third-party software changes, including upgrades | | X |
| **License/ Subscription Monitoring** | | | |

| Item | Cloud Security | Contractor | Company |
|---|---|---|---|
| 83. | Monitor expiration date of CASB, Secure Internet Access, and CSPM solutions components | X | |
| 84. | Notify Company for license recovery/renewal whenever required | X | |
| 85. | Renew licenses/subscriptions as needed | | X |
| **CASB, Secure Internet Access, and CSPM solutions Fault Management (as applicable)** | | | |
| 86. | Handle fault notification | X | |
| 87. | Identify and classify fault | X | |
| 88. | Investigate and diagnose fault | X | |
| 89. | Resolve/escalate fault | X | |
| 90. | Implement temporary workarounds (as needed) | X | |
| 91. | Provide fault resolution | X | |
| 92. | Notify and escalate to Company management regarding a specific fault | X | |
| 93. | Broadcast notification to end users in case of a Service outage in accordance with agreed cross functional processes and procedures | | X |
| 94. | Update Helpdesk about the issue with approximate time of resolution | X | |
| 95. | Update management about the problem resolution | X | |
| 96. | Notify end users about the availability on service restoration in accordance with agreed cross functional processes and procedures | | X |
| 97. | Submit emergency Change Requests in accordance with ITIL emergency change process as documented in the Runbook | X | |
| 98. | Perform Root Cause Analysis and problem resolution | X | |
| 99. | Coordinate with product manufacturer or third-party vendor for bug/issue resolution | X | |
| **Backup and Restore** | | | |
| 100. | Provide backup solution and backup storage location | | X |
| 101. | Perform CASB, Secure Internet Access, and CSPM solutions health monitoring | X | |
| 102. | Perform backup of policies, signatures, configuration, and Reports as per mutually agreed schedule | X | |
| 103. | Verify backup operation and backup sets | X | |
| 104. | Recover configuration when needed | X | |
| 105. | Analyze impact of restoration and confirm if the restoration is complete, in case of database failure/corruption (management console) | X | |
| 106. | Provide audit trail of backup/restore processes | X | |

| Item | Cloud Security | Contractor | Company |
|---|---|---|---|
| **User Access Management** | | | |
| 107. | Create/remove/update user accounts for specified service solution | X | |
| 108. | Provide role-based access rights to users | X | |
| 109. | Document and track users' accounts currently active on specified service solution | X | |
| 110. | Approve Change Request(s) | | X |
| 111. | Track non-Lightweight Directory Access Protocol (LDAP) authenticated users/systems inventory and provide Company with non-LDAP users/systems IP address statistics | X | |
| | **Disaster Recovery** | | |
| 112. | Perform Disaster Recovery planning and maintenance | | X |
| 113. | Receive Company provided Disaster Recovery Plan, update Contractor processes to follow as the Disaster Recovery Plan is changed by Company | X | |
| 114. | Maintain Disaster Recovery configuration | X | |
| 115. | Monitor failover of primary vault to Disaster Recovery site | X | |
| 116. | Validate the Disaster Recovery environment | X | |
| 117. | Participate in Disaster Recovery testing and tabletop exercises as mutually agreed | X | |
| **Common Services (Cross-Functional)** | | | |
| **Service Management** | | | |
| | **Change Management** | | |
| 118. | Raise Change | X | |
| 119. | Analyze and review Change | X | |
| 120. | Manage Change communication and implementation | X | |
| 121. | Review post Change implementation | X | |
| 122. | Handle Change closure and notification | X | |
| 123. | Communicate CMDB/Knowledge Base updates | X | |
| 124. | Roll back if needed | X | |
| | **Problem Management** | | |
| 125. | Raise problem | X | |
| 126. | Analyze and review problem | X | |
| 127. | Work with various stakeholders for problem resolution | X | |
| 128. | Provide support and inputs to assists with problem resolution | | X |

| Item | Cloud Security | Contractor | Company |
|---|---|---|---|
| 129. | Perform Root Cause Analysis for problem | X | |
| **Reporting** | | | |
| | **Basic Reporting** | | |
| 130. | Configure and schedule reports as set forth in Exhibit Q – Governance and Reports | X | |
| 131. | Generate reports | X | |
| 132. | Analyze, verify and validate reports | X | |
| 133. | Provide distribution list for report delivery | | X |
| 134. | Generate and distribute mutually agreed service and operational metrics as per schedule | X | |
| 135. | Review reports and advise on adjustments on reports | | X |
| | **Advanced Reporting** | | |
| 136. | Define and design of reports | X | |
| 137. | Provide inputs for report development - criteria, format, content and layout | | X |
| 138. | Request custom report | | X |
| 139. | Propose time and effort estimate for the custom reporting | X | |
| 140. | Accept proposed time and effort estimate for the custom report | | X |
| 141. | Generate custom reports as agreed in accordance with Change Management | X | |
| 142. | Review and provide feedback for reports | | X |

**Table 32 Cloud Security roles and responsibilities.**

## 3.2 Firewall Management

Table 33 outlines the roles and responsibilities of Company and Contractor.

| Item | Firewall Management Services | Contractor | Company |
|---|---|---|---|
| | **Firewall Security Policy and Rule Administration** | | |
| 1 | Receive and validate (pre-change) change requirements standard/emergency Firewall Policy change requests | X | |
| 2 | Approve Firewall Security rules/ Policy request | | X |
| 3 | Implement Firewall rules based on the request | X | |
| 4 | Validate changes performed post change implementation | X | |
| 5 | Participate in Firewall rule break/fix to provide any needed guidance / documentation or clarifications | | X |

| Item | Firewall Management Services | Contractor | Company |
|---|---|---|---|
| 6 | Review and remove temporary firewall rules (time-bound rule bases) in a timely manner as required. The time bound rules to follow Company's naming convention | X | |
| 7 | Configure logging level as per Company's Enterprise Security Standards, and extract the Reports when required | X | |
| 8 | Follow standard operating procedures for firewall rule administration | X | |
| 9 | Perform Quarterly review for process documents | X | |
| 10 | Perform and test scheduled rule changes on time | X | |
| 11 | Perform firewall rules review Annually and establish remediation plan in accordance with PPL Enterprise Security Standards | X | |
| 12 | Prepare and share monthly report on Rule review covering progress on mitigation completed, with trends on improvement as set forth in Exhibit Q – Governance and Reports | X | |
| | **Network Intrusion Protection – Monitoring and Analysis** | | |
| 1 | Ensure all perimeter Firewall device are enabled with Intrusion Prevention System (IPS)/Intrusion Detection System (IDS) function wherever applicable | X | |
| 2 | Enforce security profiles (Antivirus, Antimalware, Vulnerability) to each firewall rule | X | |
| 3 | Monitor for intrusion activity to identify, alert, classify and escalate as necessary via the Incident Response process | X | |
| 4 | Update signatures released as per periodic schedule from vendor or on ad hoc basis | X | |
| 5 | Review, and maintain up to date signatures and provide weekly status report as set forth in Exhibit Q – Governance and Reports | X | |
| 6 | Collaborate with Company during intrusions and in relation to subsequent remediation activities and Root Cause Analysis activities | X | |
| 7 | Provide threat monitoring and response support | X | |
| | **Patch Management** | | |
| 1 | Monitor and identify patching requirements | X | |
| 2 | Analyze and assign patch priority/send security alert for fixes | X | |
| 3 | Conduct test for patch | X | |
| 4 | Follow Change/Release management process | X | |
| 5 | Approval for patch deployment (through Change Management Process) | | X |
| 6 | Deploy the patches | X | |
| | **Incident Management** | | |
| 1 | Identify and classify Incident | X | |

| Item | Firewall Management Services | Contractor | Company |
|---|---|---|---|
| 2 | Investigate and diagnose Incident | X | |
| 3 | Provide Incident resolution | X | |
| 4 | Submit Standard Change Request and Emergency Change Requests (ECR) | X | |
| 5 | Follow Company's incident review process including root cause analysis, Post-mortem review as part of Incident management | X | |
| 6 | Provide issue remediation wherever possible to bring business back to normal with minimum downtime and resolve the problem | X | |
| 7 | Notify and escalate to Company management regarding all Incidents as required depending on the incident severity classification | X | |
| 8 | Broadcast notification to end users in case of a service outage in accordance with agreed cross functional processes and procedures | | X |
| 9 | Update Helpdesk about the issue impact and approximate time of resolution | X | |
| 10 | Update management about the incident scope of impact and resolution | | X |
| 11 | Notify end users about the availability on service restoration in accordance with agreed cross functional processes and procedures | | X |
| 12 | Raise support ticket with product vendor for support whenever required | X | |
| 13 | Provide a list of inventories with model information, location, contact person, contract details, etc., to use as a spare device in times of Disaster Recovery | | X |
| 14 | Confirm any planned maintenance activity resulting in any downtime to services is well planned, communicated and duly approved | X | |
| 15 | Coordinate RMA Return Merchandise Authorization process with product manufacturer or third-party vendors for any device replacement | X | |
| 16 | Follow the Company process to support any movement of devices in and out of the datacentre | | X |
| 17 | Provide physical onsite support (hands & feet) for any hardware replacements and initial device configuration, at Company locations | | X |
| 18 | Provide configuration support for remote/out of band access to Firewalls | X | |
| 19 | Perform regular review and test on Out of Band (OOB) connectivity for all infrastructure security devices | X | |
| 20 | Provide appropriate access to Firewall devices for Contractor resources | | X |
| 21 | Provide necessary documentation regarding network security landscape | | X |
| | **Backup and Restore management** | | |
| 1 | Manage and maintain existing Company documented technical backup, recovery, retention strategy and process | | X |
| 2 | Perform backup operation | X | |

| Item | Firewall Management Services | Contractor | Company |
|---|---|---|---|
| 3 | Maintain and update backup scripts and schedules | X | |
| 4 | Logging and alerting of all backup operations | X | |
| 5 | Test backup and recovery strategy once a year, or as agreed, and provide a formal report on the test results and the overall Business Continuity exercise consistent with the Service Description for Common IT Services and the Agreement. As set forth in Exhibit Q – Governance and Reports | X | |
| 6 | Perform data restoration from the backup and perform backup and archive test recoveries | X | |
| 7 | Implement access controls around backup data | X | |
| 8 | Follow access controls on backup data | X | |
| 9 | Provide location/facility to store backup data for Firewall Devices | | X |
| | **Disaster Recovery** | | |
| 10 | Perform disaster recovery planning and maintenance | | X |
| 11 | Receive Company provided Disaster Recovery plan, update Contractor processes to follow as the disaster recovery plan is changed by Company | X | |
| 12 | Maintain Disaster Recovery configuration | X | |
| 13 | Monitor failover of primary infrastructure service to Disaster Recovery site | X | |
| 14 | Validate the Disaster Recovery environment | X | |
| 15 | Validate access to the Disaster Recovery environment | X | |
| 16 | Participate in Disaster Recovery testing and tabletop exercises as mutually agreed | X | |
| | **General Support** | | |
| 17 | Implementation of hardware refresh for End of Life (EOL)/End of Support (EOS)devices under existing architecture, in case the efforts as mutually agreed are within 40 hours per month would be performed as Business as Usual (BAU) | X | |
| 18 | Manage the infrastructure security devices per vendor's and Company 's best practices | X | |
| 19 | Obtain additional licensing (if required), and manage existing licensing agreements | | X |
| 20 | Manage licenses for in-scope security components including tracking of expired license | X | |
| 21 | Manage and provide monthly report on the infrastructure security device lifecycle management as set forth in Exhibit Q – Governance and Reports | X | |
| 22 | Provide hands and feet support for any hardware replacements, racking and stacking, cabling, etc., in Company facilities | | X |

| Item | Firewall Management Services | Contractor | Company |
|---|---|---|---|
| 23 | Ensure firewalls are configured to forward logs & delivered to SEIM | X | |
| 24 | Prepare and share weekly reports on incidents, trend analysis, changes performed. Recommended continuous improvements as required as set forth in Exhibit Q – Governance and Reports | X | |
| 25 | Monthly infrastructure security reports detailing incidents, changes, vulnerabilities identified, Patch status, continuous service improvement opportunities and remediation efforts. as set forth in Exhibit Q – Governance and Reports | X | |
| 26 | Review and provide feedback for reports | | X |

**Table 33.** Firewall Management roles and responsibilities

## Application Security

Table 34 outlines the roles and responsibilities of Company and Contractor.

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| **Application Security Testing – SAST, SCA, DAST** | | | |
| 1. | Provide overview of the application functionality, application architecture, technology used, data criticality and application criticality for each of the In-Scope Web Applications (Attachment C-1) | | X |
| 2. | Study application documentation to understand the design and functionality of the application and application walk through to understand the flow | X | |
| 3. | Provide application owner, code base, IP address, URL, login credentials and special access (if required) for each In-Scope Web Application | | X |
| 4. | Provide any functional test data required for an application flow | | X |
| 5. | Provide the parameters for scan schedule, any special configuration required for the scan, and scan policy to be applied | | X |
| 6. | Perform scan configuration and scheduling according to Company provided scan policies and parameters | X | |
| 7. | Provide recommendations to Company for modifications to scan for improving outcomes and providing less false positives | X | |
| 8. | Review and approve recommendations provided by Contractor | | X |
| 9. | Provide list of application and infrastructure team contacts | | X |
| 10. | Send the scan notification to Company infrastructure and application teams | X | |
| 11. | Tracking and Remediation of Vulnerabilities identified in the application including validation assessment as part of quarterly scanning schedule and process, coordinate entry into PPL's Risk registries | X | |
| 12. | Review and enter application security testing entries in the Risk registry | | X |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| 13. | Reports as set forth in Exhibit Q – Governance and Reports | X | |
| 14. | Coordinate with appropriate business stakeholders within Company regarding scan and scan schedule | X | |
| 15. | Identify an emergency point of contact to resolve any issues that may arise during the scan | X | |
| 16. | Confirm resources and application URLs are accessible | X | |
| 17. | Perform Application Security Scanning | X | |
| 18. | Troubleshoot any issues with scan progress | X | |
| 19. | Provide software license for application security scanning tool | | X |
| 20. | Request for ad hoc scans/rescans | | X |
| 21. | Effort assessed for ad hoc scans or rescans | X | |
| 22. | Ad hoc scans/ rescans performed based on approval | X | |
| **Reporting** | | | |
| 23. | Provide Tool generated scheduled reports (e.g., number of events, trending analysis, etc.) as set forth in Exhibit Q – Governance and Reports | X | |
| 24. | Submit tickets quarterly into Company's ITSM tool to resolver groups (or send emails quarterly to 3rd party URL owners who are not using Company's ITSM tool) for discovered out-of-compliance vulnerability remediation or risk exception submission in accordance with Company 's vulnerability management processes | X | |
| 25. | Provide list of stakeholders to whom the reports will be distributed by Contractor | | X |
| 26. | Request ad-hoc report | | X |
| 27. | Custom or ad hoc reports review and development as part of the monthly Minor Enhancement Hours Pool | X | |
| 28. | Provide application architecture, design, and key business requirements walkthrough for conducting Application Security testing | | X |
| 29. | Remediation tracking and guidance for Application Security scans | X | |
| 30. | Allow Contractor to access and provide necessary pre-requisites to run the app sec scans | | X |
| 31. | Provide access to required applications, URL's and security tools to conduct the assessment/testing | | X |

**Table 34. Application Security Support roles and responsibilities.**

## Penetration Testing

Table 35 outlines the roles and responsibilities of Company and Contractor.

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| **Penetration Testing** | | | |
| 1 | Agree on the approach of the penetration test, define trophies and targets | X | X |
| 2 | Provide overview of the application functionality, application architecture, technology used, data criticality and application criticality for each of the In-Scope Web Applications (Attachment C-1) | | X |
| 3 | Study application documentation to understand the design and functionality of the application and application walk through to understand the flow | X | |
| 4 | Identify emergency point of contact to resolve any issues that may arise during the penetration test | X | |
| 5 | Provide the network connectivity to targets in scope Virtual Private Network (VPN), internet, jump host, etc.) | | X |
| 6 | Provide application owner, Internet Protocol (IP) address, Universal Resource Locator (URL), login credentials and special access (if required) for each In-Scope Web Application (Attachment C-1) and IP Addresses | | X |
| 7 | Confirm all prerequisites are delivered and the application URLs are accessible | X | |
| 8 | Notify Company SOC team about penetration testing activity and whitelist the source IPs. Ensure the traffic will not be blocked by any Company device | | X |
| 9 | Provide any third-party approvals (Amazon Web Services (AWS), Microsoft Azure, etc.) and final approval of the requestor | | X |
| 10 | Provide any functional test data required for an application flow | | X |
| 11 | Provide the suitable time window to perform the penetration test | | X |
| 12 | Schedule the penetration test and identify resources to perform the test | X | |
| 13 | Send notification about the penetration test start to Company infrastructure and application teams | X | |
| **Execution & Reporting (Refer Exhibit Q- Governance and Reports)** | | | |
| 14 | Perform the penetration test | X | |
| 15 | Send weekly status update on penetration test progress and identified vulnerabilities | X | |
| 16 | Document findings in agreed upon format, with the following elements<br>• Executive summary<br>• Exploitation path for each vulnerability found<br>• Remediation recommendation | X | |
| 17 | Provide final reports | X | |
| 18 | Provide list of stakeholders to whom the reports will be distributed by Contractor | | X |
| **Remediation Support** | | | |
| 19 | Provide inputs and guidelines to development team on options to fix reported vulnerabilities | X | |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| 20 | Fix the vulnerabilities | | X |

**Table 35 Penetration Testing roles and responsibilities**

## Security Engineering as a Service

Table 36 outlines the roles and responsibilities of Company and Contractor.

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| **Platform support and Engineering for Proofpoint; Abnormal; Fortify Security Center** | | | |
| **System Administration** | | | |
| 1. | Define standards and policies for In-Scope Security Tools as defined in Section 2.12 of this Exhibit | | X |
| 2. | Define and deploy required configuration parameters for In-Scope Security Tools in accordance with the Runbook | X | |
| 3. | Evaluate and tune configurations for In-Scope security Tools in accordance with the Runbook | X | |
| 4. | Perform activities set out in the Runbook to react to the outputs/ information provided from the management console of the In-Scope Security Tools and In-Scope Infrastructure | X | |
| **Availability and Health Monitoring** | | | |
| 5. | Provide software to monitor availability of the In-Scope Security Tools | | X |
| 6. | Monitor alerts from the In-Scope Security Tools related to availability | X | |
| 7. | Where availability is impacted, perform activities set out in the Runbook to react to the availability alert | X | |
| **Patch Management for the In-Scope Applications** | | | |
| 8. | Identify, analyze and prioritize patches | X | |
| 9. | Conduct testing for each patch | X | |
| 10. | Follow Change/Release Management process | X | |
| 11. | Approve Changes in accordance with the Change/Release Management process | | X |
| 12. | Deploy the patches | X | |
| **Fault Management** | | | |
| 13. | Identify and classify faults in the In-Scope Security Tools | X | |
| 14. | Notify Company of faults using the ITSM and escalation process in the Runbook | X | |
| 15. | Investigate and diagnose faults in the In-Scope Security Tools | X | |
| 16. | Resolve/escalate faults outside the In-Scope Security Tools | | X |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| 17. | Resolve/escalate faults in the In-Scope Security Tools | X | |
| 18. | Perform Root Cause Analysis and problem resolution in the In-Scope Security Tools | X | |
| 19. | Coordinate with product manufacturer or third-party vendor for issue resolution in the In-Scope Security Tools | X | |
| 20. | Develop communication about the availability on service restoration and to be shared with Company for notifying the end users | X | |
| 21. | Notify end users about the availability on service restoration in accordance with agreed processes | | X |
| **Backup and Restore Management** | | | |
| 22. | Perform backup operation of In-Scope Security Tools | X | |
| 23. | Verify backup operation | X | |
| 24. | Perform restoration from the backup | X | |
| 25. | Provide location/facility to store backup data and solution to perform backup operations | | X |
| **Disaster Recovery** | | | |
| 26. | Develop and maintain Disaster Recovery Plan | | X |
| 27. | Provide input into and approve application of Disaster Recovery Plan to the Security Tools and Infrastructure Management Services | X | |
| 28. | Build and maintain Disaster Recovery infrastructure | | X |
| 29. | Participate in Disaster Recovery planning and exercises | X | |
| 30. | Follow the Disaster Recovery Plan if implemented | X | |
| **General Support** | | | |
| 31. | In-Scope Security Tools list administration, including granting people access to the console/removing access | X | |
| 32. | Enable appropriate access to Company-owned tools including any necessary licences | | X |
| 33. | Provide bandwidth, virtual or physical hardware and storage for the In-Scope Security Tools list | | X |
| 34. | Provide license and OEM Support for In-Scope Security Tools and obtain additional licensing (if required) | | X |
| 35. | Pay for any third-party software changes, including upgrades | | X |
| **Reporting (Refer Exhibit Q – Governance and Reports)** | | | |
| 36. | Provide scheduled statistical Reports (e.g., number of events, trending analysis, etc.) | X | |

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| 37. | Provide list of stakeholders to whom the reports will be distributed by Contractor | | X |

**Table 36 Security Engineering as a service roles and responsibilities**

## Third Party Risk Management

Table 37 outlines the roles and responsibilities of Company and Contractor.

| Item | Responsibility | Contractor | Company |
|---|---|---|---|
| **Third Party Risk Assessment** | | | |
| 1 | Provide inventory of Third Parties | | X |
| 2 | Define and update the Third-Party Risk Assessment Framework (TPRM) | | X |
| 3 | Perform TPRM assessments for the vendors in scope for that month as per Company's TPRM framework | X | |
| 4 | Identify risks based on the assessments | X | |
| 5 | Review assessment reports | | X |
| 6 | Discuss and align the remediation plan for the identified gaps along with the vendor | X | |
| 7 | Define Findings Log requirements and processes to track gaps identified in Third party vendor risk assessments, | X | |
| 8 | Track the remediation monthly and report to Company as set forth in Exhibit Q – Governance and Reports | X | |
| 9 | Provide required evidence support during assessment | X | |
| 10 | Provide risk assessment report based on findings including identified gaps and recommendations | X | |
| 11 | Provide advisory support for remediation of gaps | X | |
| | Update the workflows in the Vendor Risk Management (VRM) tool to optimize the assessment process (1 workflow per quarter) | X | |
| 12 | Perform re-assessment post fixing of gaps | X | |
| 13 | Submit report for re-assessment to Company | X | |
| 14 | Review and approve report post closure of gaps | | X |

**Table 37 Third Party Risk Management roles and responsibilities**