# SCHEDULE B

CLOUD OPERATION SERVICES

# INTRODUCTION

This Schedule B to the SOW (“Schedule B” or “Cloud Operation Service Tower”) sets forth the services that Vendor will provide to Brighthouse and the Authorized Users related to Cloud Operation Services as described herein and in the related attachmeCnts (the “**Cloud Operation Services**”), which shall be considered Services under the Agreement. Vendor will assume full responsibility for performing all Cloud Operation Services upon completion of Transition. Vendor will provide the Cloud Operation Services in accordance with the Service Levels and other requirements set forth in the SOW and the Agreement, and Vendor will periodically evaluate opportunities to move to a higher operational service maturity.

Brighthouse’s environment will be supported with services aligning to processes compliant with the ITIL framework.

# DEFINITIONS

Any terms used but not defined in this Schedule B (Cloud Operation Services) have the meanings given to them in the SOW or elsewhere in the Agreement. As used in this Schedule B, the following abbreviated terms have the meanings set forth below:

|  |  |
| --- | --- |
| Abbreviation | Terminology |
| 3rd Party Product Vendor | Product Vendors whose product / application software is used by Brighthouse |
| 3rd Party Vendor | IT Vendors currently providing service to Brighthouse |
| CMDB | Configuration Management Database |
| CMS | Configuration Management System |
| IMACD | Installations, moves, adds, changes and de-installation |
| IMACs | Installation, Moves, Adds and Changes |
| ITIL | Information Technology Infrastructure Library |
| ITSM | Information Technology Service Management |
| OEM | Original Equipment Manufacturer |
| OS | Operating System |
| RACI | Responsible Accounted Consulted Informed Matrix |
| BAU | Business As Usual |
| KPI | Key Performance Indicator |
| KT | Knowledge Transfer |
| ServiceNow | Brighthouse’s ITSM as of the SOW Effective Date. |
| AWS | Amazon Web Services |
| GCP | Google Cloud Platform |
| MW | Middleware |
| KEDB | Known Error Database |
| HA | High Availability |
| DR | Disaster Recovery |
| AD | Active Directory |
| CI/CD | Continuous Integration / Continuous Deployment |
| WAN | Wide Area Network |
| ECX | Equinix Cloud Exchange Platform |
| SIEM | Security Information and Event Management |
| SIAM | Service Integration and Management |
| NOC | Network Operations Center |
| SMB | Server Message Block |
| ADFS | Active Directory Federation Services |
| NTFS | New Technology File System |
| FSMO | Flexible Single Master Operation |
| CPU | Central Processing Unit |
| RAM | Random Access Memory |
| SDLC | Software Development Lifecycle |
| SaaS | Software as a Service |

# DETAILED DESCRIPTION OF CLOUD SERVICES

Under this Schedule B, as part of the Cloud Services, Vendor shall provide the Cloud management services as set forth herein. The activities that Vendor will perform as part of the Cloud Services include the following.

**Cloud BAU Services Scope**

| Service Tower | Scope of Services |
| --- | --- |
| Cloud Operations | * Provide Level 2(L2) and Level 3 (L3) Cloud Operations Support * Remote Troubleshooting and resolving L2 & L3 Incidents * Track and ensure timely closure of tickets and create reports as required * Raises Change Request if required to facilitate the Incident resolution (workaround) * Troubleshoots complex problems that incumbent’s Level 1 engineers are unable to resolve. * Provide technical and process support, advice and direction to incumbent’s Level 1 Agents and Level 1.5 in providing Incident Management and Change Management activities for Authorized Users. * Perform Root cause analysis * Problem management and troubleshooting * Performance and availability management of Cloud environment * Performing operational planning for capacity and performance purposes. * Prepare and submit Change Requests for Brighthouse approval * Implementation of Changes after approval from the Brighthouse. * Patch installation and management wherever required in the Cloud environment * Maintain documentation, auditing and record-keeping. * Perform health checks * Vendor coordination and assist Brighthouse for Vendor management * Support for Disaster Recovery environments and activities using Cloud Native tools. * Annual DR test for the core infrastructure coordinating with BHF and for others it is based on critical application requirements. * Leverage Brighthouse toolsets to provide Cloud Operations |
| Technology Scope | * Microsoft Azure (Azure) and Amazon Web Services (AWS) environment support * Support cloud subscriptions * Cloud Operations Support as mentioned above * Cloud storage utilization monitoring and report * Azure Shared Drive Services * Active Directory * Windows/Linux Server Support & Server Management * SQL Support & Maintenance * Coordination with third party vendors * Cloud Cost management (after Azure Cost Management is implemented as part of transformation program)   *RedHat Open Shift clusters, nodes*   * Platform support * Coordination with third party vendors |

**Out of Scope:**

* Service Desk & Call center support
* Level 1 (L1) Support
* L1 Monitoring
* Any Smart hands or Hands & Feet support
* Service Management Office
* ITSM Process Ownership
* Any support for IBM SoftLayer

**3.2 In Scope Technology & Baseline Volumes:**

Following are the in scope baseline volumes considered for support. Changes to the baseline volumes

| **Service Line Items** | **Details** |
| --- | --- |
| Azure regions | US East and US West |
| AWS regions | US East 1 |
| Azure: Windows - Prod, UAT, Test (Server Images) | 65 |
| Azure: Windows – Dev (Server Images) | 9 |
| Azure: Linux - Prod, UAT, Test Server Images | 0 |
| Azure: Linux – Dev | 1 |
| Azure AD servers | 18 |
| Windows 2016 Web Application Proxy for ADFS | 6 |
| Windows PKI servers | 4 |
| Azure File Server Size in TB | 16 |
| Azure Loadbalancer | 12 |
| AWS: Windows - Prod, | 25 |
| AWS: Windows - Non Prod | 29 |
| AWS: Linux – Prod | 9 |
| AWS: Linux - Non Prod | 11 |
| AWS Windows SQL Instance | 7 |
| AWS Linux DB instance | 3 |
| AWS Loadbalancer | 12 |
| AWS Storage burst capacity – TB | 50 |
| VMs to be supported after migration from Softlayer to Azure (PKI Server) by 3rd Party Vendor | 4 |

Tools to be used for Cloud Operations Support:

Vendor will leverage the below existing Toolsets with BHF to provide Cloud Operations Support.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Functionality** | **Functionality Ownership** | **Current Tool** | **Future Tool\*** | **Current Tool Ownership** | **Future Tool Ownership** |
| Cloud Monitoring | Vendor | AWS CloudWatch, Azure Monitor | AWS CloudWatch, Azure Monitor | BHF | BHF |
| OS, DB Monitoring | Vendor | Zabbix | Zabbix | BHF | BHF |
| Server, DB Backup | Vendor | Cloud Native Backup | Cloud Native Backup | BHF | BHF |
| Windows Server Patch Management | Vendor | IBM Big Fix | Microsoft SCCM | BHF | BHF |
| Linux Server Patch Management | Vendor | Red Hat Satellite | Red Hat Satellite | BHF | BHF |
| Cloud Economics | Vendor | - Not available- | Azure Cost Management | NA | BHF |
| Cloud Management Platform (CMP) | Vendor | - Not available- | ServiceNow CMP | NA | BHF |

\*Any future tool implementation is not part of BAU support unless it is part of Transformation scope.

## **Deliverables:**

## The following are the deliverables as part of the Cloud Operations scope of Support.

## Cloud Operations Support Services as part of the agreed scope, coverage and service level agreement\*

## Cloud Operations Support Services reporting (Reports to be provided to be mutually agreed between Brighthouse and Vendor)

## All deliverables will be effective post transition phase.

## \*Service level agreement as per Attachment A-1.

# Cloud Support Operating Model (Operations View)

## The operating model of the Cloud Operations Support Services consists of

## Resourcing

## 3rd Party Support

## Support Coverage

## Tools

## **4.1 Resourcing**: Vendor will provide resources to provide agreed services in an onshore – offshore support model. Overall resourcing model consist of

## ***Integrated Operations team***: This is a Level 1.5 (L1.5) common shared team covering Network, EUC and Cloud Operations typically taking care of coordination, Reporting, assigned tickets tracking and follow up with SME, overall tracking, activity continuity to closure. This team will attempt to resolve the issues only based on Standard Operating Procedures (SOP). If they are not able to resolve, resolution will be provided by core SME team in the next support coverage window except for P1 and P2 tickets where the on call support will be invoked. The Integrated Operations team will be based out of Offshore.

## ***Cloud Architect & SME Support***: Onsite resource will play the role of Lead SME plus Architect. Offshore support will have SMEs.

## All resources at onshore and offshore will resolve tickets, participate in discussions (based on their shift availability). Onshore resource will be the front facing and go-to resource for any tower specific activities and queries. In case of onshore non-availability, Brighthouse can reach offshore resource as well.

## **4.2 3rd Party Support:** In addition to the scope of support, Vendor will provide required 3rd party vendor coordination support.

## **4.2 Support Coverage**: Support coverage Vendor will provide resources to provide agreed services in an onshore – offshore support as per the shift coverage model given in the Shift coverage section of this document.

## **4.2 Tools:** The set of tools that will be used by Vendor resources to provide Cloud Operations Support is given in Tools subsection above.

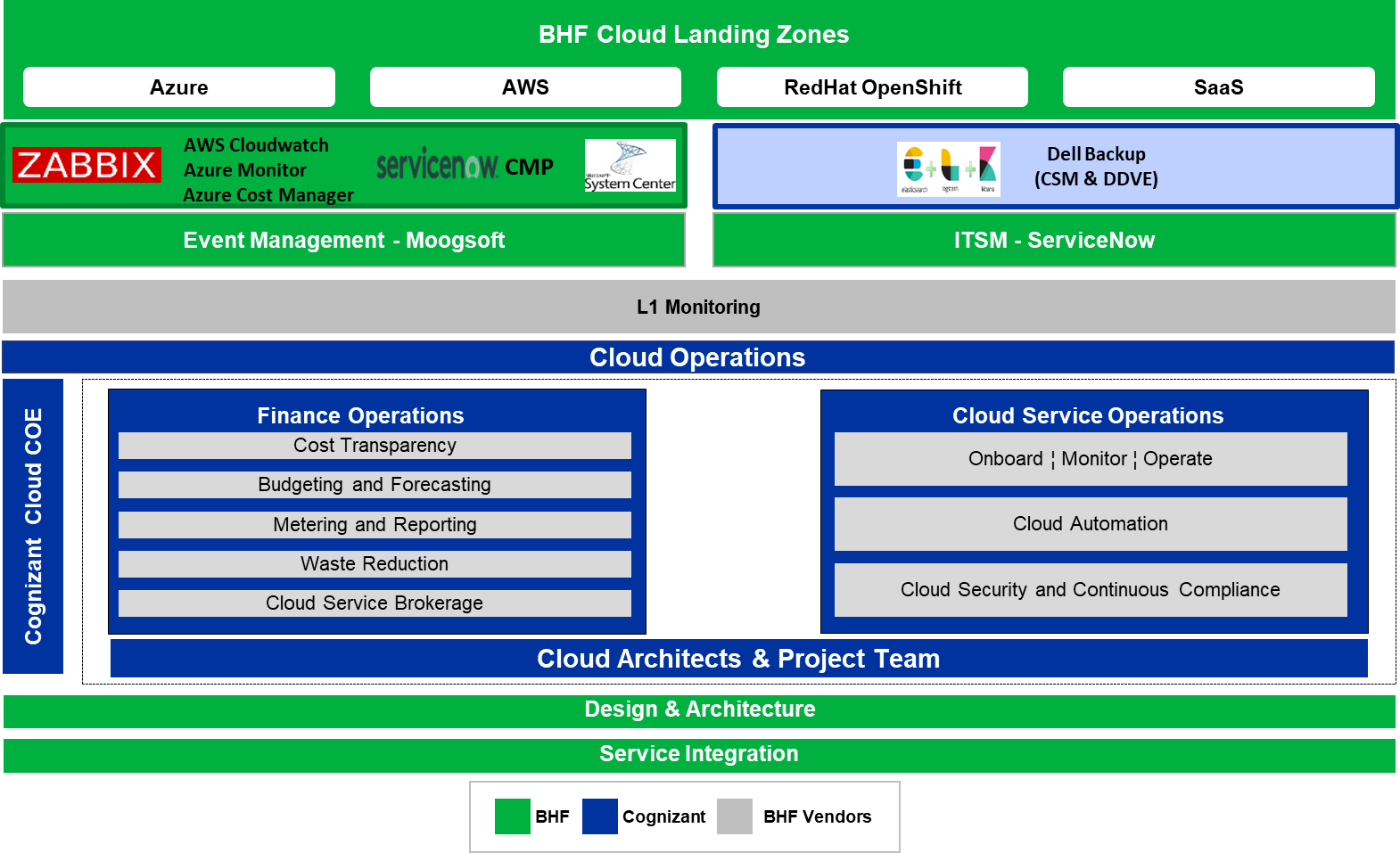
# Cloud Support Operating Model (Technology View)

Vendor’s Cloud Operation Services will provide support for end to end Cloud Managed Services for Brighthouse’s IaaS environment at Azure, AWS and Red Hat. The proposed Cloud Operation Services are built upon three distinct pillars of Governance – Cloud Financial office, Cloud Service Management Office, and Cloud Strategy Office.

**Cloud Strategy Office**: Brighthouse will retain the design, strategy of infrastructure services. Vendor will actively assist Brighthouse with the decision making process by providing cloud industry trends, published information from Azure, AWS related to in-scope services, architecture recommendation from Core Cloud Group formed within Brighthouse support framework.

**Cloud Financial Service**: Vendor will manage Brighthouse’s cloud subscription accounts of Azure & AWS on behalf of Brighthouse. Azure Cost Management will be leveraged to provide a monthly reports of cloud infrastructure utilization, optimization recommendation covering cloud services across Azure and AWS.

**Cloud Service Management**: As with other pillars, Cloud service management consists of people, process and tools perspective to carry out day to day cloud operations, continuous service optimization and standardize the cloud service elements within Brighthouse.



The cloud support structure has three layers of support resources and will work collaboratively with specialized support resources.

**Integrated Operations Team**: As specified in the operations view above.

**Cloud SME**: Cloud SME will execute the standard cloud operations including proactive diagnosis, operating system support, AD group management & support, Azure file services, backup services support, cloud services management and tracking/generating workload utilization reports.

**Cloud Lead/Architect**: Cloud expert /architect will have subject matter technology expertise across public, private cloud services. The expert layer of resources’ responsibilities include technical assistance on major cloud issues, RCA, plan and implement cloud service level changes, identifying automation opportunities, workflow creation and provide architectural recommendations to Brighthouse.

Cloud Projects Team: Project related activities are covered in a separate Schedule.

**Tools**: Tools utilized for support is given in the Tools section above.

The supported technologies within Brighthouse is listed in subsequent sections

**General Cloud Operations**: Brighthouse‘s IaaS environment includes Azure, AWS public cloud services and dedicated hosting in Open Shift. Brighthouse public cloud services is hosted across multiple regions for high availability, DR requirements. Vendor’s support for Brighthouse Cloud computing covers Azure, AWS cloud services in multiple regions, availability zones with HA, DR setup.

**Windows, Linux OS management**: Brighthouse has 95% Windows and 5% Linux servers in the environment, for which Vendor will provide OS management, OS standardization, patch update and health check, monitoring resource usage.

**Azure file services**: Vendor will support the Azure file server environment. The environment currently has 16TB size of data. The support tasks include manage Azure file server, SMB server, handling file server access requests, data backup and restore, security scanning.

**Active Directory**: Brighthouse’s active directory environment includes AD servers in Azure AD and in private cloud hosted AD servers. Vendor’s support includes AD maintenance per Brighthouse policy, maintaining high availability, resiliency, managing group policies and assisting in integration with Savyint access management system.

**SQL Server Support**: Brighthouse has MS SQL server databases in Azure and AWS cloud. Vendor’s support includes SQL server maintenance, database backup, and integrity checks, performance validation, availability.

**OpenShift Support**: Brighthouse leverages an IaaS in private cloud setup at Red Hat hosted environment. The open shift platform consists of 2 clusters and 24 nodes. It hosts custom developed applications. Vendor’s support includes platform support, vendor co-ordinate for hosting issues.

# General Assumptions

## Changes to the technology scope than what is mentioned in the scope section in this document could require changes to the effort and pricing. This will be mutually discussed between Brighthouse and Vendor

## Incumbent L1 support team will make every effort to resolve Incidents at first level (First level resolution – FLR) before they are escalated to L2/L3 support.

1. Vendor will leverage the existing ServiceNow as ITSM solution which will act as a single source of truth for all IT incidents and services requests
2. Onshore resources will be provided with required and adequate infrastructure (seat, phone, common printer)
3. Support during declared BCP situations will be on best effort basis. Vendor will make every effort to meet the agreed Service level agreement
4. During declared BCP situations, Vendor requires RTO of minimum of 24 hours.

# RACI Matrix

The following RACI matrix for Cloud Services describes which party is

A – Accountable, R – Responsible, C – Consulted, I – Informed for each task/function described herein.

| **ID** | **Requirement Description** | **Vendor Comments (If applicable)** | **BHF** | **ITSM** | **Network** | **EUC** | **Cloud** | **Security** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CLOUD.001 | Vendor will provide L2/L3 support for server operating systems (Windows/Linux) including the ability to open incident support tickets with Microsoft as requested. | Vendor will leverage BHF credential /access to raise incident support ticket to Microsoft | A | I | C, I | I | R | C, I |
| CLOUD.002 | Vendor will provide BHF direct admin access to the cloud portals under administration for audit trail and general oversight. | Vendor will manage cloud account subscriptions on behalf of BHF. As BHF will be owning the cloud subscription accounts, BHF would have the desired direct admin accesss to the cloud portals. | A | I | C, I | I | R | C, I |
| CLOUD.003 | Vendor will provide access to an Azure Security Architect that will be named for the BHF account. |  | A | I | C, I | I | R | C, I |
| CLOUD.004 | Vendor will provide a dedicated DevOps engineer(s), and supporting resources, who will interface directly with BHF's Infrastructure, Engineering, Architecture, Data, Operations and Security teams. The engineer will be responsible for updating, maintaining BHF's toolchain, develop/maintain BHF CI/CD pipelines, and code repositories (GitHub). | Not supported. DevOps support is out of scope | A | I | C, I | C, I | C, I | C, I |
| CLOUD.005 | Vendor will provide Azure and AWS expertise including sharing information on Amazon/Microsoft published roadmaps for services in this scope and existing capabilities as well as provide and ensure best practices are being followed. |  | A | I | C, I | I | R | C, I |
| CLOUD.006 | Any cloud infrastructure including data provisioned within Azure or AWS must be able to be transitioned to BHF ownership without requiring the renaming or re-IPing of any underlying assets. | Not Supported | A | I | C, I | C, I | C, I | C, I |
| CLOUD.007 | Supplier will manage BHF Azure and AWS tenants across multiple availability zone and regions. |  | A | I | C, I | I | R | C, I |
| CLOUD.008 | Vendor will integrate any future cloud hosting platforms such as GCP, if requested without incurring any additional setup costs for BHF. | Initial setup charge for GCP will be covered as part of small projects. GCP to Azure support will be considered as part of the rate card provided, any P times Q support needs to be discussed and per unit values to be created and SOW needs to be updated through CR Process wherever required. Updated as per discussion with Kris and Paul | A | I | C, I | I | R | C, I |
| CLOUD.009 | Vendor will manage all the underlying components of the Azure and AWS environments including but not limited to Virtual Networks, Virtual Machines, Storage, Load Balancers, Security Groups etc. |  | A | I | C, I | I | R | C, I |
| CLOUD.010 | BHF requires the ability to spin up or down cloud infrastructure on demand at our direction. |  | A | I | C, I | I | R | C, I |
| CLOUD.011 | Vendor will configure and manage all cloud monitoring tools for the Azure and AWS environments must integrate with the Brighthouse Financial NOC (i.e. Cloud Watch, Azure Monitoring, and any other Network Traffic Monitoring or general BI tools provided by the 3rd Party Vendor). Native cloud monitoring tools shall integrate with the BHF enterprise monitoring event correlation engine Moogsoft. | Vendor will configure and manage the native cloud monitoring tools (AWS Cloudwatch and Azure Monitor). Vendor understands that Zabbix is used for OS, DB monitoring and the management of the Zabbix will be done by the incumbent 3rd Party Vendor. Any monitoring tool integration required with Moogsoft will be performed by the 3rd Party Vendor. | A | I | C, I | I | R | C, I |
| CLOUD.012 | Provider will utilize existing BHF Dynatrace and Zabbix monitoring to report on health of cloud infrastructure and applications such as SQL server databases, web servers, etc. (anything that lives above the OS stack under management by this Vendor) which will be fed into the NOC and event monitoring. Agent level performance issues to be addressed by SIAM/ITSM provider. Cloud Vendor will need to establish baseline performance metrics of cloud infrastructure to determine any associated variance in performance. |  | A | I | C, I | I | R | C, I |
| CLOUD.013 | Vendor will be responsible for generating insights from logs, providing BHF read access to all logs and integrating Vendor's log management into BHF's NOC, SIEM and event monitoring solutions to aid with proactive detection and resolution of incidents before they become problems. |  | A | I | C, I | I | R | C, I |
| CLOUD.014 | Vendor will work with WAN connectivity team to manage and create based upon BHF direction Azure ExpressRoute and AWS DirectConnect private connections between BHF colocation facilities and those clouds. | Vendor understands that BHF already has Azure ExpressRoute and AWS DirectConnect established between ECX and the respective cloud platforms. Vendor understands that management of cloud connectivity through ECX platform is currently provided by Equinix. Management and creation of new cloud connectivity is considered out of scope as cloud connectivity management contract with Equinix is not factored by Vendor as additional details is yet to be provided by BHF.  **Contract discussion is already in progress.** | A | I | C, I | I | R | C, I |
| CLOUD.015 | Vendor will manage and maintain Azure file server environments. |  | A | I | C, I | I | R | C, I |
| CLOUD.016 | Vendor will manage existing Windows SMB file server environment hosted in Azure including, but not limited to, DFS namespace management, folder structure, group membership, and NTFS permissions. Vendor will need to handle all file server requests and integrate requests process with BHF's service catalog. |  | A | I | C, I | I | R | C, I |
| CLOUD.017 | Vendor will provide support for all access requests and/or file recovery requests. |  | A | I | C, I | I | R | C, I |
| CLOUD.018 | Vendor will be responsible for ensuring proper controls are in place to secure access and handle requests related to shared folders hosted within Azure. |  | A | I | C, I | I | R | C, I |
| CLOUD.019 | Vendor will backup and retain data per BHF's business standards, with the ability to backup for no less than 30 days and archive up to 7 years (6 months default). | Backup will be configured in the cloud as per BHF's requirements | A | I | C, I | I | R | C, I |
| CLOUD.020 | Supplier will need to run BHF provided scanning (Varonis) tools on a as needed basis and/or quarterly to look for any NPI related content. Supplier will provide reports of output from findings to security and infrastructure teams. | As per the DD discussion - Varonis is out of scope | A | I | C, I | I | R | C, I |
| CLOUD.021 | Vendor will work with security and legal teams to assist with legal holds and lifecycle management of content stored within Azure shared drives. |  | A | I | C, I | I | R | C, I |
| CLOUD.022 | Vendor will be responsible for day-to-day management of hybrid configuration of on-prem AD (private cloud hosted) and Azure AD for the enterprise including the management of group policies, domains and forests, ADFS, and FSMO roles. |  | A | I | C, I | I | R | C, I |
| CLOUD.023 | Vendor will manage and maintain domain controller configuration. |  | A | I | C, I | I | R | C, I |
| CLOUD.024 | Vendor will manage and maintain all active directory servers, including integration with hybrid Azure AD environment. |  | A | I | C, I | I | R | C, I |
| CLOUD.025 | Vendor will insure all AD set up to be active/active and highly resilient across all BHF locations. |  | A | I | C, I | I | R | C, I |
| CLOUD.026 | Vendor will manage and provide tracking of all group policies deployed across the enterprise. |  | A | I | C, I | I | R | C, I |
| CLOUD.027 | Vendor will perform regular system tuning and monitoring. All monitoring must be integrated with BHF's NOC and event management system. | Cognizant understands that L1 system monitoring and any integrations with the event management system will be done by the incumbent service provider. | A | I | C, I | I | R | C, I |
| CLOUD.028 | Vendor will assist with security architecture and monitoring of AD. |  | A | I | C, I | I | R | C, I |
| CLOUD.029 | Vendor will perform all Level 2 and Level 3 support for AD authentication services and/or attribute management. |  | A | I | C, I | I | R | C, I |
| CLOUD.030 | Vendor will validate AD attributes with source systems (saviynt), on a weekly basis, and report on any deviation, which must be integrated with BHF's NOC. |  | A | I | C, I | I | R | C, I |
| CLOUD.031 | Vendor will integrate AD group management with saviynt access management system. |  | A | I | C, I | I | R | C, I |
| CLOUD.032 | Vendor will patch and maintain AD environment at N-1 patch levels where N will be decided by BHF and Vendor. |  | A | I | C, I | I | R | C, I |
| CLOUD.033 | Vendor will maintain all technical documentation and configuration, to be reviewed and updated quarterly. All configuration information must be integrated with BHF's CMDB in real-time. | Cognizant will maintain the technical documentaions as mutually agreed with BHF. Cognizant understands that at present CMDB is not configured in ServiceNow and will be implemented by the incumbent service provider. The integration of the configuration information with BHF's CMDB will also be performed by the incumbent service provider. | A | I | C, I | I | R | C, I |
| CLOUD.034 | Vendor will manage the day-to-day operations and server health for current and future BHF infrastructure (currently Windows Server 2012 R2, 2016, and Linux OS servers). Vendor shall maintain an N-1 configuration state of all server OSs. Normal operations include but not limited to the following activities: - Verifying that backups and restores have been tested and are confirmed to be working - Checking disk usage - OS updates and patches - Monitor for OS errors or signs of underlying hardware problems - Monitor for fault and performance events related to servers - Monitor server utilization (CPU, RAM, Network Utilization) |  | A | I | C, I | I | R | C, I |
| CLOUD.035 | Vendor will establish technology and security standards, in collaboration with BHF, for Windows and Linux server operating systems. |  | A | I | C, I | I | R | C, I |
| CLOUD.036 | Vendor will develop, test, manage and maintain Windows and Linux server templates for BHF technology standards. |  | A | I | C, I | I | R | C, I |
| CLOUD.037 | Vendor will report on adherence to BHF technical and security standards of existing servers on a monthly basis. Vendor will at a minimum, integrate all existing cloud servers under their management model. This includes, but is not limited to monitoring, alerting, log management, backup/recovery and integration with ITSM tooling as defined by BHF and ITSM provider. | Cognizant will report on adherence to BHF's standards on a monthly basis. Any integration required with the ITSM tooling will be performed by the incumbent service provider. | A | I | C, I | I | R | C, I |
| CLOUD.038 | Vendor will manage the day-to-day operations for SQL Services hosted in Azure including various database administration tasks, including backups, database integrity checks, or database statistics updates, at specified intervals. Also included in this service is management of MSSQL application, replication/mirroring, connectivity, optimization, and error resolution. Please see cloud inventory for existing counts of SQL server instances. We expect minimal growth. |  | A | I | C, I | I | R | C, I |
| CLOUD.039 | Provider will address interruption or degradation of service related to MSSQL services. Provider will utilize BHF defined database monitoring tools to monitor for fault and performance events related to MSSQL. Vendor will provide proactive Database monitoring for Blocking, lock contention / deadlocks, in addition to monitor for fault and performance events related to the MSSQL Database instance. |  | A | I | C, I | I | R | C, I |
| ~~CLOUD.040~~ | ~~Supplier will provide and support DevOps toolchain and CI/CD pipelines. BHF is utilizing or looking to leverage Visual Studio Team Foundation (VSTS)/Azure DevOps, Jenkins for its pipeline. Supplier will also need to provide knowledge and basic support for development tooling such as: Artifactory, GitHub, Git, and Docker, among others.~~ |  | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.041~~ | ~~Supplier will (in accordance with BHF's SDLC and release management) need to assist with testing, debugging, documenting, code deployments, and data refreshes as needed across environment and be required to support application release activities.~~ |  | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.042~~ | ~~Supplier will help develop, update, test and manage BHF's CI/CD pipeline to address infrastructure and security delivery needs.~~ |  | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.043~~ | ~~Supplier will provide, update and maintain technical and security standards for such tooling.~~ |  | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.044~~ | ~~Supplier will backup all DevOp toolchain and pipeline configurations/orchestrations, manage under version control and provide BHF direct access to view all such information.~~ |  | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~I~~ | ~~R~~ | ~~C, I~~ |
| CLOUD.045 | Vendor shall support platforms under management such as OpenShift. BHF is leveraging a dedicated OpenShift platform currently managed by Red Hat. Vendor will need to work directly with Red Hat, Lightbend, and BHF platform team to provide general support including integration with BHF CI/CD pipeline and ITSM processes. |  | A | I | C, I | I | R | C, I |
| CLOUD.046 | Vendor will provide the capability to request, provision, deprovision and manage cloud infrastructure in support of internal or managed third party solutions/applications for different cloud service providers (SaaS onboarding/FSP). Please see existing cloud inventories and architecture connectivity diagram for quantities. | Vendor will help in provisioning and deprovisioning. Vendor will work with BHF to get existing cloud inventories and architecture connectivity diagrams | A | I | C, I | I | R | C, I |
| CLOUD.047 | Vendor will provide a non-proprietary tool with Single Sign-On (SSO) that allows for the design, configuration, deployment, and management of any associate cloud infrastructure, including Standard Server Images for Windows/Linux (existing and n-1), leveraging the native cloud templating/orchestration solution such as AWS Cloud Formation or Azure ARM Templates. This includes management of the server operating system. | Vendor has proposed ServiceNow CMP as the cloud management platform. The ServiceNow CMP license will be owned by BHF and the CMP implementation will be done by the incumbent service provider. Vendor will assist with any architecture / design / implementation consultation as needed on a T&M based engagement as mutually agreed with BHF.  Not supported. Tools provisioning is out of scope for Cloud BAU operations | A | I | C, I | I | R | C, I |
| CLOUD.048 | Vendor will provide images that will integrate with the supplied cloud broker tool. | Not supported. Image provisioning and integration is out of scope of Cloud BAU operations | A | I | C, I | I | R | C, I |
| CLOUD.049 | Vendor will provide a self-service capability. All server configurations must be under centralized version and source control and treated as code. | Not supported. Self service capability provisioning and integration is out of scope of Cloud BAU operations. SME/Magesh/Kumaresh to help answer this functional requirement | A | I | C, I | I | R | C, I |
| CLOUD.050 | Vendor will provide direct access to provision/de-provision, configure, and review all server images and configurations at all times. |  | A | I | C, I | I | R | C, I |
| CLOUD.051 | Vendor will ensure all provisioned cloud infrastructure must be tagged according to BHF naming conventions and standards. Invoices must reflect tags for proper costing. |  | A | I | C, I | I | R | C, I |
| CLOUD.052 | Vendor solution must have ability to perform showback at a minimum of cloud infrastructure in use and/or requested. |  | A | I | C, I | I | R | C, I |
| CLOUD.053 | Vendor will work with BHF to establish cost baselines for the provisioning or deprovisioning of cloud infrastructure. |  | A | I | C, I | I | R | C, I |
| CLOUD.054 | Vendor will ensure that cloud broker is highly available, resilient and secure. Solution must integrate with BHF AD, saviynt access management and support role based access controls and views. | SME/Magesh/Kumaresh to help answer this functional requirement | A | I | C, I | I | R | C, I |
| CLOUD.055 | Vendor will provide BHF with access to cloud broker to provision and deprovision cloud infrastructure without need for added costs, requests for service or change orders to the contract. |  | A | I | C, I | I | R | C, I |
| CLOUD.056 | Vendor will provide monthly reports of cloud infrastructure utilization and any opportunities to reduce or optimize cloud footprint. Vendor will track any such optimizations and provide to BHF as annual value assessment. |  | A | I | C, I | I | R | C, I |
| CLOUD.057 | Vendor will establish, maintain and manage tagging standards for cloud infrastructure provisioned by the cloud broker. |  | A | I | C, I | I | R | C, I |
| CLOUD.058 | Vendor will establish, manage and execute transformative project to introduce cloud brokering capability and migrate existing/new cloud infrastructure to BHF standard of Azure and AWS. | Vendor has proposed ServiceNow CMP as the cloud management platform. The ServiceNow CMP license will be owned by BHF and the CMP implementation will be done by the incumbent service provider. Vendor will assist with any architecture / design / implementation consultation as needed on a T&M based engagement as mutually agreed with BHF.  Not supported as part of Cloud Operations BAU support. To be reviewed by SME/Magesh/Kumaresh | A | I | C, I | I | R | C, I |
| CLOUD.059 | Vendor will ensure that cloud brokering meets all previous requirements listed above already within this tower. | Not supported as part of Cloud Operations BAU support. To be reviewed by SME/Magesh/Kumaresh | A | I | C, I | I | R | C, I |
| ~~CLOUD.060~~ | ~~Supplier will migrate all (Internal/External) existing SSO (CIS) integrations to ADFS, leveraging SAML 2.0.~~ | ~~Out of scope for this RFP. This section needs to be excluded from this exhibit as Next Gen SSO is removed from the revised RFP scope~~ | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~C, I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.061~~ | ~~Supplier will work with 3rd party providers, as needed, to establish migration plan and execute and test all SSO integrations. Supplier will partner with 3rd party and resolve any defects.~~ | ~~Out of scope for this RFP. This section needs to be excluded from this exhibit as Next Gen SSO is removed from the revised RFP scope~~ | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~C, I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.062~~ | ~~Supplier will update solution owners of new ADFS integrations for their respective applications and work with them on scheduling for migration efforts.~~ | ~~Out of scope for this RFP. This section needs to be excluded from this exhibit as Next Gen SSO is removed from the revised RFP scope~~ | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~C, I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.063~~ | ~~Supplier will follow BHF SDLC process, including project management, release management, oversight & governance.~~ | ~~Out of scope for this RFP. This section needs to be excluded from this exhibit as Next Gen SSO is removed from the revised RFP scope~~ | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~C, I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.064~~ | ~~Supplier will maintain, manage and update existing SSO (CIS) solution, estimated at no more than 500 integrations. This includes managing SAML federation with all cloud providers, and support for mobile SSO integration with MaaS360.~~ | ~~Out of scope for this RFP. This section needs to be excluded from this exhibit as Next Gen SSO is removed from the revised RFP scope~~ | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~C, I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.065~~ | ~~Supplier will need to assume support for existing SSO solution, including vanity URL, and migrate to BHF's SSO (ADFS) next gen transformative project below.~~ | ~~Out of scope for this RFP. This section needs to be excluded from this exhibit as Next Gen SSO is removed from the revised RFP scope~~ | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~C, I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.066~~ | ~~Supplier will restrict access to any internal accessible applications in current SSO (CIS) via whitelisting or other secure method approved by BHF.~~ | ~~Out of scope for this RFP. This section needs to be excluded from this exhibit as Next Gen SSO is removed from the revised RFP scope~~ | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~C, I~~ | ~~R~~ | ~~C, I~~ |
| ~~CLOUD.067~~ | ~~Supplier will establish and support new SSO integrations (via API or manual file) as needed following BHF standards.~~ | ~~Out of scope for this RFP. This section needs to be excluded from this exhibit as Next Gen SSO is removed from the revised RFP scope~~ | ~~A~~ | ~~I~~ | ~~C, I~~ | ~~C, I~~ | ~~R~~ | ~~C, I~~ |

# Shift Coverage

**Support Resource Model:** Vendor will deliver the network services by dedicated support resources for Brighthouse, considering the HIPAA, PCI DSS standards and security control requirements. The support model will consists of below

* Resource Type: Dedicated resources to Brighthouse
* Support coverage: Deliver 24x7 support operations (16x5 on floor + on call for P1 & P2)
* Resource location: Delivery through Right shoring (Onsite/Offshore Model)

Vendor’s support model will consist of onsite and offshore resources. Onsite resource will operate from Brighthouse HQ location in Charlotte

Vendor will provide support coverage for Network Services as mentioned in the table below,

| TOWER | COVERAGE  (Hours per Day x Days per week) | LOCATION | Language Support |
| --- | --- | --- | --- |
| Integrated Operations Support (L1.5 Support) | 24x7 Manned Coverage, Shared team for Network, EUC and Cloud Operations. | Offshore (Bangalore, Chennai in India) | English |
| L2/L3 SME Support (One Team) | **Onshore**:  8am EST to 5pm EST, Mon to Fri  **Offshore**  16x5 Manned Support, Monday to Friday Coverage as per timings below:  Shift 1: 4.30am EST to 1.30pm EST  Shift 2: 12.30pm EST to 8.30pm EST  **On Call**  On call remote support for P1 and P2 tickets only (through onshore or offshore resource); other than manned coverage hours during Mon-Fri plus 24x7 during Saturdays and Sundays | Onshore at Brighthouse Location (Charlotte, NC USA)  Offshore at Bangalore, Chennai In India Vendor Offices for Manned Support  On call Remote Support | English |