**Appendix A. Security Requirements Checklist**

# COMPLIANCE ASSESSMENT & Security REVIEW

|  |  |
| --- | --- |
| ☐  ☐ | Ensure that quality & security assessment has been completed in Archer tool. Application security requirements must be implemented. Any non-compliance requirements must be documented and approved exemption before application go-live on AWS.  Application must have separate environments for development and testing. Production data should not be used in lower environments. If needed, PHI & sensitive data must be de-identified in lower environments |
| ☐ | Use of hardened Baxter AMI with minimum security baseline |
| ☐ | Ensure that application is secured and highly-available (HA design w/ horizontal & auto-scaling, load-balancing/fail-over feature) for system availability, DDoS & cyber-resiliency |
| ☐ | Ensure that application has a documented *technical design specification* for security review |

# Identity & Access Management

|  |  |
| --- | --- |
| ☐ | Ensure that AWS admin users are authenticated with onPrem AD using federated access & role-based access control, instead of creating local IAM users or permanent access key credentials in AWS |
| ☐ | Ensure that least privileges (i.e. permissions) have been granted in the AWS access policies for authorized users (via 2 roles - admin & support for each application portfolio) to perform specific tasks. |
| ☐ | Ensure that application has included deny\_policy and tag conditions (Appname & region) in access policies for least privilege & application isolation in same VPC. |
| ☐ | Verify that existing AD based accounts are reused for EC2 instances, database accounts (using Centrify tool), instead of creating separate local, privileged accounts in AWS for centralized user lifecycle management. |
| ☐ | Verify that secured protocol, strong/MFA authentication mechanism and least privilege model are used for regular and admin users from application’s *access management* perspective |

# Encryption & Key Management

|  |  |
| --- | --- |
| ☐ | Verify that data is being encrypted at EBS, EFS, S3 storage using KMS encryption key |
| ☐ | Verify that data is being encrypted at database level using native TDE or other encryption method. DBA |
| ☐ | Ensure that secure protocols like HTTPS, SFTP, LDAPS etc. are being used while data in transit. |
| ☐ | Check for encryption key good practices like higher key strength, scheduled key rotation, non-default key, key user access policy, key administrator access policy etc. SUMA |

# NETWORK TOPOLOGY

|  |  |
| --- | --- |
| ☐ | Review application’s security group (virtual firewall) for proper implementation of network segmentation & secured protocol. |
| ☐ | Ensure that firewall (onPrem) rules are implemented properly to allow targeted incoming AWS traffic for accessing OnPrem resources. |
| ☐ | Ensure that routing table, NACL setting are properly implemented with Internet Gateway for external-facing applications. |

# LOGGING & MONITORING

|  |  |
| --- | --- |
| ☐ | Ensure that CloudTrail logging enabled for all allowed regions and availability zones, and aggregated to Splunk infrastructure |
| ☐ | Enable system, network, web & app server, database & application log into Splunk infrastructure |
| ☐ | AWS CloudWatch monitoring, alerts and dashboards are deployed in all regions. |

# VulneRability Management

|  |  |
| --- | --- |
| ☐ | Ensure that *vulnerability scanning* has been performed for mission-critical applications with remediation actions |
| ☐ | For internet-facing critical application, additional *penetration testing* is required. |
| ☐ | Verify AWS services and EC2 instances are included within our *patch management* process. |

# AUTOMATED COMPLIANCE

|  |  |
| --- | --- |
| ☐ | Ensure that there is no public access to S3 buckets, S3 objects etc. |
| ☐ | Automation of the alerting or remediation of non-compliance resources using AWS Config rules or some other tool |