# Architecture Assessment

## Cost Optimization

|  |  |
| --- | --- |
| Infrastructure |  |
| **Issues** | **Remediation Steps** |
| [ ] Application servers are over provisioned [ ] SQL server is under provisioned  [ ] No cost monitoring or alerting configured  [ ] Customer can leverage Azure Reserved Instances  [ ] Azure Batch Services can be configured with auto start/stop  [ ] All data is stored in hot storage  [ ] Audit logs should be stored in cold storage |  |

|  |  |
| --- | --- |
| Application |  |
| **Issues** | **Remediation Steps** |
| [ ] Front end and backend applications can be migrated to App Services [ ] Backend API can be migrated to Azure Functions  [ ] Background services can be migrated to Azure Batch services  [ ] SQL database can be migrated to Azure SQL PaaS  [ ] Azure Key Vault should be used for storing secrets  [ ] Unoptimized SQL statements causing too much DTU utilization |  |

## Operational Excellence

|  |  |
| --- | --- |
| Infrastructure |  |
| **Issues** | **Remediation Steps** |
| [ ] No logging within the infrastructure [ ] No network monitoring to determine I/O patterns and potential bottlenecks  [ ] No notifications are configured for infrastructure outages  [ ] Infrastructure is not deployed via CI/CD pipelines—it is manual deployments  [ ] Only production environment is available—development, staging, QA, etc. environments need to be configured  [ ] No proper change management for drift detection  [ ] No gated deployments  [ ] No change logging for tracking and auditing of environment changes  [ ] No tags have been set on the resources  [ ] No delete locks on resources  [ ] Naming of resources isn’t consistent—there’s no established naming convention  [ ] No operational dashboards configured  [ ] Escalation protocols have not been established/documented  [ ] No recovery protocols defined or documented  [ ] No log retention configured for compliance  [ ] SQL Server is out of date and should be upgrade |  |

|  |  |
| --- | --- |
| Application |  |
| **Issues** | **Remediation Steps** |
| [ ] Application is not deployed via CI/CD pipelines—it is manual deployments  [ ] No documented rollback procedures  [ ] No blue/green/canary deployments  [ ] No incremental deployments  [ ] No Application Performance Monitoring has been configured—App Insights should be added  [ ] Application configuration is stored in appsettings.json  [ ] No monitoring of 3rd-party services and their endpoints has been configured  [ ] Gated deployments have not been configured  [ ] Backlog is empty—no clearly defined requirements for development and nothing to check in code against  [ ] Unit test projects have been created, but no unit tests have been defined, 0% code coverage |  |

## Performance Efficiency

|  |  |
| --- | --- |
| Infrastructure |  |
| **Issues** | **Remediation Steps** |
| [ ] Application servers are over provisioned [ ] SQL server is under provisioned  [ ] Not enough web servers to handle anticipated workload  [ ] If customer chooses to utilize IaaS, then VM scale sets should be utilized  [ ] Application accesses SQL server over same NIC as public data transit—VMs should be multi-homed  [ ] Accelerated networking not enabled on VMs  [ ] No use of Proximity Placement Groups  [ ] No auto-scaling configured [ ] Front end and backend applications can be migrated to App Services and configured for auto-scale [ ] Backend API can be migrated to Azure Functions and configured for auto-scale  [ ] SQL database can be migrated to Azure SQL PaaS  [ ] Azure SQL should be configured for read-only replicas |  |

|  |  |
| --- | --- |
| Application |  |
| **Issues** | **Remediation Steps** |
| [ ] No caching (or CDN) for the website is configured  [ ] Application fails customer’s performance SLA requirements  [ ] Front ends and backends sit on the same VMs  [ ] No performance baselines have been established |  |

## Reliability

|  |  |
| --- | --- |
| Infrastructure |  |
| **Issues** | **Remediation Steps** |
| [ ] Resources are deployed to a single region—no multi-region redundancy  [ ] VMs are not using availability zones  [ ] VMs are not using availability sets  [ ] SQL is deployed to a single server—no redundancy for SQL database  [ ] Backups are not configured for the SQL database  [ ] No system health checks have been configured  [ ] Customer’s RPO/RTO SLAs cannot be met with current infrastructure  [ ] Standard SSDs are used for OS drives—maximum 99.95% SLA, should use Premium SSDs for 99.9% SLA |  |

|  |  |
| --- | --- |
| Application |  |
| **Issues** | **Remediation Steps** |
| [ ] No uptime monitoring configured for the application  [ ] Front ends and backends sit on the same VMs  [ ] Application is currently deployed to ephemeral drives (D:)  [ ] No retry pattern configured in the application |  |

## Security

|  |  |
| --- | --- |
| Infrastructure |  |
| **Issues** | **Remediation Steps** |
| [ ] No monitoring configured for infrastructure authentication and access  [ ] No RBAC policies have been configured—all users currently have Contributor permissions assigned  [ ] Security Center has not been configured—lacking vulnerability scanning  [ ] Azure Sentinel has not been configured  [ ] NSG has been created but does not restrict public access to resources  [ ] There are NSGs configured between resources—no network segmentation or isolation  [ ] Firewalls on the VMs have been disabled  [ ] No private endpoints have been configured between services  [ ] No application firewall (WAF) for the API  [ ] Lacking premium DDOS protection  [ ] Automatic updates have not been configured on the VMs  [ ] No traffic inspection  [ ] No secret management or key rotation  [ ] Azure AD doesn’t restrict guest user accounts  [ ] HTTPS isn’t enforced  [ ] TLS 1.2 isn’t enforced  [ ] FTP/FTS has not been disabled on App Services  [ ] Management port is open on SQL server  [ ] All VMs have public IP addresses  [ ] Missing Azure Bastian or jump box  [ ] Storage accounts available to all networks  [ ] No Application Security Groups defined  [ ] VMs do not have JIT enabled  [ ] No PIM has been configured  [ ] Escalation protocols have not been established/documented  [ ] Should consider moving application to an App Service Environment (ASE) |  |

|  |  |
| --- | --- |
| Application |  |
| **Issues** | **Remediation Steps** |
| [ ] SQL connection string is stored in source control  [ ] Application leverages forms authentication  [ ] Authentication password is stored in database  [ ] Database has not been configured for Row Level Encryption (RLE)  [ ] Application connects to database using SQL username and password  [ ] API is accessible from any public IP address  [ ] Front ends and backends sit on the same VMs  [ ] Application doesn’t leverage SQL encrypted connection  [ ] API isn’t protected against CORS |  |