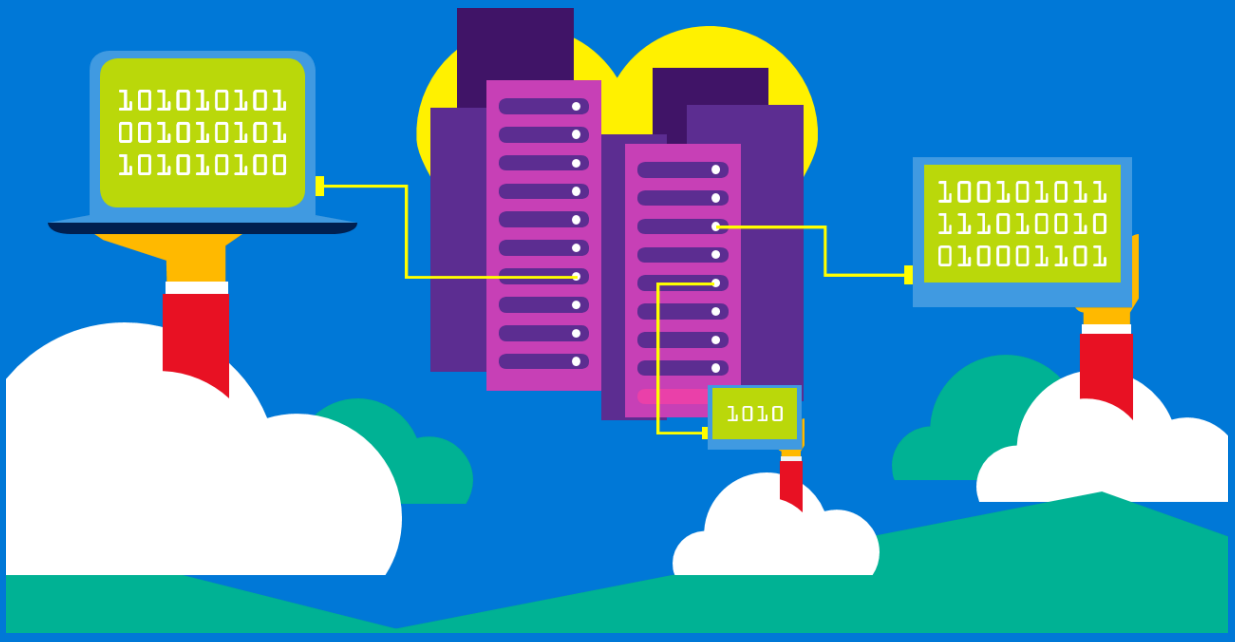
Microsoft



Structured review of Azure architectures

A guide for web application review

By Mahesh Kshirsagar
AzureCAT

September 2018

Contents

List of figures

Authored by Mahesh Kshirsagar.

Introduction

More and more customers are adopting Microsoft Azure as their preferred cloud platform. Azure enables customers and partners to run mission-critical workloads with high availability and scalability that's difficult to achieve in an on-premises setup. As development and operating teams start to get comfortable running workloads in Azure, they want to validate the architecture they have in place. There are plenty of services that customers can use, both from Microsoft and its partners, for performing an architecture review. Teams want to perform a high-level review themselves before they explore leveraging external services. The Azure team posted guidance on the Azure Architecture Center to help teams complete this review process. This paper is a synthesis of that guidance, adjusted and curated specifically for conventional web applications.

This paper describes a starting point. It identifies review drivers, how to evaluate your current architecture against these drivers, what risks the current architecture poses, and how to address those risks. With that information in hand, it also covers how to revise the architecture over multiple phases bound by clearly defined timelines to help you track progress and drive urgency.

Azure architecture review drivers

Many enterprises are moving to Azure to reap the benefits of core cloud computing. When performing a review, it's important to keep the core pillars of software quality as drivers so the review is contextualized around them.

1. **Availability:** The proportion of time that a system is functional and working, often expressed in the form of a service-level agreement (SLA). Many enterprises want to provide an SLA with as many 9s as possible for their customers.
2. **Scalability**: The ability of an application to handle increases and decreases in load and adjust with high elasticity.
3. **Resiliency**: The ability of a system to recover from failures and continue to function. Resiliency is expressed in terms of mean time between failures (MTBF) and mean time to repair (MTTR) and other similar metrics.
4. **DevOps**: The integration of development, quality assurance, and IT operations into a unified culture and set of processes for delivering software. DevOps practices play an important role in ensuring that the other pillars are met.
5. **Security:** Every application has its own specific operational and deployment needs to meet organizational IT control policies. Certain industry-specific applications, such as apps used in healthcare or banking, have external regulatory compliance rules to adhere to. Organizations want to know that when they run their application in the cloud it is secure.
6. **Management tools:** Once an application is running in the cloud, it needs to go through the full lifecycle of IT processes. These activities range from configuration to automation to disaster recovery. A management tools review ensures efficient operations measurable in terms of recovery time objective (RTO) and recovery point objective (RPO) for applications.

Review methodology

Reviews should include questions that assess the current situation of the pillars discussed in the previous section. A basic structure of such a review looks like the following:

1. Assessment questions
2. Assessment responses
3. Current risks
4. Risk mitigations and possible recommendations

This paper covers assessments for availability, scalability, resiliency, DevOps, security, and management tools as an example.

Availability review

An availability review is made up of multiple elements, such as application design, deployment and maintenance, data management, errors and failures, and monitoring and disaster recovery. Table 1 represents an availability assessment listed by serial number (SN).

Table 1. Availability assessment

SN	Review questions	Risks	Recommendations
Application design			
1	Q: Are multiple instances of the app/database running? A: <*your assessment here*>	• Individual virtual machines (VMs) become single points of congestion. • Database becomes a single point of failure.	• Deploy the application in multiple Azure paired regions. • Use auto-failover and active geo-replication for SQL Database. • Use Azure Managed Database Services for turnkey global distribution. • Deploy multiple instances of the web app.
2	Q: Are there different SLAs for application components? A: <*your assessment here*>	• Not decomposing services based on their SLAs makes it difficult to manage these services for their availability.	• Consider adopting a microservices architecture.
3	Q: Is there a message broker? A: <*your assessment here*>	• Transactions may get lost during congestion/load while waiting to get processed.	• Use Service Bus Queues between the front end and back end.
4	Q: How's throttling implemented? A: <*your assessment here*>	• Load continues to hit the application running with stretched resources, affecting even further loss of available resources.	• Use the Throttling pattern.
Deployment and maintenance			
5	Q: Are multiple datacenters (DCs) used? A: <*your assessment here*>	• An outage in one region brings down application availability.	• Deploy multiple instances of the web app. • Deploy the application in multiple Azure paired regions.
6	Q: Is deployment and testing implemented? A: <*your assessment here*>	• Manual deployment can add human error, bringing down availability. • Untested deployment process poses a risk to availability.	• Use Continuous Integration and Delivery with Visual Studio Team Services (VSTS).
7	Q: Are staging/production or rolling updates used? A: <*your assessment here*>	• Applications becomes unavailable when a new version is rolled into production.	• Use staging slots in Azure App Service.

8	Q: Is the application deployed using any technologies or methods to maintain high availability? A: <*your assessment here*>	• Applications becomes unavailable during planned/unplanned maintenance.	• Use an App Service plan that offers multiple instances. • Use virtual machine scale set. • Deploy multiple instances of the web app.
Data management			
9	Q: Is geo-replication of storage implemented? A: <*your assessment here*>	• Application becomes unavailable in case of outage or unavailability of storage.	• Use Azure Storage replication.
10	Q: Is geo-replication of databases implemented? A: <*your assessment here*>	• Application becomes unavailable in case of outage or unavailability of primary database.	• Utilize auto-failover and active geo-replication for SQL Database. • Use Azure Managed Database Services for turnkey global distribution.
11	Q: How's consistency and concurrency implemented? A: <*your assessment here*>	• Transactions are queued, affecting application availability when load starts to increase.	• Practice appropriate consistency and isolation level while making database connection.
12	Q: Are backup/restore operations scheduled and tested? A: <*your assessment here*>	• Unscheduled and untested backup/restore operations are a risk to continued availability if they do not meet the recovery point objective (RPO).	• Employ Azure to Azure Site Recovery.
Errors and failures			
13	Q: Are request timeouts configured? A: <*your assessment here*>	• Very short timeouts can cause excessive retry operations for services and resources that have considerable latency. • Very long timeouts can cause blocking if a large number of requests are queued, waiting for a service or resource to respond.	• Set SQL Connection timeout to 30s. • Use guidance on troubleshoot, diagnose, and prevent SQL connection errors and transient errors for SQL Database.
14	Q: How are transient network/other errors handled? Is there a Retry pattern? A: <*your assessment here*>	• Application becomes unavailable during a transient error.	• Use the Retry pattern.
15	Q: Is the Circuit Breaker pattern implemented? A: <*your assessment here*>	• Failure in one part of the system can lead to cascading failures, resulting in many operations becoming blocked while holding onto critical system resources, such as memory, database connections.	• Use the Circuit Breaker pattern.

16	Q: Are application components decomposed and used? A: *<your assessment here>*	• Inability to detect and avoid sending requests to failed instances minimizes availability.	• Utilize Application Gateway health monitoring. • Use Azure Traffic Manager health probing.
17	Q: Is the CQRS (Command and Query Responsibility Segregation) pattern implemented? A: *<your assessment here>*	• Command (INSERT/UPDATE) and Query (SELECT) operations target the same resource (database) affecting availability.	• Use the CQRS pattern in Azure.
Monitoring and disaster recovery			
18	Q: Are errors/failures captured and reported? A: *<your assessment here>*	• Inability to provide sufficient data to enable operations staff to determine the cause, mitigate the situation, and ensure availability.	• Use Azure Log Analytics for a detailed reporting on errors and failures. • Employ Service Map and Application Map for coherent error/failure reporting.
19	Q: Are health probes implemented? A: *<your assessment here>*	• Inability to validate response, measure latency, and extract information on availability.	• Use Application Gateway health monitoring. • Utilize Azure Traffic Manager health probing.
20	Q: Are failover/fallback processes orchestrated? A: *<your assessment here>*	• Undetected system and operation changes affect availability.	• Use Azure to Azure Site Recovery.
21	Q: What monitoring tools are used? A: *<your assessment here>*	• Inability to provide sufficient data to enable operations staff to determine the cause, mitigate the situation, and ensure availability.	• Use Azure Monitor to monitor services/infrastructure. • Build a customized Azure dashboard. • Review monitoring Azure applications and resources guidance.

Scalability review

A scalability review addresses several design areas, including application design, data management, and implementation. Table 2 represents a scalability assessment.

Table 2. Scalability assessment

SN	Review questions	Risks	Recommendations
Application design			
1	Q: Are you using the Microservices pattern? A: <*your assessment here*>	• Inability to distribute application components to maximize the use of each compute unit.	• Consider adopting a microservices architecture.
2	Q: Are you using queues? A: <*your assessment here*>	• Inability to route requests and balance application load.	• Employ the Load Levelling pattern using Azure queues/topics.
3	Q: Have you identified a correlation between scaled-up instances (web and SQL)? A: <*your assessment here*>	• Possibility of negative impact due to limitation imposed by lack of resources in some part of the overall application.	• Identify a correlation between app instance scaling and database scaling units.
4	Q: Is there client affinity? A: <*your assessment here*>	• Possibility of overhead in storing, retrieving, and maintaining state information.	• Avoid using Application Request Routing (ARR) Affinity in the App Service Environment (ASE).
5	Q: What provisions are in place when the load on the application increases? A: <*your assessment here*>	• Possibility of delay in additional resources/capacity increase.	• Use Autoscaling guidance. • Implement autoscale for services.
6	Q: Are you using background jobs? A: <*your assessment here*>	• Possibility of application becoming unresponsive and not taking requests.	• Review background jobs guidance. • Use Azure Logic Apps to create and schedule regularly running tasks.
Data management			
7	Q: Are you using multiple databases or sharding? A: <*your assessment here*>	• Possibility of poor query performance, complex scalability, poor management, and poor availability.	• Implement partitioning guidance to meet scalability requirements.
8	Q: How are you implementing data consistency? A: <*your assessment here*>	• Inability to improve scalability by reducing time needed for data synchronization.	• Use Data Consistency Primer guidance. • Ensure appropriate consistency and isolation level while making database connections.

9	Q: Are you using data batch operations? A: <*your assessment here*>	• Inability to reduce chatty operations with database/services.	• Use batch queries over multiple and frequent queries.
10	Q Are you using queues/cache? A: <*your assessment here*>	• Possibility of services becoming overwhelmed causing escalating failure. • Inability to reduce load on database that generates and serves data.	• Review caching guidance. • Use the Queue-Based Load Leveling pattern. • Use Service Bus Queue/topic. • Employ Azure Redis Cache to cache frequently used data.
11	Q: Are you using offline data processing? A: <*your assessment here*>	• Inability to serialize/deserialize XML/JSON data and store it in native database datatype making it difficult to scale.	• Consider using Azure Cosmos DB for storing XML/JSON documents.
12	Q: Have you optimized database queries/indexes? A: <*your assessment here*>	• Possibility of poor query/database performance.	• Review Query Tuning guidance. • Utilize automatic tuning in Azure SQL Database. • Use Azure Managed Database Services for automatic tuning.
13	Q: Do you have plans for data growth and retention? A: <*your assessment here*>	• Possibility of increased latency, and reduced application throughput and performance.	• Manage future growth with options provided by Azure SQL Database. • Use Azure Managed Database Services for built-in security, automatic monitoring, threat detection, automatic tuning, and turnkey global distribution.
14	Q: Are you using a content delivery network (CDN)? A: <*your assessment here*>	• Inability to reduce server load for dynamically generated content for each request.	• Review content delivery network guidance. • Utilize cache control headers when applicable.
Implementation			
15	Q: Are you using the async/await pattern? A: <*your assessment here*>	• Possibility of locking the thread while accessing resources with higher latency, limited I/O, or network bandwidth.	• Use the Asynchronous Programming pattern available in your programming language.
16	Q: What is your locking approach? A: <*your assessment here*>	• Possibility of poor performance from services with high latency.	• Ensure appropriate consistency and isolation level while making database connection.
17	Q: Are you using data compression? A: <*your assessment here*>	• Inability to reduce load on the network.	• Use GZip compression in web.config. • Utilize bundling and minification.

18	Q: Are you using connection pooling? A: <*your assessment here*>	• Inability to limit connection resources.	• Use SQL Database connection pooling.
19	Q: Have you conducted performance profiling and load testing? A: <*your assessment here*>	• Inability to determine if application performs and scales as expected.	• Run VSTS load testing for regular stress testing to identify and fix hotspots.

Resiliency review

A resiliency review addresses many design areas, including requirements, application design, data management, security, testing, deployments, operations, and telemetry. Table 3 represents a resiliency assessment.

Table 3. Resiliency assessment

SN	Review questions	Risks	Recommendations
Requirements			
1	Q: Are resiliency requirements (SLA, RPO, and others) documented/desired in the new system? A: *<your assessment here>*	• Incorrect documentation leads to a system design that may not meet the customer's expectations.	• Review resiliency requirements guidance.
Application design			
2	Q: Is failure mode analysis (FMA) performed? A: *<your assessment here>*	• Inability to identify what types of failures an application might experience, capture the potential effects and impacts of each type of failure on the application, and identify recovery strategies.	• Perform failure mode analysis to identify possible failures, impacts, and recovery strategies.
3	Q: Are multiple app service instances deployed? A: *<your assessment here>*	• Individual VMs become single points of congestion. • Database becomes a single point of failure.	• Utilize an App Service plan that offers multiple instances. • Use virtual machine scale sets. • Deploy multiple instances of the web app.
4	Q: What provisions are in place when the load on the application increases? A: *<your assessment here>*	• Possibility that the application's services will fail if they become saturated with user requests.	• Implement autoscale for services.
5	Q: Is load balancing implemented? A: *<your assessment here>*	• Inability to distribute an application's requests to healthy service instances by removing unhealthy instances from rotation.	• Adopt Load Balancer to distribute the load on the application. • Use Azure Traffic Manager.
6	Q: Is the application deployed using RAID clusters to maintain high availability? A: *<your assessment here>*	• Inability to serve user requests when an instance of a service goes down.	• Deploy the application in multiple Azure paired regions. • Deploy multiple instances of the web app.
7	Q: Is multi-DC set up implemented? A: *<your assessment here>*	• Inability to serve user requests when a site goes down.	• Use business continuity and disaster recovery (BCDR): Azure paired regions.

8	Q: Are health probes/checks implemented for load balancers (LB) and application gateway (AGW)? A: *<your assessment here>*.	• Inability to prevent user requests going to faulty instance of service.	• Use the Health Endpoint Monitoring pattern.
9	Q: Are third-party services monitored? A: *<your assessment here>*	• Inability to gauge the effect of third-party services on the application.	• Review monitoring and diagnostics guidance. • Utilize Analytics in Application Insights to predict reliability issues and monitor third-party SLAs.
10	Q: Are third-party services SLAs bound? A: *<your assessment here>*	• Inability to serve user requests when third-party service goes down.	• Implement the Health Endpoint Monitoring pattern.
11	Q: Are Retry and Circuit Breaker patterns used? A: *<your assessment here>*	• Inability to serve user requests when remote service communication fails.	• Use the Retry pattern and Circuit Breaker pattern. • Use resiliency strategies and asynchronous programming with async and await.
Data management			
12	Q: Are storage and database services replicated/fail-over? A: *<your assessment here>*	• Inability to serve user requests when storage and/or database service fails.	• Use Azure Storage replication and SQL Database active geo-replication to ensure that the application's data requirements are satisfied. • Employ Azure Managed Database Services for turnkey global distribution.
13	Q: Is the user account for the production database and backup separate? A: *<your assessment here>*	• A single user can maliciously delete *all* data (original and backup) resulting in compromised backup.	• Keep user permissions separate between production and backup data.
14	Q: Are failover and fallback processes orchestrated/tested? A: *<your assessment here>*	• Inability to verify that an operator following the processes can successfully fail over and fail back the data source.	• Use auto-failover and active geo-replication for SQL Database. • Employ Azure Managed Database Services for built-in resiliency.
15	Q: Is data backup validated? A: *<your assessment here>*	• Inability to validate data integrity, schema, and queries of the backup.	• Use automatic SQL Database backups.

Security			
16	Q: Is web application firewall (WAF) and distributed denial-of-service (DDoS) protection enabled? A: *<your assessment here>*	• Inability to distinguish true user requests from malicious user requests.	• Use WAF in front of a web app. • Review Azure DDoS Protection guidance. • Utilize Azure Key Vault to manage secrets, such as *connectionstring*.
17	Q: Is role-based access control (RBAC) implemented? A: *<your assessment here>*	• Possibility of someone purposely or accidentally deleting resources making application unavailable.	• Use RBAC with Azure AD for Azure subscription. • Utilize Azure Security Center for threat detection and protection.
Testing			
18	Q: Are the failover and failback processes tested? A: *<your assessment here>*	• Uncertainty on application services coming back online in a synchronized manner.	• Use Azure Site Recovery failback process for servers.
19	Q: Is fault-injection testing done? A: *<your assessment here>*	• Uncertainty on ability to recover from all types of faults, alone and in combination. • Uncertainty on cascading failures in system.	• Test the application by simulating or triggering real failures, such as deleting certificates, artificially consuming system resources, or deleting a storage source.
20	Q: Is performance testing done? A: *<your assessment here>*	• Uncertainty on application behavior in production under real load and fully deployed.	• Use load testing with VSTS to identify application behavior under load.
Deployment			
21	Q: Is the release process automated and documented? A: *<your assessment here>*	• Possibility of an operator deploying a bad update or improperly configuring settings for an application.	• Use VSTS release management for end-to-end traceability. • Utilize VSTS history and auditing for a consolidated view of changes to code and infrastructure.
22	Q: Are blue/green or canary release deployment techniques used? A: *<your assessment here>*	• Possibility of users not being redirected to production code in the event of a failure.	• Use the blue/green or canary release deployment technique.
23	Q: Is the deployment process logged and audited? A: *<your assessment here>*	• Inability to determine which version of an application is causing a problem after a new release.	• Use VSTS release management for end-to-end traceability. • Utilize VSTS history and auditing for a consolidated view of changes to code and infrastructure.

24	Q: Do you have a rollback plan? A: *<your assessment here>*	• Inability to go back to a last-known good version and minimize downtime.	• Use App Service deployment slots to fall back on last-known good menu. • Run VSTS conditional rollback.
Operations			
25	Q: Have you implemented alerting and monitoring? A: *<your assessment here>*	• Inability to detect failures in an application and alert an operator to fix them.	• Review monitoring and diagnostics guidance. • Review monitoring Azure applications and resources guidance.
26	Q: Are remote API/SQL call statistics available to the app team? A: *<your assessment here>*	• Inability to have an instantaneous view into the health of an application and reveal issues in the services.	• Employ usage analysis with Application Insights.
27	Q: Do you track retries for transient errors? A: *<your assessment here>*	• Possibility of an issue or failure remaining hidden by an application's retry logic.	• Review retry service-specific guidance.
28	Q: Have you assigned operators for system alerts? A: *<your assessment here>*	• Possibility of unidentified issues becoming critical.	• Use action groups to ensure people receive alerts.
29	Q: Are multiple people trained for monitoring? A: *<your assessment here>*	• Possibility of a single person being unavailable, resulting in a single point of failure.	• Train multiple people on Azure Monitor. • Send alerts and notifications to multiple recipients.
30	Q: Are your Azure subscription/service limits documented and known within the team? A: *<your assessment here>*	• Possibility of poor customer experience when hit with subscription limits.	• Review Azure subscription limits.
31	Q: Are VM sizes appropriate for your workload? A: *<your assessment here>*	• Possibility of application experiencing capacity issues when VMs approach their limit.	• Use VSTS load testing for regular stress testing to identify and fix capacity hotspots.
32	Q: Is the DB/SQL tier right for your workload? A: *<your assessment here>*	• Possibility of data use getting throttled.	• Review SQL Database options and performance guidance. • Use Azure Managed Database Services for built-in automatic tuning.
33	Q: Is the process to contact Azure support understood by your team? A: *<your assessment here>*	• Possibility of prolonged downtime as support process is navigated for the first time.	• Understand Azure support plans. • Refer to Azure support FAQs. • Familiarize your team with Azure support.

Telemetry			
34	Q: Do you collect all telemetric information? A: *<your assessment here>*	• Possibility of not having sufficient information for issues while they are actively serving users.	• Use Azure Application Insights to log and monitor application events and exceptions.
35	Q: Have you used the async pattern for logging? A: *<your assessment here>*	• Possibility of logging operations blocking application code.	• Use the asynchronous programming with async and await pattern.
36	Q: Do you have correlated log information across tiers? A: *<your assessment here>*	• Inability of tracking user requests across multiple tiers/Azure services.	• Use Service Map and Application Map for logs across multiple components.

DevOps review

A DevOps review covers many design areas, including culture, development, testing, release, monitoring, and management. Table 4 represents a DevOps assessment.

Table 4. DevOps assessment

SN	Review questions	Risks	Recommendations
Culture			
1	Q: Do all stakeholders have a single view of goals and timelines? A: *<your assessment here>*	• Possibility of conflict over resources, purposes, goals, and priorities.	• Adopt VSTS Agile as a single source of truth for all stakeholders to avoid mismatched expectations and to give an accurate picture of the current status.
2	Q: Have you automated build, test, and deployment? A: *<your assessment here>*	• Inability to know what each team member is doing and should be doing in the future.	• Utilize VSTS continuous testing. • Use VSTS Test Case Management for documenting and fixing bugs after test execution. • Practice VSTS Unit, Integration, and UAT testing for code coverage.
3	Q: Have you implemented continuous improvement? A: *<your assessment here>*	• Inability to quickly identify issues, escalate, fix, and confirm resolution.	• Use VSTS dashboards and VSTS Power BI integration for data-driven reporting and improvement.
4	Q: Do you have documented operations? A: *<your assessment here>*	• Inability to understand design, architecture, tools, processes, and code.	• Track ideas to implementation using VSTS work-item tracking. • Implement DevOps using VSTS.
5	Q: How do you share knowledge within the team? A: *<your assessment here>*	• Inability to keep knowledge organized and quickly discoverable.	• Use VSTS Wiki to distribute information, share knowledge, and collaborate.
Development			
6	Q: Do you have a production-like environment for dev/test? A: *<your assessment here>*	• Inability to test and diagnose problems.	• Use VSTS load testing with cloud scale and mimic real-life, peak-usage scenario.
7	Q: Do you have existing scripts for deployment? A: *<your assessment here>*	• Possibility of needing manual tasks or detailed technical knowledge of application.	• Employ Azure Resource Manager and VSTS to implement infrastructure-as-code model.

8	Q: Are you using application instrumentation for insight? A: *<your assessment here>*	• Inability to understand application health, performance, or errors.	• Use Azure Monitor, Azure Advisor, Azure Service Health, Activity Log, Azure Application Insights, Log Analytics, ExpressRoute monitor, Service Map, availability tests, and general monitoring Azure applications and resources.
9	Q: Are you tracking technical debt? A: *<your assessment here>*	• Possibility of shortcuts and non-optimal code with respect to the release schedule.	• Track technical debt using SonarQube with Visual Studio Team Services (VSTS).
10	Q: How do you push updates to production? A: *<your assessment here>*	• Inability to reduce cycle time for production release.	• Use feature toggles and canary releases. • Utilize App Service deployment slots to safely deploy applications.
Testing			
11	Q: Have you automated testing? A: *<your assessment here>*	• Possibility of tedious and error-prone manual testing.	• Review development and test guidance. • Use VSTS continuous testing. • Use VSTS Test Case Management for documenting and fixing bugs after test execution. • Practice VSTS Unit, Integration, and UAT testing for code coverage.
12	Q: How do you test in production? A: *<your assessment here>*	• Inability to determine if code is working as expected.	• Use App Service deployment slots for testing in production.
13	Q: How do you manage performance, load, and stress testing? A: *<your assessment here>*	• Inability to detect serious performance issues.	• Practice VSTS load testing with cloud scale.
14	Q: How do you manage capacity testing? A: *<your assessment here>*	• Inability to determine resource limitations.	• Use VSTS load testing for regular stress testing to identify and fix resource limitations.
15	Q: Are you doing penetration testing? A: *<your assessment here>*	• Inability to determine possible vulnerabilities and attacks.	• Request a penetration test for your application.

16	Q: Do you have BCP (Business Continuity Process)/DR (Disaster Recovery) drills? A: *<your assessment here>*	• Inability to determine business continuity.	• Review guidance on disaster recovery for Azure applications. • Use Azure Site Recovery drills.
Release			
17	Q: Have you automated release and deployment? A: *<your assessment here>*	• Inability to release consistent deployments quickly and reliably.	• Use VSTS Release Management for continuous delivery of software at a faster pace and with lower risk.
18	Q: Do you use continuous integration (CI)? A: *<your assessment here>*	• Inability to let developers work on a single codebase and find bugs early.	• Employ VSTS continuous integration to build, test, and deploy applications quickly.
19	Q: Do you use continuous delivery (CD)? A: *<your assessment here>*	• Inability to deliver tested production code in a very short time.	• Use VSTS continuous delivery to deploy tested code automatically.
20	Q: Do you document/log changes in deployment? A: *<your assessment here>*	• Possibility of confusion and versioning conflict.	• Use VSTS extensions to create documentation from source code. • Utilize VSTS history and auditing for a consolidated view of changes to code and infrastructure.
21	Q: How do you prevent infrastructure changes after deployment? A: *<your assessment here>*	• Inability to determine ad-hoc changes and their impact.	• Use VSTS access management to grant or restrict access to resources and features you want to control. • Use Azure Automation Change Tracking.
Monitoring			
22	Q: How do you monitor the health of your application/services? A: *<your assessment here>*	• Inability to determine application health and status.	• Use Azure Monitor, Azure Advisor, Azure Service Health, Activity Log, Azure Application Insights, Log Analytics, ExpressRoute monitor, Service Map, availability tests, and general monitoring Azure applications and resources.
23	Q: How do you correlate logs? A: *<your assessment here>*	• Inability to have a cohesive view of issues. • Inability to have an up-to-date picture of system health.	• Use Azure Log Analytics for viewing data for a particular application. • Utilize Service Map and Application Map for logs across multiple components.

24	Q: Are there automated alerts and notifications? A: *<your assessment here>*	• Inability to detect patterns or conditions that indicate potential or current issues and send alerts to address them.	• Create, view, and manage alerts using Azure Monitor. • Use Log Analytics Alerts based on conditions in Log Analytics data.
25	Q: How do you monitor assets and resources for expiration? A: *<your assessment here>*	• Inability to determine services or features that depend on the expiration of resources.	• Use Azure VM expire and certificate monitoring.
Management			
26	Q: Are there manual activities to automate? A: *<your assessment here>*	• Possibility of error-prone manual handling of repetitive operations.	• Use Azure Automation for complete control during deployment, operations, and decommissioning of workloads and resources.
27	Q: Do you have existing scripts for deployment? A: *<your assessment here>*	• Inability to minimize the amount of manual configuration needed to provision resources.	• Utilize Azure Resource Manager templates and scripts for automated resource provisioning.
28	Q: Are you planning to use containers? A: *<your assessment here>*	• Inability to create self-contained packages, including all dependencies and files needed to run the application, which simplifies the deployment.	• Use VSTS hosted CI/CD for containers to create and deploy containers.
29	Q: Do you have an operations manual? A: *<your assessment here>*	• Inability to refer to any documented operations scenarios and mitigation plans during a failure or other disruption in service.	• Use Azure Operations Management Suite (OMS) for process automation.
30	Q: Do you have on-call procedures documented? A: *<your assessment here>*	• Inability to refer to on-call duties, schedules, and procedures.	• Employ third-party extensions such as Remedy OnDemand to notify on-call responders for critical VSTS work items.
31	Q: Do you have escalation procedures documented? A: *<your assessment here>*	• Inability to deal with outages, including identifying support contacts and escalation paths.	• Practice agile planning and portfolio management with VSTS for a full view of the work escalation and decomposition of tasks.
32	Q: How do you implement configuration management? A: *<your assessment here>*	• Inability to plan, create, and record configuration changes and make them visible to operations.	• Employ VSTS configuration management for visibility to dev and operations teams. • Use PowerShell DSC for configuration management.

33	Q: Do you have an Azure support plan? A: <*your assessment here*>	• Inability to understand details of the plan, how the support process works, getting service limits changed, and opening support tickets.	• Understand Azure support plans. • Refer to Azure Support FAQs.
34	Q: Have you implemented RBAC? A: <*your assessment here*>	• Inability to manage access to resources and enforce security principles.	• Use role-based access control (RBAC) to grant access based on Azure Active Directory identities and groups.
35	Q: Do you use a bug-tracking system? A: <*your assessment here*>	• Possibility of missed items, duplicate work, or introduction of additional problems.	• Utilize VSTS bug tracking tool for establishing links between code and bugs. • Use Bugzilla integration with VSTS.
36	Q: Do you audit and track changes in code and infrastructure? A: <*your assessment here*>	• Inability to track and audit changes (code, infrastructure, configuration, documentation, and scripts).	• Employ VSTS history and auditing for a consolidated view of changes to code and infrastructure.

Security review

A security review covers areas such as network boundary security, network security, database security, data storage security, identity management, and operational security. Table 5 represents a security assessment.

Table 5. Security assessment

SN	Review questions	Risks	Recommendations
Network boundary security			
1	Q: How do you implement DDoS protection? A: *<your assessment here>*	• Potential of smaller-scale attack that doesn't trip the platform-level protection.	• Use Azure DDoS Protection to prevent volumetric attacks, protocol attacks, and resource (application)-layer attacks.
2	Q: How do you configure public IPs for which traffic is passed in, and how and where it's translated? A: *<your assessment here>*	• Inability to provision VMs with private IP addresses for protection.	• Use Azure Firewall for built-in high availability and unrestricted cloud scalability. • Utilize Azure IP address to determine which traffic is passed in, and how and where it's translated on to the virtual network.
3	Q: How do you isolate network traffic? A: *<your assessment here>*	• Inability to ensure VMs and communication between them remains private within a network boundary.	• Use Azure Virtual Network to allow VMs to securely communicate with each other, the Internet, and on-premises networks.
4	Q: How do you configure traffic flow between multiple application tiers? A: *<your assessment here>*	• Inability to define different access policies based on the workload types, and to control traffic flows between them.	• Employ Azure Virtual Network Subnet to designate separate address spaces for different elements or "tiers" within the workload, define different access policies, and control traffic flows between the tiers.
5	Q: How do you route network traffic through security appliances for security boundary policy enforcement, auditing, and inspection? A: *<your assessment here>*	• Inability to define communication paths between different tiers within a network boundary.	• Use Azure Virtual Network User Defined Routes (UDR) to control next hop for traffic between Azure, on-premises, and Internet resources through virtual appliance, virtual network gateway, virtual network, or Internet.

6	Q: Do you use firewalls, load balancers, and intrusion detection systems (IDS)/intrusion prevention systems (IPS)? A: *<your assessment here>*	• Possibility of not being able to select comprehensive solutions for secure network boundaries.	• Use Network Appliances from Azure Marketplace to deploy a variety of preconfigured network virtual appliances. • Utilize Application Gateway WAF to detect and protect against common web attacks.
Network security			
7	Q: How do you segment the larger address space into subnets? A: *<your assessment here>*	• Inability to allow or deny inbound network traffic to, or outbound network traffic from, within larger network space.	• Use network security groups (NSGs) to allow or deny traffic to and from single IP address, to and from multiple IP addresses, or even to and from entire subnets.
8	Q: How do you control routing behavior between VM connectivity? A: *<your assessment here>*	• Inability to customize the routing configuration.	• Employ Azure Virtual Network User Defined Routes (UDR) to customize the routing configuration for deployments.
9	Q: How do you implement forced tunneling? A: *<your assessment here>*	• Potential of outbound connections from any VM increasing attack surface area leveraged by attackers.	• Utilize forced tunneling to ensure that connections to the Internet go through corporate network security devices.
10	Q: How do you implement enhanced levels of security (firewall, IPS/IDS, antivirus, vulnerability management, botnet protection) on top of network-level controls? A: *<your assessment here>*	• Inability to enable security for other OSI model layers other than network and transport layer.	• Use Azure Marketplace to provision devices for higher levels of network security than with network-level access controls.
11	Q: How do you establish cross-premises connectivity? A: *<your assessment here>*	• Potential of access to company's information assets on-premises.	• Use Azure site-to-site VPN or ExpressRoute to set up cross-premises connectivity to on-premises networks.
12	Q: How do you implement global load balancing? A: *<your assessment here>*	• Inability to make services available even when datacenters might become unavailable.	• Utilize Azure Traffic Manager to load balance connections to services based on the location of the user and/or other criteria.
13	Q: How do you disable RDP/SSH access to virtual machines? A: *<your assessment here>*	• Potential for attackers to use brute force techniques to gain access and launch other attacks.	• Disable RDP/SSH access to Azure Virtual Machines and use VPN/ExpressRoute to access these virtual machines for remote management.

14	Q: How do you prevent, detect, and respond to threats? A: <*your assessment here*>	• Inability to have a single pane of visibility to prevent, detect, and respond to threats.	• Employ Azure Security Center for increased visibility into, and control over, the security of Azure resources, integrated security monitoring, and policy management across Azure subscriptions.
15	Q: How do you monitor and diagnose conditions of the network? A: <*your assessment here*>	• Inability to understand, diagnose, and gain insights to the network in Azure.	• Use Network Watcher to understand, diagnose, and gain insights to the network in Azure.
16	Q: How do you gain access to real-time performance information at the packet level? A: <*your assessment here*>	• Inability to investigate an issue in detail for better diagnoses.	• Utilize packet capture to set alerts and gain access to real-time performance information at the packet level.
17	Q: How do you gather data for compliance, auditing, and monitoring the network security profile? A: <*your assessment here*>	• Inability to build a deeper understanding of the network traffic pattern.	• Use network security group flow logs to gather data for compliance, auditing, and monitoring of your network security profile.
18	Q: How do you diagnose VPN connectivity issues? A: <*your assessment here*>	• Inability to identify the issue and use the detailed logs for further investigation.	• Use Network Watcher troubleshooter to diagnose most common VPN gateway and connections issues.
Database security			
19	Q: How do you restrict database access? Do you use a firewall? A: <*your assessment here*>	• Inability to grant access to databases based on the originating IP address of each request.	• Use firewall rules to restrict database access. • Utilize Virtual Network service endpoints to secure databases to only your virtual networks.
20	Q: How do you enable database authentication? A: <*your assessment here*>	• Inability to prove a user's identity.	• Use database authentication. • Employ Azure Managed Database Services for built-in security, automatic monitoring, threat detection, automatic tuning, and turnkey global distribution.
21	Q: Do you use encryption for data protection? A: <*your assessment here*>	• Potential threat of malicious activity.	• Protect data using encryption. • Use Storage Encryption, Disk Encryption, and SQL Encryption to encrypt data in Azure.

22	Q: How do you protect data in transit? A: <*your assessment here*>	• Susceptibility for man-in-the-middle attacks, eavesdropping, and session hijacking.	• Use Azure site-to-site VPN or ExpressRoute or application-level SSL/TLS for protection.
23	Q: How do you perform database auditing? A: <*your assessment here*>	• Inability to maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies.	• Enable database auditing. • Use Azure Managed Database Services for built-in security, automatic monitoring, threat detection, automatic tuning, and turnkey global distribution.
24	Q: How do you monitor database threat detection? A: <*your assessment here*>	• Inability to identify suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns.	• Enable database threat detection.
Data storage security			
25	Q: Do you use Azure Multi-Factor Authentication (MFA) for verifying a user's identity? A: <*your assessment here*>	• Risk of credential theft attack, which may lead to data compromise.	• Use Azure AD MFA to secure data and application access without added hassles for customers. • Enforce MFA.
26	Q: Do you use RBAC to assign permissions to users, groups, and applications at a certain scope? A: <*your assessment here*>	• Risk of giving more privileges than necessary to users, leading to data compromise by having some users having access to data that they shouldn't have in the first place.	• Use role-based access control (RBAC).
27	Q: Do you encrypt Windows and Linux virtual machine (VM) disks? A: <*your assessment here*>	• Risk of data integrity issues, such as malicious or rogue users stealing data and compromised accounts gaining unauthorized access to data.	• Use Azure Disk Encryption to protect and safeguard data to meet organizational security and compliance commitments. • Encrypt Azure Virtual Machines.
28	Q: How do you implement key management for data protection? A: <*your assessment here*>	• Risk of attackers gaining access to the secret keys to decrypt the data and potentially have access to confidential information.	• Use Azure Key Vault to safeguard cryptographic keys and other secrets used by cloud apps and services. • Use Hardware Security Modules.

29	Q: How do you secure workstations for endpoint protection? A: <*your assessment here*>	• Risk of attacker compromising workstation and leveraging a user's credentials to gain access to organizational data.	• Use Azure Information Protection to secure email, documents, and sensitive data shared outside the company. • Manage with Secure Workstations.
30	Q: How do you enforce file-level data encryption? A: <*your assessment here*>	• Risk of data leakage and lack of business insights monitor for abuse and prevent malicious access to files.	• Use Azure Managed Disks for persistent and secure disk storage for Azure virtual machines. • Enforce file-level data encryption.
Identity management and access control security			
31	Q: Do you use a centralized identity management system? A: <*your assessment here*>	• Risk of increased administrative overhead in managing accounts, increasing the likelihood of mistakes and security breaches.	• Centralize identity management.
32	Q: How have you enabled Single Sign-On (SSO)? A: <*your assessment here*>	• Exposure to scenarios where users have multiple passwords, increasing the likelihood of users reusing passwords or using weak passwords.	• Enable Single Sign-On (SSO).
33	Q: Do you use self-service password reset and password management? A: <*your assessment here*>	• Susceptibility to a higher call volume to the service desk due to password issues.	• Deploy password management.
34	Q: Do you enforce multi-factor authentication (MFA) for users? A: <*your assessment here*>	• Risk of not complying with industry standards, such as PCI DSS version 3.2 and credential theft type of attack, such as Pass-the-Hash (PtH).	• Enforce MFA for users.
35	Q: Have you implemented role-based access control (RBAC)? A: <*your assessment here*>	• Risk of giving more privileges than necessary to users, leading to data compromise by having some users having access to data that they shouldn't have in the first place.	• Use RBAC.
36	Q: How do you control how resources are created? Do you use governance? A: <*your assessment here*>	• Susceptibility to users that may abuse the service by creating more resources than they need.	• Control resource creation using Resource Manager.

37	Q: How do you enforce identity control to access software-as-a-service (SaaS) apps? How do you guide developers on securely integrating apps with the identity management system? A: <*your assessment here*>	• Risk of a credential-theft type of attack, such as weak authentication and session management described in Open Web Application Security Project (OWASP) Top 10.	• Guide developers to leverage identity capabilities for SaaS apps.
38	Q: How do you actively monitor for suspicious activities? A: <*your assessment here*>	• Risk of compromised user credentials and suspicious activities occurring using these credentials.	• Actively monitor for suspicious activities.
39	Q: How do you manage, monitor, and control access of admin account holders? A: <*your assessment here*>	• Risk of compromised admin accounts negating the value of all the other measures taken to ensure the confidentiality and integrity of data.	• Limit and constrain administrative access.
Operational security			
40	Q: How do you harden systems? A: <*your assessment here*>	• Exposure of service endpoints that are not required for installed applications.	• Use Security Compliance Manager to import the current configuration by using either group policies based on Active Directory or configuration of a "golden master" reference machine by using the LocalGPO tool. You can then import the local group policy into Security Compliance Manager.
41	Q: How do you manage antimalware? A: <*your assessment here*>	• Risk of malware infecting machines.	• Install and manage antimalware.
42	Q: How do you deploy and test a backup solution? A: <*your assessment here*>	• Exposure to data loss.	• Use Azure Backup to address backup requirements.
43	Q: How do you actively monitor all resources? A: <*your assessment here*>	• Inability to visualize, query, route, archive, and take action on the metrics and logs coming from resources.	• Utilize Azure Monitor to get the granular, up-to-date monitoring data all in one place. • Use monitoring services.
44	Q: How do you manage and protect your infrastructure? A: <*your assessment here*>	• Exposure to gathering data from multiple security and management systems.	• Utilize Azure Monitor to get the granular, up-to-date monitoring data all in one place. • Review monitor, manage, and protect cloud infrastructure guidance.

45	Q: How do you collect and process data about resources (security event log, Windows firewall log, antimalware assessment)? A: *<your assessment here>*	• Inability to prevent, detect, and respond to threats.	• Use Operations Management Suite (OMS) Security and Audit Solution to collect and processes data about resources.
46	Q: How do you trace requests, analyze usage trends, and diagnose issues? A: *<your assessment here>*	• Inability to trace requests, analyze usage trends, and diagnose issues with your storage account.	• Use Azure Security Center for security management and advanced threat protection across hybrid cloud workloads. • Review trace requests, analyze usage trends, and diagnose issues guidance.
47	Q: Have you defined security policies according to your company's security needs, and tailored it to the type of applications or sensitivity of the data? A: *<your assessment here>*	• Inability to correlate information from multiple sources to identify threats.	• Use Azure Security Center for security management and advanced threat protection across hybrid cloud workloads. • Review Prevent, detect, and respond to threats guidance.
48	Q: How do you implement secure deployment using proven DevOps tools? A: *<your assessment here>*	• Potential of unproductive and inefficient enterprises and teams.	• Use Secure DevOps Kit for Azure to build and deploy applications on Azure with security integrated at every step.

Management tools review

A management tools review covers areas such as monitoring, configuration, governance, and protection. Table 6 represents a management tools assessment.

Table 6. Management tools assessment

SN	Review questions	Risks	Recommendations
Monitoring			
1	Q: Do you get proactively notified of critical conditions and take corrective action? A: <*your assessment here*>	• Risk of critical conditions going unnoticed.	• Use Azure alerts to get proactive notifications. • Employ action groups to notify recipients to respond to alerts.
2	Q: How do you combine different kinds of data into a single pane? A: <*your assessment here*>	• Inability to combine metrics, activity, usage, and logs for unified monitoring.	• Use Azure dashboards to combine data into a single pane and share it with multiple stakeholders.
3	Q: How do you do additional visualizations and make them available to others within and outside of your organization? A: <*your assessment here*>	• Inability to look at monitoring from multiple perspectives and dissecting logs.	• Export Log Analytics data to Power BI to create additional visualizations.
4	Q: How do you monitor the collection of metrics, activity logs, and diagnostic logs? A: <*your assessment here*>	• Inability to track when new resources are created/modified, or to monitor performance statistics with trending and detailed analysis.	• Use Azure Monitor for collection of metrics, activity logs, and diagnostic logs.
5	Q: How do you monitor resource configuration and usage telemetry? Do you generate best-practice recommendations from usage? A: <*your assessment here*>	• Inability to improve performance, security, and availability.	• Utilize Azure Advisor for monitoring resource configuration and usage telemetry, and to get personalized recommendations based on best practices.
6	Q: How do you identify issues with underlying services that affect your application? A: <*your assessment here*>	• Inability to proactively take steps to know about application unavailability and notify application users about it.	• Use Azure Service Health to identify issues with services affecting application and plan for scheduled maintenance.
7	Q: How do you monitor configuration changes, service health incidents, and other similar events? A: <*your assessment here*>	• Risk of configuration changes and health incidents going unnoticed.	• Utilize Activity Log for detecting configuration changes, health incidents, better utilization, and autoscale operations.

8	Q: How do you monitor availability, performance, and usage of applications? A: <*your assessment here*>	• Inability to achieve deep insights, quickly identify and diagnose errors, and make informed choices on application maintenance and improvements.	• Use Azure Application Insights to monitor availability, performance, and usage of application.
9	Q: Do you analyze logs using query language? A: <*your assessment here*>	• Inability to form a complete picture of the operating environment.	• Use Log Analytics to collect data from a variety of resources into a single repository and analyze it using a powerful query language.
10	Q: How do you monitor third-party services (containers, SQL)? A: <*your assessment here*>	• Inability to monitor third-party services and their impact on application unavailability.	• Employ Management solutions for monitoring third-party solutions, such as Container Monitoring and Azure SQL Analytics.
11	Q: How do you monitor and diagnose different network scenarios? A: <*your assessment here*>	• Inability to detect reachability, latency, and network topology changes between the VM and the endpoint.	• Use Network Watcher for scenario-based monitoring.
12	Q: How do you monitor security, performance, and operations-related insights based on DNS servers? A: <*your assessment here*>	• Inability to detect clients that try to resolve malicious domain names, stale resource records, request load on DNS servers, and dynamic DNS registration failures.	• Utilize DNS Analytics for gathering security, performance and operations-related insights of DNS servers.
13	Q: How do you test the reachability of applications and detect performance bottlenecks across on-premises, carrier networks, and cloud/private datacenters? A: <*your assessment here*>	• Inability to correlate application delivery with network performance, detect precise location of degradation along the path between the user and the application, and test application reachability from multiple user locations across the globe.	• Employ Service Endpoint Monitoring for testing reachability of applications and detect performance bottlenecks across on-premises, carrier networks and cloud/private data centers.
14	Q: Do you gather insight by analyzing virtual machines with their different processes and dependencies on other computers and external processes? A: <*your assessment here*>	• Inability to visualize interconnected systems delivering critical services mapping servers, processes, and ports.	• Use Service Map to gain insight by analyzing virtual machines with their different processes and dependencies on other computers and external processes.

15	Q: How do you monitor connectivity across public clouds, datacenters, and on-premises environments? A: <*your assessment here*>	• Inability to detect traffic blackholing, routing errors, and issues that conventional network monitoring methods can't detect.	• Adopt Network Performance Monitor (NPM) for monitoring across public clouds, datacenters, and on-premises.
16	Q: How do you monitor ExpressRoute circuits? A: <*your assessment here*>	• Inability to detect loss and latency across various VNets, monitor all paths (including redundant paths), troubleshoot transient and point-in-time network issues, determine a specific cause degrading performance, track throughput per virtual network, and see ExpressRoute system state from a previous point in time.	• Use ExpressRoute Monitor for monitoring connectivity and performance of ExpressRoute circuits.
Configuration			
17	Q: How do you automate frequent, time-consuming, and error-prone management tasks? A: <*your assessment here*>	• Inability to reduce errors, boost efficiency, and lower operational costs.	• Use automation runbooks with hybrid runbook worker to unify management by orchestrating across on-premises environments. • Use webhooks to provide a way to fulfill requests and ensure continuous delivery and operations by triggering automation from ITSM, DevOps, and monitoring systems.
18	Q: How do you monitor and automatically update machine configuration? A: <*your assessment here*>	• Inability to automatically receive configurations, conform to the desired state, and report back on compliance.	• Use Azure Automation State Configuration to provide configuration management required for enterprise environments.
19	Q: How do you schedule deployments to orchestrate the installation of updates within a defined maintenance window? How do you get visibility into update compliance? A: <*your assessment here*>	• Inability to quickly assess the status of available updates on all agent computers and manage the process of installing required updates for servers.	• Employ Update Management to manage VM updates in Azure, on-premises, or in other cloud providers.

20	Q: How do you monitor resource configuration and usage telemetry? Do you generate best-practice recommendations from usage? A: <*your assessment here*>	• Inability to get personalized recommendations to help manage the Azure environment.	• Use Azure Advisor to follow best practices to optimize Azure deployments and analyze your resource configuration and usage telemetry.
21	Q: How do you identify opportunities to reduce overall cost? A: <*your assessment here*>	• Inability to identifying idle and underutilized resources.	• Adopt Advisor cost recommendations to optimize and reduce overall Azure spend.
22	Q: How do you generate recommendations with proposed actions inline? A: <*your assessment here*>	• Inability to improve speed and responsiveness of applications.	• Review Advisor performance recommendations and Advisor high-availability recommendations for proposed actions inline.
23	Q: How do you deploy, manage, and monitor a solution as a group rather than handling its components individually? A: <*your assessment here*>	• Inability to apply common lifecycle to interdependent application parts that can be deployed or deleted in a single action.	• Use Azure Resource Manager to define the dependencies between resources so they're deployed in the correct order.
24	Q: How do you repeatedly deploy solutions throughout the development lifecycle? A: <*your assessment here*>	• Lack of confidence that resources are deployed in a consistent state.	• Utilize Azure Resource Manager deployment modes to provision all resources specified in the template.
25	Q: Do you manage infrastructure through declarative templates rather than scripts? A: <*your assessment here*>	• Inability to make deployments consistent and repeatable across environments.	• Use Azure Resource Manager templates to ensure that investments for one location are reusable in another.
26	Q: How do you define dependencies between resources so they're deployed in the correct order? A: <*your assessment here*>	• Inability to evaluate dependencies between resources and deploy them in their dependent order.	• Use Azure Resource Manager templates to define dependencies for resources that are deployed in the same template.
27	Q: How do you apply access control to all services? A: <*your assessment here*>	• Inability to provide fine-grained access management of resources.	• Use Azure Resource Manager RBAC to manage access to Azure resources, what users can do with those resources, and to what areas they have access.
28	Q: How do you apply tags to resources to logically organize all the resources in your subscription? A: <*your assessment here*>	• Inability to associate resources with the appropriate department, customer, and environment.	• Utilize resource tags to logically organize Azure resources by categories.

29	Q: Do you clarify your organization's billing by viewing costs for a group of resources? A: *<your assessment here>*	• Inability to organize resources for billing or management.	• Use resource tags for the purposes of chargebacks.
30	Q: How do you implement recurring application actions? A: *<your assessment here>*	• Inability to create, maintain, and invoke scheduled work for apps.	• Employ Azure Scheduler to declaratively describe actions to run in the cloud, on-premises, or with another provider.
31	Q: How do manage daily pruning of logs, performing backups, and other maintenance tasks? A: *<your assessment here>*	• Inability to set multiple one-time and recurring schedules.	• Adopt Azure Scheduler jobs for a wide variety of business scenarios.
32	Q: Do you have browser-based command-line experience for management tasks? A: *<your assessment here>*	• Inability to manage Azure resources without the overhead of installing, versioning, and maintaining a machine.	• Use Azure Cloud Shell for an interactive, browser-accessible shell for managing Azure resources.
33	Q: How do you plan to switch between Bash and PowerShell? A: *<your assessment here>*	• Inability to integrate with open-source tooling, such as Terraform, Ansible, and Chef InSpec.	• Use Azure Cloud Shell tools for deep integration with open-source tooling.
34	Q: How do you securely authenticate for instant access to resources? A: *<your assessment here>*	• Inability to provide secure and automatic authentication account access.	• Use Cloud Shell to secure automatic authentication for the Azure CLI 2.0 and Azure PowerShell.
35	Q: How do you stay connected to your resources regardless of time or location? A: *<your assessment here>*	• Inability to keep track of Azure resources when on the go.	• Download the Azure mobile app and stay connected to Azure resources—anytime, anywhere.
Governance			
36	Q: How do you monitor usage and spending? A: *<your assessment here>*	• Inability to provide a view to people with different responsibilities (financial controller, executives, project owners) in your organization.	• Use Cost Management metrics with dashboards to view key cost metrics and business-trend highlights to help make important business decisions.
37	Q: How do manage costs and improve efficiency? A: *<your assessment here>*	• Risk of usage exceeding agreement thresholds, resulting in unexpected cost overages.	• Utilize Cost Management budgeting to set up budgets and budget-based alerts to improve cloud governance and accountability.

38	Q: How do you build custom policies to enable security and management (restrict deployment options for organization to specific datacenters or enable the creation of specific resource types only) at scale? A: *<your assessment here>*	• Risk of resources not staying compliant with corporate standards and service-level agreements (SLAs).	• Use Custom Azure Policy to enforce different rules and effects over resources to ensure that resources stay compliant with corporate standards and SLAs.
39	Q: How do you apply policy over resources at scale (from a single subscription to a management group with control across your entire organization)? A: *<your assessment here>*	• Inability to provide RBAC assignments over multiple subscriptions.	• Employ Azure Policy scoping to apply governance conditions to multiple subscriptions (management groups) all at once.
40	Q: How do audit policy compliance against best practices? A: *<your assessment here>*	• Risk of resources getting created in wrong location, enforcing common and consistent tag usage, or auditing existing resources for appropriate configurations and setting.	• Use Azure Policy compliance monitoring to understand the compliance state of environment.
Protection			
41	Q: Do you have pay-as-you-go backup service reducing unnecessary costs? A: *<your assessment here>*	• Inability to pick and choose the data you want to protect.	• Use Azure Backup to pay only for the storage you consume.
42	Q: How do you automatically detect virtual machines for backup? A: *<your assessment here>*	• Inability to detect virtual machines to back up.	• Adopt Azure Backup VMWare integration to back up VMware server to Azure.
43	Q: How do you access control backup operations so only authorized users can perform them? A: *<your assessment here>*	• Inability to segregate duties within your team and grant only the amount of access users need to perform backups.	• Use RBAC to manage Azure Backup recovery points.
44	Q: Do you get notifications if any suspicious activity in backup is detected? A: *<your assessment here>*	• Risk of insecure backups and recovery if production and backup servers are compromised.	• Utilize Azure Backup security capabilities to prevent, alert, and recover suspicious activities.
45	Q: How do you ensure applications are available during outages with automatic recovery? A: *<your assessment here>*	• Inability to orchestrate replication, perform disaster recovery testing, and run failovers and failback.	• Use Azure Site Recovery to deploy application-aware replication to the cloud or to a secondary site.
46	Q: Do you minimize recovery issues by sequencing the order of multi-tier applications running on multiple virtual machines? A: *<your assessment here>*	• Possibility of manual backup and file recovery, which is cumbersome, error-prone, and not scalable.	• Employ Azure Site Recovery Replication of multi-tier web applications to prevent loss of productivity.

47	Q: Do you ensure compliance by testing your disaster recovery plan without impacting production workloads or end users? A: *<your assessment here>*	• Inability to test failover without impacting ongoing replication or production environment.	• Use Azure Site Recovery test failover to validate replication and disaster recovery strategy.
48	Q: How do you reduce costs by conducting business during outages? A: *<your assessment here>*	• Inability to automate tasks that require manual intervention and convert from multi-step recovery to a single-click recovery action.	• Use Azure Automation integration with Azure Site Recovery to make recovery consistently accurate, repeatable, and automated.
49	Q: How do you minimize downtime (RPO, RTO) with dependable recovery (SLA)? A: *<your assessment here>*	• Inability to define a systematic recovery process by creating small independent units that can fail over.	• Use Azure Site Recovery Plan to model an app around its dependencies and automate recovery tasks to reduce RTO.

Revised architecture

Once risks associated with your current architecture are identified and mitigated with Azure services, a revised architecture can be arrived at with these new services. To manage the complexity, new Azure services can be introduced in a phased manner. Figure 1 and Figure 2 provide an example of a revised architecture that can be implemented over two phases.

Phase 1

Figure 1 is a depiction of the first phase of a revised architecture. It covers the most essential Azure services needed.

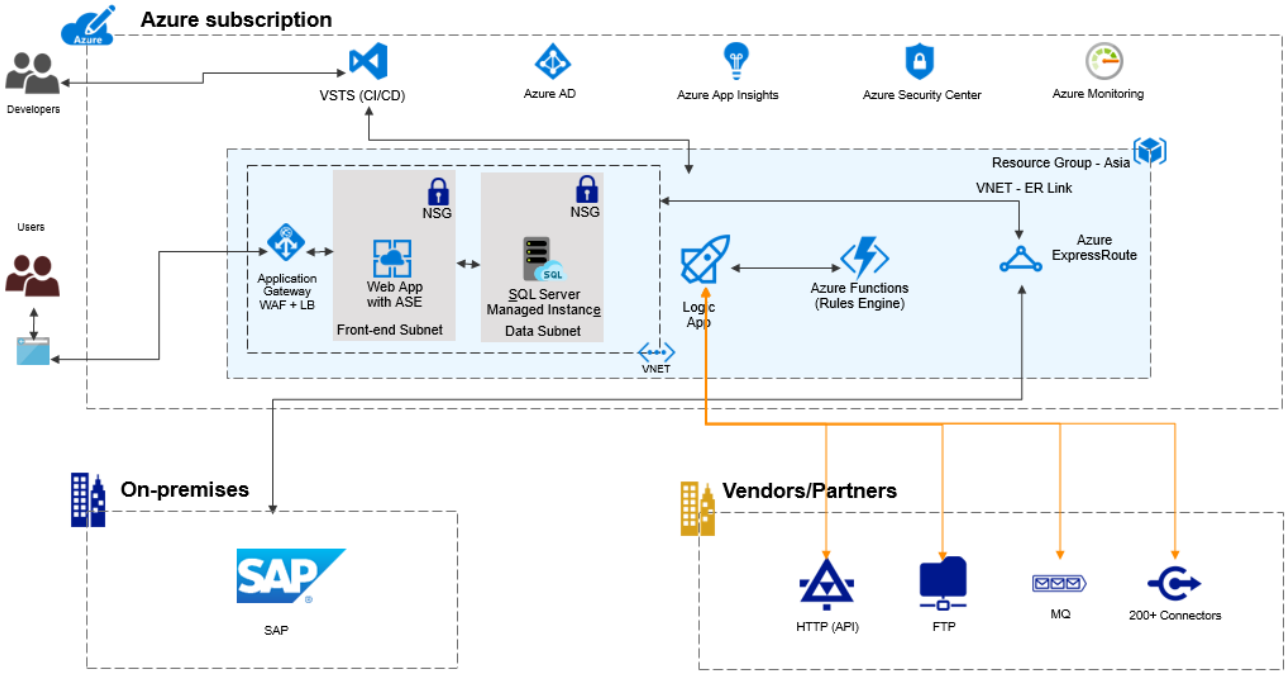


Figure 1. Phase 1 of a revised architecture

Phase 2

Phase 2 architecture builds on the Phase 1 architecture and introduces additional services identified in the review process.

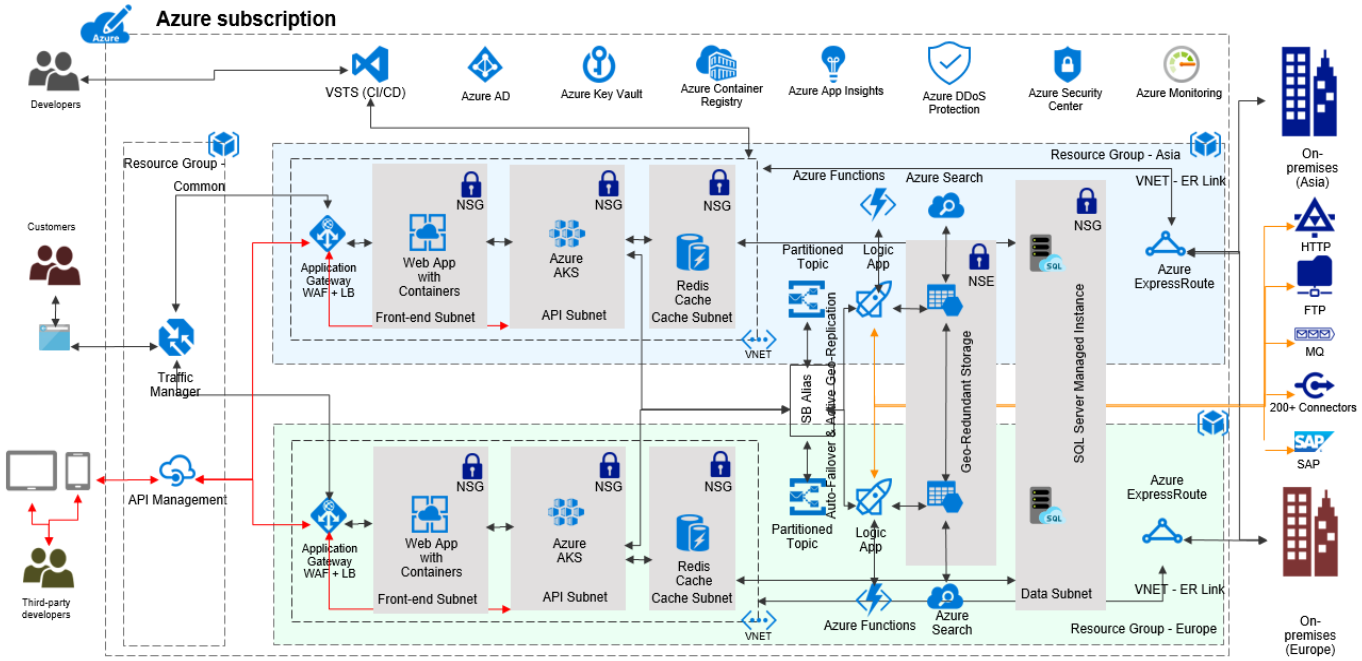


Figure 2. Phase 2 introduces additional services identified in the review

Roadmap and timelines

While it's a good idea to split a revised architecture into multiple phases, it's equally important to time-bound these phases. This helps you track progress and drive urgency within enterprise stakeholders. Table 7 is an example of how a roadmap and timeline might look.

Table 7. Timeline example

SN	Phases	Application areas	Azure services	Proposed start dates	Proposed end dates
1	Phase 1	Networking	ExpressRoute/VPN, Virtual Network, NSG	June xx, 2018	July xx, 2018
2		DevOps	VSTS	July xx, 2018	July xx, 2018
3		Availability /Scalability	App Service	July xx, 2018	July xx, 2018
4		Database	SQL Server Managed Instance	July xx, 2018	July xx, 2018
5		Monitoring	Application Insights, Azure Monitoring	July xx, 2018	July xx, 2018
6		Security	Application Gateway + WAF, Azure Security Center,	July xx, 2018	July xx, 2018
7		Workflow/Integration Service	Logic App/Function App	July xx, 2018	August xx, 2018
8		Identity	Azure AD	August xx, 2018	August xx, 2018
9	Phase 2	Availability/Scalability	Traffic Manager, Paired Regions	August xx, 2018	August xx, 2018
10		Security	Key Vault/DDoS Protection, NSE	August xx, 2018	August xx, 2018
11		Microservices/Containers	ACR, Web App with Containers, AKS	August xx, 2018	August xx, 2018
12		Availability/Scalability	Redis, Service Bus	August xx, 2018	September xx, 2018
13		Storage	Azure Storage, Azure Search	September xx, 2018	September xx, 2018
14		Mobile Development/ Documentation	API Management	September xx, 2018	September xx, 2018

Summary

Performing an Azure architecture review is not an activity limited to experts. Project teams (development and operations) of any size can self-start a review with the resources already available to them.

Learn more

For more information, see the following resources:

- Azure Architecture Center
- Availability checklist
- DevOps Checklist
- Resiliency checklist
- Scalability checklist
- Security best practices and patterns
- Management Tools