Kubernetes on Microsoft Azure Specialization

Program guide, audit checklist, and FAQ

V2.3 Checklist
Valid Aug 12 - Dec 31, 2024

Microsoft

Program updates and announcements

Module B – Aug 12, 2024
No changes to the Module B checklist were made, this checklist is required to Dec 31, 2024

Module A – Aug 12, 2024
The new Module A checklist is published and required August 12, 2024. These are the changes in the Module A controls:

- Control 1.1 Cloud Adoption Business Strategy now refers to FinOps rather than Economics and has provided an updated template link for a FinOps Assessment
- Control 2.1 Cloud Adoption Plan has provided updated evidence clarification
- Control 3.1 Repeatable Deployment has provided updated control clarification and provided updated links to templates mentioned
- Control 3.1 Repeatable Deployment – A special Evidence Note for Analytics on Azure specialization deployments and Data Warehouse Migration to Azure specialization deployments only. If no Identity or Networking components are deployed in the Azure Landing Zone, a documented focus on Resource organization attributes is sufficient to pass this control
- Control 4.1 Governance Tooling has provided an updated link to current Governance tools
- Control 5.1 Operations Management Tooling for Analytics on Azure specialization deployments and Data Warehouse Migration to Azure specialization deployments only: If no Operations Management Tooling is deployed, this control may be skipped

Please note audit price increases July 1, 2024

Module B – Dec 1, 2023
No changes to the V2.3 checklist have been made. This checklist is active until Dec. 31, 2024, or until further updates are released

Module A – Oct 1, 2023
Azure Active Directory has been renamed Microsoft Entra ID

August 28, 2023
The Microsoft Cloud Partner Program has changed its name to the Microsoft AI Cloud Partner Program effective immediately

Module B- July 5, 2023
V2.3 Kubernetes on Microsoft Azure Specialization checklist is published. This checklist version is required for audits during July 5, 2023- Jan 2, 2024. No control changes have been made in V2.3 from the V2.2 checklist

The AMMP Program has been renamed Azure Migrate and Modernize (AMM) for FY24

Module B- Jan 2, 2023
V2.2 Kubernetes on Microsoft Azure Specialization checklist is published. This checklist version is required Jan 2, 2023- June 30, 2023

■■ Microsoft

Module B- Dec 5, 2022

The PREVIEW for V2.2 Kubernetes on Microsoft Azure Specialization was made available for partners. This checklist version will be required Jan 2, 2023

- There are no new Module A or B Control updates

- FAQ clarification that a "No Pass" results when a partner fails or withdraws from the audit. This status resets from "Audit Failed" within one week to "Not Enrolled," allowing partners to reapply

Module B - Oct 3, 2022

Microsoft retired Gold Cloud partner competency, Solutions partner designations are required.
Gold and Silver competencies are retired and replaced with [Solutions Partner](#) designations. For this specialization, your organization must have an active Solutions Partner for Digital & App Innovation (Azure) or Data & AI (Azure) designation to apply

Module A- July1,2022

Checklist updates published in the May 2, 2022, preview for Module A is now required
In Control 2.2, a new Skilling Plan has been added to the checklist. This is required July 1, 2022

Module B - May 2, 2022

- Guidance for the Definition of Proof of Concept and Pilots has been updated in the Partner FAQ

- The partner Preview for the updated Module A Cloud Foundation checklist was published for Module B. This Module will be required starting July 1, 2022

Jan 1, 2022

General Guidance and FAQ updates

Contents

Kubernetes on Microsoft Azure Specialization Program Overview

This document defines the requirements to earn the Kubernetes on Microsoft Azure specialization. It also provides further requirements, guidelines, and the audit checklists for the associated audit that is required to earn this Azure specialization.

The Kubernetes on Microsoft Azure specialization is designed for partners to demonstrate their deep knowledge, extensive experience, and proven success in planning and deploying production workloads in the cloud by using containers and managing hosted Kubernetes environments in Microsoft Azure. Such partners empower their customers to realize the full breadth of Kubernetes to build transformative, secure solutions at enterprise scale.

The Kubernetes on Microsoft Azure specialization allows partners with an active, aligned Solutions Partner designation to further differentiate their organizations, demonstrate their capabilities, and build stronger connections with customers. For this specialization, an active Solutions Partner for Digital & App Innovation (Azure) or Data & AI (Azure) designation is required to apply.

Partners will receive a Pass or No Pass result upon completion of the audit process. A Pass result satisfies the audit requirement for this Azure specialization for two (2) years. See the Partner FAQ for renewal information.

Partners who meet the comprehensive requirements to earn an Azure specialization, receive a customer-facing label they can display and a prioritized business profile in Microsoft AppSource partner gallery. See the FAQ for more benefit information.

How to apply

Please note: This specialization requires 3rd party certifications to proceed to audit. These requirements are found in Module B Control 1.1.

Partners with the appropriate role and access permissions can apply. Only a Microsoft AI Cloud Partner Account Administrator or a Global Administrator of an organization's Microsoft partner account can submit an application for the Azure specialization on behalf of the organization. To do so, they sign into their Partner Center account.

On the left pane, select Azure under the **Specialization section**. Toggle to the specialization that you wish to apply for by using the drop-down menu at the top of the page.

NDAs for the audit

Auditors comply with requests from partners to sign a direct NDA. All ISSI auditors are under a nondisclosure agreement (NDA) with Microsoft. If a partner would like an NDA to be signed directly between ISSI and the partner organization for purposes of the audit, one can be provided by the partner during the audit scheduling process to ISSI. ISSI will sign and return it.

Payment terms and conditions

Pricing schedule as of July 1, 2024

Module B Audit: $2,400 USD

Module A+B Audits: $3,600 USD

A Gap Review Meeting is included with each audit.

Payment terms

The cost of the audit is payable in full to the audit company and must be settled before the audit begins. Failure to pay will result in cancellation of the audit.

Program status term

When a partner meets all prerequisite requirements shown in Partner Center and Microsoft receives a valid Pass Report from the third-party audit company, the partner will be awarded Kubernetes on Microsoft Azure specialization for one (1) calendar year.

The status and the Kubernetes on Microsoft Azure specialization label can be used only by the organization (determined by Partner Center MPN PGA ID account) and any associated locations (determined by MPN PLA ID) that met all requirements and passed the audit. Any subsidiary or affiliated organizations represented by separate Partner Center accounts (MPN PGA ID) may not advertise the status or display the associated label.

Microsoft

Audit blueprint

Audits are evidence-based. During the audit, partners will be expected to present evidence they have met the specific requirements on the checklist. This involves providing the auditor with access to live demonstrations, documents, and SME personnel to demonstrate compliance with checklist requirements.

The audit checklist will be updated to stay current with technology and market changes, and the audit is conducted by an independent, third-party auditor. The following is included in the audit blueprint:

1. Audit Roles
2. Audit Process: High level overview
3. Audit Process: Details
4. Audit Best practices and resources

Audit roles

Role of the auditor

The auditor reviews submitted evidence and objectively assesses whether the evidence provided by the partner satisfies the audit checklist requirements.

The auditor selects and evaluates evidence, based on samples of the information available from live systems. The appropriate use of such sampling is closely related to the confidence that can be placed in the audit conclusions. All ISSI auditors are under a non-disclosure agreement (NDA) with Microsoft. Auditors will also comply with requests from partners to sign a direct NDA.

Role of the partner

The partner must provide objective evidence that satisfies the auditor for all checklist items. It is the responsibility of the partner to have reviewed all check-list items prior to the audit, to have collected all necessary documentation and evidence, and to have ensured that the right subject matter experts are available to discuss and show systems, as appropriate. All audit evidence must be reproducible and verifiable.

Role of the Microsoft Partner Development Manager

For partners that have an assigned Microsoft Partner Development Manager (PDM), the PDM is responsible for ensuring that the partner fully understands the requirements prior to applying for the audit. The PDM may attend the optional consulting engagements that ISSI offers, but the PDM and other Microsoft FTEs may not attend the audit.

Audit Process: High-level overview

Step	Action	Responsibility
1	**Review:** Specialization requirements in Partner Center. Review audit checklists in the specialization and begin to prepare the necessary evidence with personnel for an evidence-based audit. <u>Recommended</u>: Before you apply, review the specific audit checklist thoroughly and confirm SME personnel required for the audit date.	Partner
2	**Meet the prerequisites and apply for the audit:** In the initial application phase, applications are submitted in two (2) stages: 1. Prerequisite requirements (see Partner Center for details) 2. Audit <u>Do not start the application process unless you are ready to undertake the audit</u>. Assess your firm's ability to complete the audit, including considerations for readiness, employee availability, and holidays.	Partner
3	**Validate**: The partner meets all requirements prior to audit.	Microsoft
4	**Confirmed by Microsoft**: Microsoft confirms with the third-party audit company that the partner is eligible for audit.	Microsoft
5	**Schedule with partner:** The auditor will schedule within two (2) business days.	Auditor (with partner)

6	Conduct the audit: Within thirty (30) calendar days of the approval for audit.	Auditor
7	Provide a Gap Report: If applicable, to the partner within two (2) business days of the completed audit, listing any Open Action Items. *	Auditor
8	**Acknowledge Gap Report receipt and schedule meeting:** Within two (2) business days of receiving the Gap Report, the partner acknowledges receipt of the report and schedules a Gap Review Meeting. Partners can begin immediate remediation of open items.	Partner
9	**Complete the meeting**: Within fifteen (15) calendar days of receiving the Gap Report, the partner schedules and completes the Gap Review Meeting with the auditor to provide evidence and address any Open Action Items. *	Auditor (with partner)
10	**Issue Final Report**: To the partner within five(5) business days. Notify Microsoft of audit Pass or No Pass result.	Auditor
11	**Notify the partner:** About program status within two (2) business days.	Microsoft

These steps will be skipped if the partner has no Open Action Items after the audit.

Microsoft

Audit Process: Details

Microsoft uses an independent third-party audit company, Information Security Systems International, LLC (ISSI), to schedule and conduct Azure specialization audits. After the audit date has been confirmed, ISSI will provide an agenda to the partner. The duration of an audit is four (4) hours for Module B workloads and eight (8) hours for Module A+B audits combined, depending upon the scope of the audit.

During the audit, the partner must provide access to the appropriate personnel who can discuss and disclose evidence that demonstrates compliance with program requirements. We highly recommend that subject matter experts for each section attend as well as a person who is familiar with the entire audit.

On the day of the audit, the partner must be prepared to provide the auditor with access to live demonstrations, documents, and personnel, as necessary to demonstrate compliance with the requirements. During the audit, the auditor will seek to verify that the partner's evidence has addressed all required audit checklist items satisfactorily.

A note on audit checklist effective dates: Partners are audited against the checklist items that are active on the date of their remote audit, not the date they apply. Audits are updated twice annually. The partner application or renewal date has no bearing on the version of the checklist that is used for the audit.

The audit can produce either of two (2) outcomes:

1. The partner passes the audit.
   - The auditor will present a brief synopsis of the audit. This will include identifying observed strengths and opportunities for improvement.
   - The auditor will provide a Final Report to the partner.
   - The auditor will notify Microsoft.

2. The partner does not satisfy all checklist items during the audit.
   - The auditor will present a brief synopsis of the audit at the end of the day, including observed strengths and Open Action Items, as outlined in the Gap Report, within two (2) business days.
   - The partner will acknowledge receipt of the Gap Report within two (2) business days.
   - The partner will move into the Gap Review phase and schedule their Gap Review Meeting within fifteen (15) calendar days.

The Gap Review

If the partner does not, to the auditor's satisfaction, provide evidence that meets the required scores across all audit categories during the audit, the partner will move into a Gap Review. A Gap Review is part of the audit and completes the process.

Within two (2) business days after the audit, the partner will receive a Gap Report, which details any Open Action Items and the outstanding required evidence. It is suggested to begin remediation on any open action items as soon as possible following the audit.

The partner then has two (2) business days to acknowledge receipt of the Gap Report and schedule a Gap Review Meeting. The Gap Review Meeting is conducted with the auditor over the partner's virtual conference platform of choice. The meeting must take place within fifteen (15) calendar days of when the Gap Report was sent, and it may last no longer than one (1) hour. During the Gap Review Meeting the partner must present evidence that addresses any and all Open Action Items.

The Gap Review Meeting can produce either of two (2) outcomes:

1. The partner resolves all Open Action Items.
   - The auditor confirms that the partner has provided the required evidence.
   - The auditor provides a Final Report to the partner.
   - The auditor notifies Microsoft about the outcome (subject to Auditor Terms and Conditions).
2. The partner does not resolve all Open Action Items.
   - The auditor presents a brief summary of the audit, including missed items.
   - The partner receives a Final Report that details the missed items.
   - The auditor notifies Microsoft about the outcome (subject to Auditor Terms and Conditions).

If the partner is still unable to provide satisfactory evidence to the auditor during their Gap Review Meeting, the partner will be deemed to have failed the audit. Partners that still want to earn this Azure specialization will need to begin the application process again.

Completion of the audit

The audit process concludes when ISSI issues the Final Report after the audit or after the Gap Review. Partners will be awarded a Pass or No Pass result upon completion of the audit process, including if they withdraw from the audit process. At the conclusion of the audit process, the auditor will issue a Final Report to the partner and notify Microsoft of the pass or no pass result.

A Pass result satisfies the audit requirement for this Azure specialization for two (2) years. A "No Pass" result is generated when a partner fails or withdraws from the audit. When a No Pass result is entered into Partner Center, you will first see your status as "Audit Failed" in your dashboard. This status will reset within one week to "Not Enrolled," allowing you to reapply. Contact Partner Center Support if needed.

Audit preparation best practices and resources

Partners should ensure that the audit checklist has been thoroughly read in advance of the audit
- Partners should ensure that all partner stakeholders involved have a copy of the audit checklist and that a stakeholder who knows the entire process is available for the duration of the audit
- Partners should confirm that they have live access granted, and files and tools are readily available during the audit exhibits

Stakeholder SME attendance in the audit

Stakeholders who can best address the relevant section should be available for the audit. However, please make sure that a stakeholder who knows the entire process is available for the duration of the audit.

Auditors often probe for more information

The auditor probes for more information to ensure that mature and repeatable processes are in place with the partner and that they are established, effective, and efficient. The auditor is looking to see how a document was created, where it is located, and what source materials were used to create the document. By probing for more information, the auditor evaluates and validates that the partner is operating at an advanced level. This can only be done by questioning during the audit. This approach is explained to the partner during the opening meeting.

Acceptable evidence: Excerpts, exhibit file formats and use of PowerPoints

PowerPoints are a common and accepted format for presenting a high-level overview of a partner's systems. However, please also be prepared to present live demonstrations from source files so that the auditor may confirm that the systems in place are mature and effective. Excerpts can be used to communicate the high-level overview but are not acceptable evidence, source documents must be presented.

Additional resources: Two optional audit preparation offers from the auditing firm *

To ensure objectivity, consulting auditors and auditors conducting the actual audits are different ISSI auditors.

1. Partners can participate in an <u>optional</u>, one (1)-hour, live Audit Process & Controls Overview session provided by ISSI. This session provides a high-level overview of key aspects of the Azure Specialization audit process. The session includes a discussion of the checklist requirements along with best practices to help partners prepare for the audit. Partners work directly with ISSI to schedule this remote session (via online web conference). For more information about this session, see https://www.issi-inc.com/services/process-and-controls-overview.
2. ISSI also provides <u>optional</u> extensive, in-depth consulting engagements to help partners prepare for their Azure specialization audit. Partners work directly with ISSI to schedule this remote session (via online web conference). For more information about this type of in-depth engagement, see Azure Specialization Consulting Offer https://www.issi-inc.com/services/audit-readiness-preparation.

* Please note that there is a cost associated with the consulting and audit preparations services. See Payment Terms and Conditions.

Microsoft

Audit checklists

The Kubernetes on Microsoft Azure specialization audit checklist contains **two (2)** modules, **Module A:** Cloud Foundation and the **Module B**: Kubernetes on Microsoft Azure workload.

Module A, The Cloud Foundation module evaluates the use of a consistent methodology and process for Azure adoption that is aligned with customers' expected outcomes, spanning the entire cloud adoption lifecycle. Module B, The Kubernetes on Microsoft Azure workload validates that the partner has adopted robust processes to ensure customer success across all phases of deploying Kubernetes on Azure solutions, from the assessment phase to design, pilot, implementation, and post-implementation phases.

Review the following audit checklist tables for more details about each control phase and to learn how the partner will be evaluated for an audit. The estimated length of both modules together is eight (8) hours.

Module A: Cloud Foundation
1   Strategy
2   Plan
3   Environment readiness and Azure landing zone
4   Governance
5   Manage

Module B: Kubernetes on Microsoft Azure workload
1   Third-party certifications
2   Assess
3   Design
4   Deployment
5   Review and release for operations

To pass the audit, the partner must complete all audit checklist items.

Module A: The Cloud Foundation evaluates the use of a consistent methodology and process for Azure adoption that is aligned with customers' expected outcomes, spanning the entire cloud adoption lifecycle. Module A is part of the Module B specialization audit package, and as a requirement must be renewed by audit for all Azure specializations.

To complete or renew Module A, the partner needs to pass all controls in Module A by providing the specified evidence or providing evidence of a recent (within two years) Module A+B Pass result. The relevant date for each partner is the Module B Anniversary Date (AD) shown in Partner Center.

Microsoft

To waiver out of Module A, the partner must provide evidence of a recent (within two years) Pass result for an applicable A+B audit or a Pass result for the AEMSP Control 3.A within the last year.

Module A waivers:

All Azure Specializations: When applying to renew subsequent Azure specializations, a previous Module A +B audit Pass result will satisfy the requirements for Module A if the result has been within two (2) years and is on the same Module A version. (Module A updates every two years in July). Partners who have passed an A+B Azure specialization audit within the last two years have satisfied the requirements for Module A in all Module A+B Azure specialization audits, unless otherwise noted. The relevant Module B Anniversary Date (AD) is shown in Partner Center.

Special note: Partners who have passed a Module B Azure specialization audit before July 1, 2021, and specifically for the Analytics on Microsoft Azure specialization before Oct 1, 2021, have likely not passed the Module A audit and will need to do so to qualify for an Azure Module B specialization audit.

AEMSP: Partners who have passed Azure Expert MSP V1.9 and later Module 3.0 (in Full and Progress audits) have satisfied the requirements for Module A in all Module A+B Azure specialization audits, unless otherwise noted. AEMSP Partners audit yearly to stay enrolled, and Module 3.A Cloud Adoption Framework is a yearly control requirement.

Special note: Partners who sequentially waiver out of Module A in multiple Module A+B audits and then subsequently waiver out of AEMSP Module 3.A within a two-year timeline will likely be required to take a Module A audit at Module A+B renewal.

If there are questions regarding a potential waiver for Module A, reach out to the Azure Partner Specializations <azureAS@microsoft.com>

Module B, Kubernetes on Microsoft Azure workload. Each control has **one (1)** or more requirements with required evidence the partner must provide for the auditor. Both the requirements and the required evidence are defined in the following tables. For some controls, a reference customer or customer evidence

is the documentation requested. Unless otherwise stated, the partner must show at least **three (3)** unique customers with deployments completed within the last **twelve (12)** months. Please note some checklists call for **four (4)** customer examples.

The partner can use the same customer across audit checklist controls, or they can use a different customer. For audit evidence relating to customer engagements, the partner can use a customer case study and reference it multiple times. The same or different customers can be used for Modules A & B if they demonstrate requirements.

Microsoft

Module A: Cloud Foundation

1.0 Strategy and FinOps
The partner must have a defined approach for helping their customer evaluate and define a cloud adoption strategy beyond an individual asset (app, VM, or data).
Requirement

1.1	**Cloud Adoption Business Strategy**

The partner must have a defined process that captures the data-driven business strategies being used to guide customer decisions. The process should include, at minimum, the following:

1. A strategy review that captures the customer's business needs and the problems the customer is trying to solve.

2. Personalized recommendations from the partner for the customers' business strategies.

Required evidence:

A Report, Presentation, or Documented Plan that captures strategic inputs and decisions for **two (2)** unique customers, and that demonstrate the Azure Cloud Adoption Business decisions for the Azure Cloud Framework, by using the Cloud Adoption Strategy Evaluator (CASE) assessment output.

These projects should have been completed in the past **twelve (12)** months. The projects must be aligned with the above-described processes 1 and 2 and highlight both customer Business and FinOps (Financial) outcomes.

For an example, see the Cloud Adoption Strategy Evaluator, Strategy and plan templates in the Cloud Adoption Framework for Azure, and especially the FinOps Assessment best practices in Build.

2.0 Plan
The partner must have a consistent approach to planning for cloud adoption that is based on the strategy outlined in the preceding section.
Requirement

Microsoft

2.1	**Cloud Adoption Plan**	
	The partner must have a process and approach for planning and tracking the completion of cloud adoption projects. **Required evidence:** The partner must provide evidence of their capability for process and approach to planning and completion with examples of **two (2)** unique customer projects that were completed in the past **twelve (12)** months. Acceptable evidence will include at least **one (1)** of the following for each customer: - Azure DevOps backlog **OR** - Tools for project planning and tracking used by the partner **OR** - Cloud Adoption Plan Generator output using the Azure Cloud Adoption Framework	
2.2	**Plan for Skilling** When customers adopt the cloud, their existing technical staff will need a variety of new skills to aid in making technical decisions and to support the new cloud implementations. To ensure the long- term success of the customer, the partner must document a skilling plan to prepare the customer's technical staff. The Partner must document a list of key customer technical roles expected to require new skills such as, but not limited to, IT Admins, IT Governance, IT Operations, and IT Security. **The documentation must include:** 1. A description of the new skills the technical roles will need to achieve to successfully manage the new environment. 2. Resources the customer can leverage when training their technical employees such as Microsoft learning paths, technical certifications, or other comparable resources. For guidance, review Microsoft docs Azure Cloud Adoption Framework How to build a skilling readiness plan. **Required evidence:** The partner must provide a skilling plan for at least **two (2)** unique customer engagements completed within the last **twelve (12)** months. The **two (2)** skilling plans documented can include a customer-facing presentation, planning documents, post deployment documentation or similar plan documentation.	

3.0 Environment Readiness and Azure Landing Zone

The partner must be able to demonstrate that the following design areas are addressed through their approach to landing zone implementation.

Requirement

Microsoft

| 3.1 | **Repeatable Deployment**

The partner must demonstrate adherence to Azure landing zone (ALZ) design areas through a repeatable deployment. The deployment should configure, at minimum, the following identity, network, and resource organization attributes:

• Identity
   o Adoption of identity management solutions, such as Microsoft Entra ID (formerly Azure Active Directory) or equivalent

• Networking architecture design (topology)
   o [Define an Azure network topology - Cloud Adoption Framework \| Microsoft Docs](#)
   o Application of hybrid architectures that use Azure ExpressRoute, VPN Gateway, or equivalent services for connecting local datacenters to Azure

• Resource organization
   o Implementation of tagging and naming standards during the project

The partner must demonstrate which of the following [approaches](#) they used when they deployed Azure landing zones for **two (2)** unique customers:

1. Start small and expand: Azure landing zone does not deploy governance or operations configurations, which are addressed later in the implementation.

2. Full Azure landing zone (ALZ) conceptual architecture: Azure landing zones implement standard approach to the configuration of governance and operations tools prior to implementation.

3. Alternative approach: If the partner follows a proprietary approach or a mixture of the **two (2)** approaches above, the partner must clearly articulate their approach to environment configuration.

4. Brownfield scenario: The partner's customer has a landing zone that does not follow best practices, and an update is required to follow best practices in the Cloud Adoption Framework.

Required evidence:
The partner must provide evidence of a repeatable deployment they used to create landing zones, aligned to the Azure landing zone (ALZ) conceptual architecture, deployed to **two (2)** unique customer environments using [Bicep](#) or [Terraform](#) modules, and ARM (AZURE Resource Manager) templates to automatically deploy the environment configuration.

If a customer deviates from the specified architecture, the partner must demonstrate the customer requirements to justify the deviation.

The provided template can be pulled directly from the Cloud Adoption Framework Landing zone [implementation options,](#) or it can be based on the partner's own IP (Intellectual Property).

In either case, the output evidence must demonstrate the configuration of the identity, network, |

Microsoft

and resource organization, as described earlier above.

Special Evidence Note:
For Analytics on Azure specialization deployments and Data Warehouse Migration to Azure specialization deployments only: If no Identity or Networking components are deployed in the Azure Landing Zone, a documented focus on Resource organization attributes is sufficient to pass this control.

4.0 Governance

The partner must demonstrate their customer's role in governing cloud-based solutions and the Azure tools they use to facilitate any governance requirements their customer might have today or in the future.

Requirement

4.1	**Governance Tooling** The partner must demonstrate the ability to deploy the required governance tools for **two (2)** unique customer projects. **Required evidence:** The partner must demonstrate the use of Azure Policy to provide controls to govern the environment for **two (2)** unique customers with Azure projects that were completed in the past **twelve (12)** months. See governance tools for templates.

5.0 Manage

The partner must demonstrate that they have set up their customers for operational success after the deployment is completed. All partners have a role in setting up operations management, even if they do not provide long-term managed services.

Requirement

5.1	**Operations Management Tooling** The partner must demonstrate the use of Azure products or equivalent to help their customer and/or managed service provider operate the environment after deployment. **Required evidence:** The partner must demonstrate the deployment of at least **one (1)** of the following Azure products or third-party equivalents: Azure Monitor, Azure Automation, or Azure Backup/Site Recovery, for **two (2)** unique customers with projects that were completed in the past **twelve (12)** months. **Special Evidence Note**: For Analytics on Azure specialization deployments and Data Warehouse Migration to Azure specialization deployments only: If no Operations Management Tooling is deployed, this control may be skipped for both specializations.

Microsoft

Module B: Kubernetes on Microsoft Azure workload specialization

1.0 Third-party Certifications
The partners resources must be highly skilled.
Requirement

1.1	**Certification** The partner's delivery resources must have deep knowledge of Kubernetes. The partner must have **two (2)** full-time employees who have at least **one (1)** of the following certifications: • Certified Kubernetes Administrator (CKA) • Certified Kubernetes Application Developer (CKAD) • Red Hat OpenShift Developer • Red Hat OpenShift Administrator **Required evidence:** Individual certifications that are verified from **one (1)** of the following: • The Linux Foundation • Red Hat The partner must also provide evidence that the certified personnel are currently full-time employees.

2.0 Assess
The partner must have a consistent approach to assessing customer requirements for the workload.
Requirement

2.1	**Workload Assessment** The partner must demonstrate how they assess each workload prior to migration to ensure that adequate pre-migration and pre-deployment planning and sizing are performed. The assessment must include: • Dependency mapping that shows the dependencies upstream from the resources that will be modernized. • Remediation steps for the migration to the cloud. **Required evidence:** The partner should provide relevant design documents showing that the preceding items were reviewed for at least **three (3)** unique customers with Kubernetes on Azure projects that were completed within the last **twelve(12)** months. The evidence must show that all assessment details were considered for those customers. Assessments may be done manually or through an industry-accepted assessment tool. **Accepted Documentation**: Output from assessment tools, such as Azure Migrate, Movere, or other similar third-party tooling reports, assessment checklist, templates, questionnaires, or project plans. For partners that use Kubernetes solely for greenfield scenarios, a Well-Architected Review (Section 3.2) may be used as alternative evidence for this section (Section 2.1).

3.0 Design
The partner has robust methodologies for designing the workload.
Requirement

Microsoft

3.1	**Solution Design**

The partner must provide solution designs showing a consistent approach that addresses the customer requirements that were captured from the assessment phase and are specific to Kubernetes.

The solution design must show:

- Application landscape**:**

  - Current infrastructure or greenfield physical infrastructure
  - Logical architecture and requirements for migration, if applicable
  - Information for all applications and, specifically, web-based applications
- Performance benchmarks

  - Determine application performance requirements and data transfer requirement
  - Recommendations for rightsizing and resizing
- DevOps**:**

  - Source repository
  - Coding language
  - Redesign code or plan for backward compatibility
  - Code deployment process

Azure landing zone:
Kubernetes on Azure landing zones have specific requirements that might not be present in other landing zones. The environment that supports the reference deployments should address each of the following required design areas below. If an item is not relevant, the partner must document the customer's decision to deviate from applying best practices.

  - Implementing Identity & Access Management(IAM) and role-based access control (RBAC), data sovereignty and encryption, application security, and auditing.

  - Establishing a network architecture or retrofitting the existing deployment to separate out the network components of a hub for optimal performance and security.

  - Using security products, such as Azure security services, Microsoft 365 security, or other security solutions, to secure access to the data.

  - Using governance tooling to support cost optimization across the environment. After estimating the initial cost, setting budgets and alerts at different scopes to proactively monitor the cost.

  - Using backup and recovery solutions to ensure data retention.
  - Meeting requirements for government regulatory compliance in the new environment, such as GDPR and HIPAA, and implementing them through multiple datacenter regions, as needed.

3.1	
	o Configuring access to cluster resources that use Kubernetes role-based access control, such as Microsoft Entra ID (formerly Azure Active Directory) identities in Azure Kubernetes Service.

o   Configuring access to cluster resources that use Kubernetes role-based access control, such as Microsoft Entra ID (formerly Azure Active Directory) identities in Azure Kubernetes Service.

o   Continuous scanning of container images against vulnerabilities by using solutions such as Azure Security Center or similar ISV solutions.

o   Setting resource request limits for deployed pods. Using Kubernetes namespaces to properly isolate Kubernetes resources, with resource quotas enforced at the namespace level.

o   Monitoring applications and clusters.

o   Workloads implement liveness and readiness probes.

o   Application and cluster monitoring enabled with alerting, using a solution such as Azure Monitor.

o   Visualization considerations are in place, where appropriate.

o   Managing workloads.

o   Ensuring that application secrets are stored in a proper secret store, such as an Azure key vault.

- **Kubernetes cluster design document**

  o   Documenting virtual machine sizes for the system and user node pools, depending on application resource requirements and capacity planning.

  o   Documenting the logical and physical isolation of environments.

- **Network design document**

  o   Cluster network design considerations, compare network models, and choose the Kubernetes networking plug-in that fits customer needs.

  o   Choice of appropriate ingress controller driven by the requirements of the workload, the skillset of the operator, and the supportability of the technology options to meet the customer's service-level objective (SLO) expectations.

  o   Secure exposed applications with a web application firewall (WAF), such as Azure Application Gateway.

  o   Control egress traffic flow by integrating with a solution such as Azure Firewall.

Required evidence:

The partner should provide relevant solution design documents that address the preceding points, for at least **three (3)** unique customers with Kubernetes on Azure migration projects that were completed within the past **twelve (12)** months.

Acceptable Documentation: Design Documents, Project Plan, Functional Specifications, Architectural Diagram, Automated Tooling Reports, and Physical and Logical Diagrams.

Tooling output only is not acceptable for documentation but can be combined with other documents.

Microsoft

3.2	**Azure Well-Architected Review of Workloads**
	The partner must demonstrate the usage of a [Azure Well-Architected Review](#) on container-based workloads or applications in Azure.
	The Azure Well-Architected Review is designed to help partners evaluate your customers' workloads against the latest set of industry best practices. It provides actionable guidance to design and improve your customers' workloads.
	The review can be used to evaluate each workload against the pillars of the Azure Well-Architected Framework that might apply to that workload.
	Required evidence:
	Unless otherwise specified, Reviews may be conducted before, during, or after deployment. The partner must provide exported results from the completed Well-Architected Review, using the assessments in the review for at least **three (3)** workloads or applications running in Kubernetes on Azure that were completed within the last **twelve (12)** months, indicating the customer's name.
	The **three (3)** workloads can come from **one (1)** or more customers.

4.0 Deployment

The partner has robust methodologies for deploying the workload.

Requirement

4.1	**Delivery**
	The partner must provide evidence of their ability to implement customer application modernization or migration projects to Azure, from one of the following Azure scenarios:
	• Azure Kubernetes Service
	• Azure Red Hat OpenShift
	Required evidence:
	The partner must provide documentation for **three (3)** unique customers with Kubernetes projects that were completed within the last **twelve (12)** months.
	To cover the entire sequence of the project, including design and production deployment, the **documentation** must include at least **two (2)** of the following:
	• Signed statements of work(SOWs) for all projects
	• Solution design documents for all projects
	• Project plan and migration/deployment sequence
	• Architecture diagrams
	• As-built documentation

5.0 Review and Release for Operations

The partner has robust methodologies for transitioning the workload.

Requirement

Microsoft

5.1	**Service Validation and Testing** The partner must validate the deployment, including: • Demonstrating a process and approach to testing and evaluating the performance of all applications against customer expectations and Azure best practices. • Demonstrating a process and approach to evaluating and improving architectural best practices to remediate issues with migrated platforms or workloads that do not meet performance or cost expectations. **Required evidence:** <u>**Documentation**</u> of the testing, validation, and performance evaluation that addresses the preceding points for **three (3)** unique customers with Kubernetes on Azure projects that were completed in the past **twelve (12)** months. The documentation must indicate that the implemented solution met customer expectations, and it must include a sign-off from the customer. These projects can be the same as the projects evidenced in Control 3.0.

5.2	**Post-deployment Documentation**
	The partner must provide post-deployment documentation to show that their customers are successfully using the new service in Azure.
	
	Post-deployment documentation must include:
	• The software release lifecycle process (continuous integration and continuous delivery, or CI/CD).
	• Post-deployment operations guidelines to:
	    o Keep up to date with the service-level agreement (SLA) or SLO requirements.
	    o Troubleshoot and triage issues.
	    o Stay current with the latest platform features and security updates.
	    o Plan for future growth.
	
	For more information about post-deployment operations best practices, go to the <u>Triage practices</u> overview page.
	
	Required evidence:
	<u>Documentation</u> that addresses the preceding points for the **three (3)** unique customers with Kubernetes on Azure projects that were completed in the last **twelve (12)** months.

■■ Microsoft

Azure Specializations Partner FAQ

Questions regarding the Azure Partner program specializations, the current checklists and pre-qualifications for partners can usually be answered by visiting [Microsoft Azure Partner Specializations](#)

Questions on the audit checklists and program can be sent to the Azure Partner Specializations help alias <mailto:AzureAS@microsoft.com>

If you have questions that have not been answered, please go to [Partner Center support](#) to create a ticket with our Frontline team.

Microsoft