DevOps with GitHub on Microsoft Azure Specialization

Program guide, audit checklist, and FAQ

Checklist V2.3
Valid July 5, 2023 - June 30, 2024

Microsoft

Program updates and announcements

Dec 1, 2023
No changes to the V2.3 checklist have been made. This checklist is active until June 30, 2024

October 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 DevOps with GitHub on Microsoft Azure Specialization checklist is published. This checklist version is required for audits during July 5, 2023 – Jan 1, 2024. No control changes have been made in V2.3 from the V2.2 checklist

Module B - Jan 2, 2023
V2.2 DevOps with GitHub on Microsoft Azure Specialization audit checklist is published. This checklist version is required Jan 2, 2023- July 5, 2023

Module B- Dec 5, 2022
The PREVIEW for V2.2 DevOps with GitHub on Microsoft Azure Specialization was made available for partners in preview July 15, 2022. The V.2.2 checklist will be required Jan 2, 2023. Due to the audit checklist version update requirements, the partner preview for the Jan 2, 2023 checklist is renumbered to V2.2 from V2.1

Oct 3, 2022
Microsoft retired Gold Cloud partner competency, Solutions partner designation required. Gold and Silver competencies are retired & replaced with Solutions Partner designations. Azure specialization requirements are associated with your achievement of a required Solutions Partner designation. Your organization must have an active Solutions Partner for Digital & App Innovation (Azure) designation to apply for this specialization.

Module B - July 15, 2022
The partner Preview for V2.2 DevOps with GitHub certifications requirements is now available for partners. The V2.2 DevOps with GitHub audit checklist was made available in Preview. Control 1.2 GitHub Certifications have been added to the Module B audit checklist as part of the requirements. These will be required in audits on Jan 1, 2023

Module A - July 1, 2022
The Cloud Foundation Module A checklist has added a new Skilling Plan in Control 2.2. This is now required as evidence in the checklist.

Module B - July 1, 2022
The V2.0 DevOps with GitHub checklist on Microsoft Azure specialization was published July 1, 2022

- The 1.1 Controls for a DevOps consulting practice have been streamlined to require a public webpage and best practices for IP in the DevOps environment. Four (4) documents are required for evidence, rather than five (5), as of July 1, 2022
- **Controls 2.1, 3.1, 4.1, 5.1 and 5.2** have new streamlined requirements for evidence.

If a partner holds an active Kubernetes on Microsoft Azure specialization, or an active Modernization of Web Applications Azure specialization, only one (1) customer using a DevOps with GitHub solution is required to pass these controls. This is live July 1, 2022

- **Control 3.2** The Well Architected Review has been modified to require one (1) unique customer with Apps deployed to Azure, using a DevOps with GitHub solution, completed in the last twelve (12) months, rather than three (3) unique customers with one (1) using a DevOps with GitHub solution, completed in the last twelve (12) months. In the Well Architected Core Review Assessment, the Operational Excellence pillar must be completed

Module A - May 2, 2022

The partner Preview for the Module A Cloud Foundation audit checklist was made available. The Cloud Foundation Module A checklist has added a new Skilling Plan in control 2.2. This supports a consistent approach to planning for cloud adoption is required for Module A audits beginning July 1, 2022

Module B - May 2, 2022

Guidance for the Definition of Proof of Concept and Pilots was added to the FAQ

Module B- Mar 1, 2022

The V1.1 DevOps with GitHub Module B checklist on Microsoft Azure specialization was published as required March 1, 2022

Module B - Feb 8, 2022

The preview for V1.1 DevOps with GitHub checklist on Microsoft Azure specialization was made available for partners. The V1.1 audit checklist was made available for partner preview. In V1.1 Module B, DevOps with GitHub on Microsoft Azure customer evidence requirements were streamlined for most controls

Guidance and FAQ content was updated for DevOps with GitHub checklist V1.1 publication There were uniform updates to all published Azure specialization audit checklist program overviews and partner FAQ content

Module B - Feb 1, 2022

An audit timeline extension to Feb 28, 2022 for V1.0 DevOps with GitHub on Microsoft Azure specialization checklist was given. The timeline for the V1.0 DevOps with GitHub on Microsoft Azure specialization audit checklist was extended to February 28, 2022

Contents

DevOps with GitHub on Microsoft Azure Specialization Program Overview

This document defines the requirements to earn the DevOps with GitHub on 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 DevOps with GitHub on Microsoft Azure specialization is designed for partners to demonstrate their deep knowledge, extensive experience, and proven success in planning and deploying DevOps with GitHub on Microsoft Azure for their customers. Such partners empower their customers to use DevOps with GitHub on Microsoft Azure from the assessment phase to design, pilot, implementation, and post-implementation phases, to build transformative solutions at enterprise scale.

The Microsoft DevOps with GitHub Azure specialization allows partners with an active Solutions Partner designation to further differentiate their organizations, demonstrate their capabilities, and build stronger connections with customers. For this specialization, partners must have an active Solutions Partner for Digital & App Innovation (Azure) designation.

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.

Please note: Certifications are required to apply for this specialization, these are found in Module B control 1.2.

How to apply

Partners with the appropriate role and access permissions can apply. 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

Module B Audit: $2,000 USD

Module A+B Audits: $3,000 USD

A Gap Review Meeting is included with each Module 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 the DevOps with GitHub on Microsoft Azure specialization for one (1) calendar year.

The status and the DevOps with GitHub 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.

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 collated 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 needed evidence with personnel for an evidence-based audit. Recommended: Before you apply, review the specific audit checklist thoroughly and confirm SME personnel	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 Do not start the application process unless you are ready to undertake the audit. 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 to 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.*

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 synopsis 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 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 ISSI consulting offers *

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

1. Partners can participate in an optional, 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 Azure Specialization - Audit Process and Controls Overview
2. ISSI also provides optional 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://issi-inc.com/az-advspeconsulting/

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

Audit checklists

The DevOps with GitHub on Microsoft Azure specialization audit checklist contains two (2) modules, **Module A**: Cloud Foundation and **Module B**: The DevOps with GitHub on Microsoft Azure specialization 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 DevOps with GitHub on Microsoft Azure specialization workload module validates that the partner has adopted robust processes to ensure customer success across all phases of deploying DevOps with GitHub on Microsoft Azure, 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 same customers may be used for Module A & B. 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: DevOps with GitHub on Microsoft Azure workload

1. DevOps Consulting Practice
2. Assess
3. Design
4. Delivery
5. Review and Release for Operation

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

Module A: Cloud Foundation is required for multiple Azure specializations. To complete Module A, Cloud Foundation, the partner needs to pass all controls in Module A by providing the specified evidence. Partners who have passed Azure Expert MSP V1.9 (Full and Progress) and later have satisfied the requirements for Module A in all audit versions unless otherwise noted. Module A: Cloud Foundation is required for multiple Azure specializations. When applying to subsequent Azure specializations, a previous audit Pass result will satisfy the requirements for Module A if the Pass result has been within two (2) years. It can only be applied to the same version of Module A. Alternatively, the partner may present evidence of a previous pass result from another Azure specialization audit conducted on V2.0 or later. Partners who have passed an Azure specialization audit before July 1, 2021 and for the Analytics on Microsoft Azure specialization audit before Oct 1, 2021, have likely not passed the Module A audit and will need to do so to qualify for the Module B workload audits.

Module B: DevOps with GitHub on Microsoft Azure. Each control has one (1) or more requirements and 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 Apps deployed to Azure, at least **one (1)** using a GitHub DevOps solution, completed in the last **twelve (12)** months. 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.

Module A: Cloud Foundation

1.0 Strategy and Economics		
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 process that captures the data-driven business strategies being used to guide customer decisions. The process should include, at minimum, the following: • A strategy review that captures the customer's business needs and the problems the customer is trying to solve • Personalized recommendations from the partner for the customers' business strategies **Required evidence:** A Report, Presentation, or Document that captures strategic inputs and decisions for **two (2)** unique customers, that demonstrates Cloud Adoption Strategy Evaluator assessment output, with projects completed in the past **twelve (12)** months. These projects must be aligned with the above-described process and highlight both customer Business and Financial outcomes. For an example, see the Strategy and plan template in the Cloud Adoption Framework for Azure, or the Cloud Adoption Strategy Evaluator.	

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

2.1	**Cloud Adoption Plan** The partner must have a process and approach for planning and tracking the completion of cloud adoption projects. For an example of a cloud adoption plan, see the Azure DevOps Demo Generator for the Cloud Adoption Framework. **Required evidence:** The partner must provide evidence of their capability with examples of **two (2)** unique customers, with projects that were completed in the past **twelve (12)** months. Acceptable evidence must include at least **one (1)** of the following: • Cloud Adoption Plan Generator output or • Azure DevOps backlog or • Any other tools for project planning and tracking	

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: • A description of the new skills the technical roles will need to achieve to successfully manage the new environment. • 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 12 months. The **two (2)** skilling plans documentation 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	

3.1	**Repeatable Deployment**
	The partner must demonstrate adherence to Azure landing zone design areas through a repeatable deployment. The deployment should configure, at minimum, the following identity, network, and resource organization attributes:
	• Identity
	  ○ Adoption of identity management solutions, such as Microsoft Entra ID (formerly Azure Active Directory) or equivalent
	• Networking architecture design (topology)
	  ○ Define an Azure network topology - Cloud Adoption Framework
		Microsoft Docs
		  ○ Application of hybrid architectures that use Azure ExpressRoute, VPN Gateway, or equivalent services for connecting local datacenters to Azure
		• Resource organization
		  ○ Implementation of tagging and naming standards during the project
		The partner must demonstrate which of the following deployment approaches they used when they deployed Azure landing zones:
		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 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.
		Required evidence:
		The partner must provide evidence of a repeatable deployment they used to create landing zones aligned to the Azure landing zone conceptual architecture or equivalent complete architecture deployed to **two (2)** unique customer environments using Bicep, ARM (AZURE Resource Manager) templates, Terraform modules, or equivalent tools to automatically deploy the environment configuration.
		If a customer deviates from specified architecture, the partner must demonstrate the customer requirements to justify the deviation.
		The provided template can be pulled directly from the implementation options, or it can be based on the partner's own IP (Intellectual Property). In either case, the script as evidence must demonstrate the configuration of the identity, network, and resource organization, as described earlier.

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 or equivalent tool to provide controls to govern the environment for **two (2)** unique customers with projects that were completed in the past **twelve (12)** months.
5.0 Manage	
The partner must demonstrate that they have set up their customer 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 • Azure Backup/Site Recovery For **two (2)** unique customers with projects that were completed in the past **twelve (12)** months.

Module B: DevOps with GitHub on Microsoft Azure workload specialization

1.0 DevOps Consulting Practice	
The partner must have a robust DevOps consulting practice.	
Requirement	
1.1	**DevOps Consulting Practice** The partner must provide evidence of a mature Devops Consulting practice. Evidence must include: 1. Public webpage explaining partner's offering for DevOps on Azure using GitHub 2. Best practices and reusable IP to have consistent build quality and efficiency including DevOps environment setup scripts, standard templates to deploy infrastructure as code. The partner must provide **each** of the following two **(2)** documents: 1. A practice charter document with clearly documented execution model and success criteria. 2. A DevOps Readiness plan and roadmap for customers. **And two (2)** documented items from the list below: o Documented DevOps process and standardized reference architecture guidelines o A Customer assessment plan, including assets for example: Questionnaires, Assessment worksheets and Templates o Defined Governance Model documentation o Change control process document o Offering **or** Accelerator for customer DevOps adoption and execution (minimum **one(1)** offering) o GTM strategy documents o SOWs o DevOps Knowledge repository
1.2 Certifications	
The partner's resources are highly knowledgeable in DevOps with GitHub technologies.	
Requirement	

1.2	**Certifications** The partner must have a total of five (5) certifications from the list below, for full-time employees. No more than two (2) certifications of the five (5) can be fulfilled by the GitHub Administration certification. Three (3) certifications must be from GitHub Actions or GitHub Advanced Security. • GitHub Actions • GitHub Advanced Security • GitHub Administration **Required evidence:** The partner must provide a screenshot of the email from PSI that shows their name and the passing score report. Individual certifications can also be verified through one of the following methods: • The individual's profile on Credly • Download a certificate from the GitHub Certifications Exam History https://examregistration.github.com/dashboard/exams See https://examregistration.github.com/faq for more information. The partner must also provide evidence that the certified personnel are current full-time employees.

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

2.1	**Environment Assessment** The partner must demonstrate how they assess customer's DevOps maturity. The assessment must include **two (2)** of the following: • DevOps best practices, DevSecOps related assets to enable • Current state assessment and capability/Maturity assessment model • Target state definition • Execution plan (sprint or other methodology) • CI/CD Pipelines • SecOps • Test Cases • Assessment/Approval Gates at each state • Infrastructure as Code (Automated deployment of Environment/Infrastructure using tools like GitHub Actions/DevOps pipelines with proper policies and controls in place) **Required evidence:** The partner must provide relevant documents showing that the preceding items were reviewed for **three (3)** unique customers, with Apps deployed to Azure, at least **one (1)** using DevOps with GitHub, completed in 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. If a partner holds an active Kubernetes on Microsoft Azure specialization, or an active Modernization of Web Applications on Azure specialization, only **one (1)** customer using DevOps with GitHub is required to pass this control. Accepted Documentation: Assessment checklists, Templates, Questionnaires, and Project plans.

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

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 to the solution design for DevOps adoption. The solution design must demonstrate **three (3)** of the following:
	• Current DevOps and source code state:
	  ○ Existing tools for managing code and automation
	  ○ Basic practices for managing and building/deploying/provisioning
	  ○ Related DevOps systems integrations
	• Migration or modernization approach:
	  ○ Relationships between existing systems/tools and proposed DevOps environments
	  ○ Tools and practices to migrate/modernize the DevOps environments
	• Proposed DevOps automation for application code including:
	  ○ Automated build and packaging tools and practices
	  ○ Automated or Shift-left application security including Software Composition Analysis and Static or Variant Code Analysis
	  ○ Automated deployment to Azure environment(s)
	• Proposed Infrastructure-as-code management(as appropriate):
	  ○ Code management practices for ARM Templates, Terraform or other Azure-compliant Infrastructure as Code
	  ○ Automated compliance checks(e.g., Azure Policy)
	  ○ Automated provisioning in both pre-production and production environments
	• Code security and sharing:
	  ○ Categorization of target code bases describing access restrictions
	  ○ Roles and permissions describing who can access, modify and/or maintain different codebases
	  ○ Pull-request or similar workflow describing how code quality and compliance will be verified
	  ○ Branch Protections/Policies used to ensure compliant code workflows

3.1 con't	• Learning and DevOps feedback loop:
	  ○ Monitoring and logging-in operational systems(e.g., Azure Monitor, Application Insights, etc.)
	  ○ Tools and practices providing developers/engineers access to operational data for troubleshooting and maintenance activities
	Required evidence:
	The partner must provide relevant solution design documents that address the preceding points as appropriate, for at least **three (3)** unique customers with Apps deployed to Azure, at least **one (1)** using DevOps with GitHub, completed in the last **twelve (12)** months. If a partner holds an active Kubernetes on Microsoft Azure specialization, or an active Modernization of Web Applications to Azure specialization only **one (1)** customer using DevOps with GitHub is required to pass this control.
	Acceptable Documentation: Design document, Project plan, Functional specifications, Architectural diagram, Automated tooling reports, and Physical and Logical diagrams

3.2	**Azure Well-Architected Review of Workloads** The partner must demonstrate usage of the Azure Well-Architected Review on DevOps with GitHub on Azure workloads. 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 matter 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 Microsoft Well Architected Review using the assessments in the Well Architected Reviews for at least **one (1)** unique customer with Apps deployed to Azure, using DevOps with GitHub, completed in the last **twelve (12)** months, indicating the customer's name. In the Well Architected Core Review, the **Operational Excellence** pillar must be completed.

4.0 Delivery	
The partner has robust methodologies for implementing GitHub and Azure in DevOps engagements.	
Requirement	
4.1	**Delivery** The partner must provide evidence of their ability to embed GitHub into DevOps engagements. **Required evidence:** The partner must provide documentation for at least **three (3)** unique customers with Apps deployed to Azure, at least **one (1)** using a DevOps with GitHub, completed in the last **twelve (12)** months. If a partner holds an active Kubernetes on Microsoft Azure specialization, or an active Modernization of Web Applications Azure specialization, only **one (1)** customer using DevOps with GitHub is required to pass this control Selected engagements must comply with the following criteria: • All **three (3)** engagements must use Git repositories to store engagement assets (e.g., application code, scripts, ML models, etc.), with at least **one (1)** engagement using GitHub Enterprise (Cloud, Server, or AE) • All **three (3)** engagements implement continuous integration or similar automated build strategy using GitHub Actions, Azure Pipelines, Jenkins, or Circle CI, with at least **one (1)** engagement using GitHub Actions To cover the entire sequence of the engagement, including design and production deployment, the documentation must include at least **two (2)** of the following: • Signed Statements of Work (SOWs) for all engagements • Solution design documents for all engagements • 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	
5.1	**Service Validation and Testing** The partner must validate the deployment and demonstrate the process and approach to testing and evaluating the DevOps process against customer expectations. **Required evidence:** Documentation of the testing and validation that addresses the preceding points for **three (3)** unique customers with Apps deployed to Azure, at least **one (1)** using a GitHub DevOps solution, completed in the last **twelve (12)** months. If a partner holds an active Kubernetes on Microsoft Azure specialization, or an active Modernization of Web Applications Azure specialization, only one (1) customer using DevOps with GitHub is required to pass this control. The documentation must indicate that the implemented solution met customer expectations, and it must include a sign-off from the customer.
5.2	**Post-deployment Documentation** The partner must provide post-deployment documentation to show that their customers are successfully leveraging the DevOps solution. Post-deployment documentation must include: • Updated design documentation reflecting the "as-built "DevOps implementation • Measurements or appropriate KPIs showing the performance of the solution (e.g., Cycle Time, Lead Time and/or similar Process performance metrics) • Post-deployment guidelines and recommendations for ongoing migration, adoption, and improvements. **Required evidence:** Documentation that addresses the preceding points for **three (3)** unique customers, with Apps deployed to Azure, at least **one (1)** using DevOps with GitHub, completed in the last **twelve (12)** months. If a partner holds an active Kubernetes on Microsoft Azure specialization, or an active Modernization of Web Applications Azure specialization only **one (1)** customer using DevOps with GitHub is required to pass this control.

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.