

مبادرة تمكين القطاع الحكومي للتحول الرقمي

مبادرة مشتركة بين الجهاز المركزي لتكنولوجيا المعلومات وشركة مايكروسوفت لدعم الجهات الحكومية ومساعدتها في وضع خارطة طريق للتحول الرقمي. تقدم المبادرة خدمات تقييم (Assessment) من خلال البرامج التالية :

برامج المبادرة



تقييم البنية التحتية

Infrastructure Assessment

- تحليل كامل للبنية التحتية الحالية وتوثيق كافة العوامل المرتبطة بها من ناحية الصيانة والتكاليف المباشرة والغير مباشرة.
- توصيات حول التطبيقات والبنية التحتية التي يفضل انتقالها الى السحابة مع وضع خارطة طريق حسب الأهداف والأولويات.
- تقديم دراسة مالية وفنية واضحة تتماشى مع الأهداف الأساسية للجهة.



تقييم التطبيقات والبرامج

Application Assessment

- عملية دراسة ومسح شاملة لجميع التطبيقات الموجودة في الجهة.
- تحديد 3-5 تطبيقات ذات الأولوية قابلة للتطوير والتحديث.
- وضع دراسة لتطوير هذه التطبيقات ومساعدة من قبل مايكروسوفت في تطويرها.



تقييم الأمن السيبراني

Cybersecurity Assessment

- تقييم وضع المؤسسة الحالي للأمن السيبراني.
- تقديم ملخص عن مواطن الضعف والمخاطر.
- بناء خارطة طريق الأمن السيبراني على أساس نموذج الاستعداد باستخدام ضوابط TM CIS
- وضع خطة واضحة لمعالجة نتائج التحليل الذي يقيم جميع مواطن الضعف الأمنية الحيوية بعد معرفة الرقم الحالي للمؤسسة (Score Secure)

النتائج المرجوة من المبادرة

عملية التقييم هي فرصة للتعرف على الجهة ومساعدتها على رسم أفضل مسار للمضي قدمًا. حيث يتم أخذ معلومات حول ما هو مهم لأعمالهم ، إلى جانب البيانات من بيئتهم، للوصول إلى تحليل شامل لوضعهم الحالي. وهذا التحليل هو جوهر توصياتنا النهائية.



منهجية المبادرة

تتبع المبادرة منهجية عمل تعتمد ركائزها على سرية البيانات والمعلومات وتحديد افضل المسارات بناء علي تقييم شامل بأحدث التقنيات والخبرات.

سرية البيانات والمعلومات

سرية البيانات والمعلومات هي أساس عملنا ومنهجيتنا ويتم مراعاتها في كل خطوة من خطوات عملنا مع الجهة

افضل المسارات

وضع أفضل المسارات وخطط العمل القابلة للتنفيذ الفوري مع مراعاة قيود العمل وأقل كلفة ممكنة

تقييم شامل

عملية تقييم شاملة باستخدام أحدث التقنيات مضاف إليها الخبرة الإحترافية لشركه مايكروسوفت

خطوات التنفيذ

بعد طلب الجهة الحكومية لبرامج المبادرة التي تود الإستفادة منها والتأكد من احتياجها الفعلي لهذه البرامج، يتم تنفيذ المراحل التالية لكل برنامج يتم اعتماده في فترة تتراوح مدتها من 4 إلى 6 أسابيع:

6	5	4	3	2	1
تقرير المخرجات	التوصيات	الوضع الحالي	تجميع البيانات	تأكيد نطاق العمل	فريق العمل
عرض المخرجات على القياديين بالجهة وشرح خطة التغيير والتوصيات وتحديد الخطوات القادمة.	إعداد التوصيات والمقترحات ووضعها في شكل نموذج عمل (Build a business case)	تحليل البيانات والمعلومات التي تم تجميعها ووضع صورة تفصيلية للوضع الحالي ومراجعتها مع الجهة.	تجميع البيانات والمعلومات المطلوبة حسب كل برنامج عمل. قد يتطلب الأمر استخدام بعض الأدوات المعتمدة من مايكروسوفت لتجميع تلك البيانات.	التأكيد على نطاق العمل مع الجهة وتحديد الإجراءات والموارد المطلوبة خلال فترة تنفيذ البرنامج.	يتم تحديد مسؤول الاتصال لتنسيق تنفيذ البرنامج المطلوب وفريق العمل المشارك في التنفيذ.

الخطوة التالية

على الجهة الحكومية الراغبة في الاستفادة من المبادرة أن ترسل البيانات التالية على البريد الإلكتروني tamkeen@cait.gov.kw :

- البرامج التي تود الاشتراك بها.
- تحديد ضابط اتصال من قبل الجهة .

Cybersecurity Assessment SOW

Contents

Introduction	1
Assessment overview	1
Before you begin	2
Letter of Engagement (LOE)	2
Incentive Payment Process	2
Learning about your customer	2
Data collection.....	2
Analysis.....	5
Delivering recommendations	6
Final Assessment Report.....	6
Cloud Adoption Resources	6

Introduction

Solution Assessments are to be used by partners in collaboration with the Solution Assessment Specialists (SAS) to help customers understand their current environment and receive recommended next steps for their cloud journey. It is important that partners deliver all the specific requirements articulated in this SOW to the customer, ensuring they receive the full value of this assessment.

Assessment overview

The Cybersecurity Assessment provides the customer with a foundational analysis of their cybersecurity state and areas of potential risk. The analysis will also provide guidance on cybersecurity programs and policies.

The assessment process captures information critical to the assessment output via modern discovery tools. The deliverable is the Final Assessment Report, which summarizes the process and findings and makes key next steps recommendations. Each project recommendation should clearly articulate the value proposition for undertaking the project.

Before you begin

Solution Assessments are a collaborative engagement between Microsoft, partners, and customers. To set clear expectations, outline engagement requirements, and define next steps, we require a Letter of Engagement (LOE) be delivered to, and accepted by, customers at the beginning of an assessment. Assessments cannot begin without an agreed upon LOE that has been reviewed by the SAS.

Letter of Engagement (LOE)

Microsoft expects the partner to communicate the following and gain agreement with the customer at the start of the project:

1. Discuss the scope of work for the assessment being performed and how it aligns to their cloud strategy, business objectives, and current challenges. Include a list of all deliverables, defining the scope and any scope limitations.
2. Ensure the assessment will address a clear challenge or need that the customer has, and that the opportunity has been qualified in terms of budget, timeline, and commitment from relevant stakeholders.
3. Review the [Conditions of Funding](#) with your customer to ensure they understand the resources required to complete a successful assessment.
4. Gain customer agreement on disclosure of assessment deliverables shared with Microsoft.
5. Confirm adherence to the [Microsoft Privacy Policy](#).
6. Obtain customer agreement to proceed with the assessment through either a physical signature or written electronic confirmation.

Incentive Payment Process

In order to receive payment via the Solution Assessment Incentive Program, you must adhere to the Proof of Execution (POE) process as documented in the [Solution Assessment Incentive Program Guide](#).

Learning about your customer

A Solution Assessment is an opportunity to learn about a customer and help them chart the best path forward. We take information about what is important to their business, along with data from their environment, to complete a thorough analysis of their current state. This analysis is at the core of our final recommendations.

Data collection

Within the scope of the project, it is expected that partners utilize modern tools for all data collection and discovery efforts. Check with your SAS about criteria for data collection tools. Check out the [Tools Overview](#) for more information.

Our approach

- A comprehensive assessment of the customer's existing IT infrastructure, including on-premises, cloud, and outsourced installations (as available for the in-scope environment)
- A complete inventory of relevant utilization such as CPU, network, RAM, disk, and storage as available through the modern tool reporting
- Through data discovery, make sure to identify:
 - System recovery failure logs
 - Windows Update availability on all machines

- System Center Endpoint Protection, anti-virus and/or firewall software
- Inventory of the password policy setting information from Active Directory (AD)

Basic, foundational, and organizational assessment data collection requirements:

For the Basic controls, through interviews/data discovery, make sure to answer/identify:

Basic Control	Collection Method	Deliverables/Inventory Data
1. Inventory and Control of Hardware Assets	Cybersecurity Questionnaire – Start Here	Enumerate all infrastructure platforms in-use by the customer.
	Cybersecurity Questionnaire – Basic (1.)	Answers to two (2) questions.
	MAP Toolkit or equivalent	Landscape overview to determine the extent of the organization’s assets. For Example, MAP Toolkit Reports: <ul style="list-style-type: none"> • InventoryResults; “Hardware Inventory” tab • ServerAndCloudEnrollment; “Windows Server” tab
2. Inventory and Control of Software Assets	Cybersecurity Questionnaire – Start Here	Enumerate the core business applications in-use by the customer. Enumerate all applications/services in-use by the customer. (Include PaaS, SaaS, IDaaS, ...)
	Cybersecurity Questionnaire – Basic (2.)	Answers to two (2) questions.
	Manual or Automated Collection	An overview of all network devices with vendor, type and firmware revision (if using SCCM or other tools that capture this information as part of discovery process).
	MAP Toolkit or equivalent	Life-cycle management inventory to determine the current status of all software assets including operating systems, database engines and applications. Check the End-of-Life status, service pack levels and versions. For Example, MAP Toolkit Reports: <ul style="list-style-type: none"> • LegacyWindowsServerInventory; “ServerInventory” tab • WindowsEnvironmentSummary; “Hardware Inventory Application Summary” tab • LinuxEnvironmentSummary; “Hardware Inventory” tab
	Optional: MDM Tooling	Life-cycle management inventory on mobiles devices including the apps. Check the End-of-Life status, service pack levels, and versions.
3. Continuous Vulnerability Management	Cybersecurity Questionnaire – Basic (3.)	Answers to two (2) questions.
	WSUS / Other	An inventory of the patch management status of the customer’s systems.
4. Controlled Use of Administrative Privileges	Cybersecurity Questionnaire – Basic (4.)	Answers to three (3) questions.
	AD Users & Computers or equivalent	An inventory of the Administrative Accounts, including Domain Admins, Enterprise Admins, Schema Admins, etc.
5. Secure Configuration for Hardware and Software on Mobiles Devices, Laptops, Workstations and Servers	Cybersecurity Questionnaire – Basic (5.)	Answers to two (2) questions.
	Microsoft Security Compliance Toolkit or equivalent	The secure configuration scan output of 5 sample systems (servers and clients).
6. Maintenance, Monitoring and Analysis of Audit logs	Cybersecurity Questionnaire – Basic (6.)	Answers to two (2) questions.
	Domain Controller Security Events, PowerShell Get-EventLog or other tooling	Detect failed logons (30 days) or abuse of privileges.

For the Foundational controls, through interviews/data discovery, make sure to answer/identify:

Foundational Control	Collection Method	Deliverables/Inventory Data
7. Email and Web Browser Protections	Cybersecurity Questionnaire – Foundational (7.)	Answers to three (3) questions.
	Manual or Automated collection	Collect the antispam protection DNS records for the email domains (SPF, DKIM and DMARC).
8. Malware Defenses	Cybersecurity Questionnaire – Foundational (8.)	Answers to two (2) questions.
	Antivirus management solutions like Intune or other tooling	An inventory of the presence, status and update status of System Center Endpoint Protection (SCEP), Windows Defender or other anti-virus software on all systems.
9. Limitation and Control of Network Ports, Protocols, and Services	Cybersecurity Questionnaire – Foundational (9.)	Answers to two (2) questions.
	Group Policy Management or tooling for collection	Collect the presence and status of Firewall software on all systems, also collect if there is a GPO to enforce this on all systems.
10. Data Recovery Capabilities	Cybersecurity Questionnaire – Start Here	Collect, or be informed on, the customer’s disaster recovery plans.
	Backup (Report) Tooling	Request a summarized (90 days) report on the current Backup and Restore status to determine the “recoverability” of the organization.
	Cybersecurity Questionnaire – Foundational (10.)	Answers to two (2) questions.
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	Cross-reference	Check for all network equipment collected in (Basic 3) if the current running firmware version is the latest stable firmware release of the vendor.
	Manual or Automated collection	Collect if all the network equipment is configured as accordingly to the approved company standard.
	Cybersecurity Questionnaire – Foundational (11.)	Answers to two (2) questions.
12. Boundary Defense	Manual or Automated collection	Collect the status of the security features like IDS and IPS that are used on the company firewall(s)
	Manual or Automated collection	Request a summarized overview of all the networks used, include also the allow and deny overview between the networks
	Cybersecurity Questionnaire – Foundational (12.)	Answers to three (3) questions.
13. Data Protection	Cybersecurity Questionnaire - Foundational (13.)	Answers to two (2) questions.
	Manual or Automated collection	<i>Use System Center Configuration Manager or other tools to detect and collect the presence and status of BitLocker or another encryption software.</i>
14. Controlled Access Based on the Need to Know	Cybersecurity Questionnaire - Foundational (14.)	Answers to three (3) questions.
	Manual collection	Request how the company policy states how sensitive data should be handled
15. Wireless Access Control	Cybersecurity Questionnaire – Foundational (15.)	Answers to two (2) questions.
	Through Manual or Automated by a tool like Wi-Fi Analyzer	Inventory the wireless networks and request access to the guest wireless network to determine guest isolation.

16. Account Monitoring and Control	Cybersecurity Questionnaire – Foundational (16.)	Answers to two (2) questions.
	Group Policy Management	An inventory of the password policy setting information from Active Directory.
	AD Users & Computers, PowerShell Get-ADUser or other tooling	Extract a list of all accounts, including their status (enabled/disabled) and password options. A check within the organization should provide clearance on legitimacy of account enablement.

For the Organizational controls, through interviews/data discovery, make sure to answer/identify:

Organizational Controls	Collection Method	Deliverables/Inventory Data
17. Implement a Security Awareness and Training Program	Cybersecurity Questionnaire – Organizational (17.)	Answers to two (2) questions.
18. Application Software Security	Cybersecurity Questionnaire – Organizational (18.)	Answers to three (3) questions.
	<i>Optional: Cybersecurity Questionnaire – Start Here</i>	<i>Collect how the company build applications are code checked and use secure coding</i>
19. Incident Response and Management	Cybersecurity Questionnaire – Organizational (19.)	Answer to one (1) question.
	Cybersecurity Questionnaire – Start Here	Be informed how the incident response procedure is setup and if there is a regular exercise
20. Penetration Tests and Red Team Exercises	Cybersecurity Questionnaire – Organizational (20.)	Answers to two (2) questions.
	Cybersecurity Questionnaire – Start Here	Be informed if there are regular external and internal penetration tests done
AD.1. IT Governance	Cybersecurity Questionnaire – Organizational (AD.1.)	Answers to three (3) questions.
	Cybersecurity Questionnaire – Start Here	Collect or be informed on the customer’s IT strategy and/or roadmap, including their current privacy and security concerns and action plans.
AD.2. Data Governance	Cybersecurity Questionnaire – Organizational (AD.2.)	Answers to three (3) questions.

Analysis

The data collected during the assessment should be analyzed and reviewed with the customer and the SAS. This data, along with the additional customer discovery, will provide a basis for the development of the Final Assessment Report recommendations and next steps.

- Review of current cloud environment mapped to optimized proposed environment based on the customer’s goals, including an assessment of capabilities and barriers to move to the cloud.
- Assessment of all business and technology requirements necessary to meet the identified customer challenge set out in the LOE.

Delivering recommendations

The most important outcome of a Solution Assessment is that customers receive detailed recommendations and next steps to shape their cloud journey and drive digital transformation. We require a Final Assessment Report be delivered to customers at the conclusion of an assessment.

Final Assessment Report

A Final Assessment Report must include:

1. **Executive Summary:** A high-level summary of project background and scope, data discovery.
2. **Summary of Current Environment:** An assessment of the customer's overall cybersecurity state, in relation to their IT infrastructure, including:
 - a. Service Pack deviations.
 - b. Anti-virus software/Anti-malware running in environment.
 - c. Password controls and policies.
 - d. Provide client lifecycle insights including hardware refresh candidates, giving consideration to the Surface portfolio.
3. A cybersecurity roadmap based on a maturity model using the CIS Controls™
4. Security risks on identify management and Secure Score results
5. **Business case:** Deliver a compelling business case aligned to the customer's initial objective, evaluating the benefit, cost, and risks of the proposed solution. Leverage the [Business Case Template](#) as needed.
6. **Recommended Next Steps:** Provide a customized Migration Plan that addresses scope, time, and cost, including recommendations for a base architecture and landing zone foundation.

Cloud Adoption Resources

The [Cloud Adoption Framework](#) (CAF) is a resource available for customers to help them understand their maturity when it comes to cloud adoption. Partners can look to leverage a maturity tracker, like CAF, to help customers understand their current position and the requirements for improving their cloud maturity.

Application Assessment SOW

Contents

Introduction	1
Assessment overview	1
Before you begin	1
Learning about your customer	2
Data collection.....	2
Analysis.....	2
Delivering recommendations	3
Final Assessment Report.....	3
Cloud Adoption Resources	3

Introduction

Solution Assessments are to be used by partners in collaboration with Solution Assessment Specialists (SAS) to help customers understand their current environment and receive recommended next steps for their cloud journey. It is important that partners deliver all the specific requirements articulated in this SOW to the customer, ensuring they receive the full value of this assessment.

Assessment overview

The Application Modernization Assessment assists customers in identifying and prioritizing applications for modernization to Azure, thereby enhancing business agility and streamlining processes to meet current and future business objectives. Applications are evaluated from both a business and architectural perspective to provide customers with cost consumption estimates, reference architecture design, and a modernization plan.

The assessment process captures information critical to the assessment output via modern discovery tools. The deliverable is the Final Assessment Report, which summarizes the process and findings and makes key next steps recommendations. Each project recommendation should clearly articulate the value proposition for undertaking the project.

Before you begin

Solution Assessments are a collaborative engagement between Microsoft, partners, and customers. To set clear expectations, outline engagement requirements, and define next steps, we require a Letter of Engagement

(LOE) be delivered to, and accepted by, customers at the beginning of an assessment. Assessments cannot begin without an agreed upon LOE that has been reviewed by the SAS.

Learning about your customer

A Solution Assessment is an opportunity to learn about a customer and help them chart the best path forward. We take information about what is important to their business, along with data from their environment, to complete a thorough analysis of their current state. This analysis is at the core of our final recommendations.

Data collection

Within the scope of the project, it is expected that partners utilize modern tools for all data collection and discovery efforts. Check with your SAS about criteria for data collection tools.

Our approach

- Discuss with the customer the scope of which applications will be in the range for discovery, targeting customized applications as the priority targets:
 - The scope of this assessment should be established first with a scan of all applicable applications.
 - Consideration should be given to:
 - If the customer's full infrastructure details and dependencies are known
 - Applications in the languages of Java, .NET, JavaScript, & PHP
 - If the customer has access to the source code
 - After the full inventory of applications has been collected and reviewed with the customer, 3 – 5 applications should be agreed to for analysis for migration.
- Scan application source code, database scripts, and configuration files to identify specific code/DB changes required to successfully migrate applications & data to Azure.

Analysis

The data collected during the assessment should be analyzed and reviewed with the customer and the SAS. This data, along with the additional customer discovery, will provide a basis for the development of the Final Assessment Report recommendations and next steps.

- Review of current cloud environment mapped to proposed optimized environment based on the customer's goals, including an assessment of capabilities and barriers to move to the cloud.
- Assessment of all business and technology requirements necessary to meet the identified customer challenge set out in the LOE.
- Assess applications for migration to Containers, VMs and App Services.
- Assess databases for migration to Azure VMs, SQL Azure or DBMI, as well as Elastic Pool.
- Detailed time estimates (days and hours) & monthly costs for Containers, VMs and App Services.
- Detailed cost estimates for different scenarios (e.g. Apps: Containers, VMs, App Services; Data: VMs, SQL Azure or DBMI).

Delivering recommendations

The most important outcome of a Solution Assessment is that customers receive detailed recommendations and next steps to shape their cloud journey and drive digital transformation. We require a Final Assessment Report be delivered to customers at the conclusion of an assessment.

Final Assessment Report

A Final Assessment Report must include:

1. **Executive Summary:** A high-level summary of project background and scope, data discovery.
2. **Summary of Current Environment:** A summary review of the collected and assessed applications and data, be sure to:
 - a. Identify risks to business on data security loss and vulnerabilities by identifying current or upcoming end-of-life products and/or hardware with upgrade path recommendations.
 - b. Include guidance on best practices for governance principles (security, identity, cost, deployment acceleration) for applications in scope.
 - c. Provide analysis and recommendations on the applications in scope to assess their readiness for modernization via the following:
 - i. App Modernization estimates
 - ii. Containerized app estimates
 - iii. SQL database migration
 - iv. SQL Managed Instances
 - v. Azure cost analysis
 - vi. Detailed coded level analysis
 - vii. App portfolios roll up
3. **Business case:** Deliver a compelling business case aligned to the customer's initial objective, evaluating the benefit, cost, and risks of the proposed solution.
4. **Recommended Next Steps:** Provide a customized Migration Plan that addresses scope, time, and cost, including recommendations for a base architecture and landing zone foundation.

Cloud Adoption Resources

The [Cloud Adoption Framework](#) (CAF) is a resource available for customers to help them understand their maturity when it comes to cloud adoption. Partners can look to leverage a maturity tracker, like CAF, to help customers understand their current position and the requirements for improving their cloud maturity.

Infrastructure Assessment SOW

Contents

Before you begin	1
Learning about your customer	2
Data collection.....	2
Analysis.....	2
Delivering recommendations	2
Final Assessment Report.....	2
Cloud Adoption Resources	3

Assessment overview

The Data and Infrastructure Migration Assessment is designed to provide the customer with an end-to-end analysis and mapping of their entire IT estate (both physical and virtual), taking into consideration customer plans, current deployment, usage, processes, and data. This analysis will help us evaluate the customer’s overall infrastructure in relation to their on-premises and cloud-strategy as well as identify modernization opportunities in Windows Server and SQL environments. Our goal is to help customers optimize their current application and server workloads while providing insights on the business and technology benefits of moving additional workloads to the cloud.

The assessment process captures information critical to the assessment output via modern discovery tools. The deliverable is the Final Assessment Report, which summarizes the data analysis and makes key next steps recommendations. Each project recommendation should clearly articulate the value proposition for undertaking the project.

Before you begin

Solution Assessments are a collaborative engagement between Microsoft, partners, and customers. To set clear expectations, outline engagement requirements, and define next steps, we require a Letter of Engagement (LOE) be delivered to, and accepted by, customers at the beginning of an assessment. Assessments cannot begin without an agreed upon LOE that has been reviewed by the SAS.

Learning about your customer

A Solution Assessment is an opportunity to learn about a customer and help them chart the best path forward. We take information about what is important to their business, along with data from their environment, to complete a thorough analysis of their current state. This analysis is at the core of our final recommendations.

Data collection

Within the scope of the project, it is expected that partners utilize modern tools for all data collection and discovery efforts. Check with your SAS about criteria for data collection tools.

Our approach

- A comprehensive assessment of the customer's existing Windows Server, SQL Server and VM infrastructure, including on-premises, cloud, and outsourced installations (as available for the in-scope environment)
- A complete hardware and software inventory of the customer's physical and virtual servers, including relevant performance data and utilization such as CPU, network, RAM, disk, and storage as available through the modern tool reporting
- Information on how the customer is using or plans to use SQL Server, including what types of workloads or applications are currently implemented and what future implementation plans are under consideration
- Customer's server workload vision and/or roadmap

Analysis

The data collected during the assessment should be analyzed and reviewed with the customer and the SAS. This data, along with the additional customer discovery, will provide a basis for the development of the Final Assessment Report recommendations and next steps.

- Review of current cloud environment mapped to proposed optimized environment based on the customer's goals, including an assessment of capabilities and barriers to move to the cloud.
- Assessment of all business and technology requirements necessary to meet the identified customer challenge set out in the LOE.
- Review of existing workloads and related infrastructure to identify consolidation and/or modernization opportunities.

Delivering recommendations

The most important outcome of a Solution Assessment is that customers receive detailed recommendations and next steps to shape their cloud journey and drive digital transformation. We require a Final Assessment Report be delivered to customers at the conclusion of an assessment.

Final Assessment Report

A Final Assessment Report must include:

1. **Executive Summary:** A high-level summary of project background and scope, data discovery.
2. **Summary of Current Environment:** A summary review of the customer's IT environment captured in data collection should be sure to:
 - a. Identify risks to business on data security loss and vulnerabilities by identifying current or upcoming end-of-life products and/or hardware with upgrade path recommendations.

- b. Review consumption information on installed products that are unused or underutilized, with a consumption plan for adoption of technology.
 - c. Recommend users, workloads, and applications prioritized to move to Azure.
 - d. Deliver a full set of recommendations on optimizing server workload and virtualization usage in Azure.
3. **Business case:** Deliver a compelling business case aligned to the customer's initial objective, evaluating the benefit, cost, and risks of the proposed solution.
 4. **Recommended Next Steps:** Provide a customized Migration Plan that addresses scope, time, and cost, including recommendations for a base architecture and landing zone foundation.

Cloud Adoption Resources

The [Cloud Adoption Framework](#) (CAF) is a resource available for customers to help them understand their maturity when it comes to cloud adoption. Partners can look to leverage a maturity tracker, like CAF, to help customers understand their current position and the requirements for improving their cloud maturity.