Amazon Selling Partner

Assessment Kick-Off

This document outlines our security assessment requirements, detailing both the evaluation process and key technical focus areas. Understanding these elements in advance will help you prepare effectively and ensure a smooth assessment experience.

Resources to help you prepare for the assessment:

1. Video Resources: Open Link
2. SP-API Technical Papers: Open Link
3. Security assessments: Best Practices and Readiness-Blog Post: Open Link
4. Check out our new Security Product: Open Link
5. Selling Partner API Policies
    - Amazon Services API Developer Agreement: Open Link
    - Data Protection Policy: Open Link
    - Acceptable Use Policy: Open Link

Assessment Overview and Timeline

Key details

Why?
Amazon Agents conduct the security assessment in accordance with regulatory requirements and assist developers in improving their cyber security and data use posture

Support Provided
Amazon will assist you during the remediation process by providing the support of solution architects that can help tackle the plan of action (POA) to solve for the gaps in controls

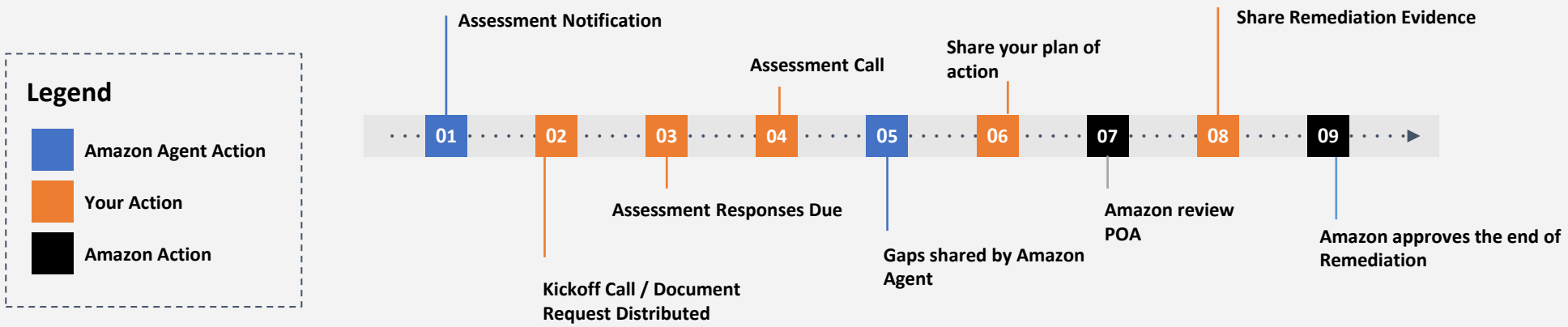
How?
The assessment has three stages:

- **Submit Assessment:** Provide responses to questions in relation to the assessment
- **Assessment Call:** Discuss the controls in place to manage the Amazon data received
- **Remediation**: Implementing solutions for any gaps

Time and Effort
The total assessment takes an estimated 8 hours of time across the month. The split is as follows:

- Assessment Submission – **4-6 hours**
- Assessment Call – **2 hours**
- Follow up questions – **2 hours** *(done via email communication between Amazon Agent and developer)*

Assessment Timeline



Key Assessment Domains

For each of the following topics, please identify key personnel who are knowledgeable about each of the various processes. These personnel would need to be available to provide insight during the assessment call.

#	Domain	Topics Covered
1	Business and system Overview	Understanding an overview of services and processes. Understanding the network architecture and flow of data through the environment.
2	Security governance	• Policy management, • Risk and Compliance Regulations Management, • Privacy regulation management, • Third party risk management
3	Infrastructure security*	• Data Storage • Asset management and security controls for assets • Asset Baseline Configuration • Asset destruction • Anti-malware controls
4	Data protection*	• Tools utilized to protect data • Encryption protocols for data at rest and in transit • Management and classification of data • Data retention and back-up • Dark Web Review • API Key security

*Potential topics where key personnel may need to screen share with the assessment team

Key Assessment Domains

#	Domain	Topics Covered
5	Network security and vulnerability management*	• Security controls utilized to manage, monitor and protect the network. • Vulnerability Management • Remediation of Vulnerabilities • Network Segregation
6	Application security*	• Software development lifecycle (including Software Testing) • Change Management
7	Identity and access management*	• Access provisioning and de-provisioning • Privileged access Management • Remote access • Password Management
8	Security monitoring and incident response	• Log management • Incident management plan
9	Privacy	• Management of privacy regulation requirement • Movement of data • Security Awareness Training • Data subject rights
10	Data Handling and Management	Various stages of the Amazon data lifecycle • Collection & Storage • Access • Transfer
11	Third-Party Integration	• Amazon data sharing with third parties • Data sharing process and mechanism
12	Customer Support	• Seller support tools (CRM) • Seller support process and mechanism

Frequently Asked Questions

1. ***Why are we being assessed?***
   - Developers are selected for assessment based on a variety of factors, including the nature and extent of their data access, as well as the potential risks associated with such access. The primary purpose of these assessments is to ensure that developers are effectively managing and safeguarding sensitive data in alignment with Amazon's data and privacy policies. This process also involves verifying adherence to the most recent updates to Amazon's assessment framework. Through these assessments, we aim to maintain high standards of data security and privacy, thereby protecting both the company and its customers.

2. ***Who needs to be on the assessment call?***
   - To ensure a thorough and efficient assessment process, it is essential that you include team members who possess comprehensive knowledge and the capability to address all relevant topics. Specifically, individuals who are familiar with and can speak to the areas outlined in the Key Assessment Domains section should be present. This might include representatives from your data security team, compliance officers, and any other personnel involved in data handling and protection. Their expertise and insights will be crucial in providing accurate and complete information during the assessment.

3. ***What if we have gaps and are currently not complaint?***
   - The goal of the assessment is to identify any potential gaps in your current practices and to assist you in addressing and remediating these issues. If your organization is found to be non-compliant with Amazon's standards, it is important to take prompt action to close these gaps. We encourage you to work closely with your internal team as well as with the Amazon team to develop and implement a remediation plan within the specified timeframe. During this period, it is imperative that you remain responsive and open to communication, as this will facilitate a smoother and more effective resolution of the identified issues.

4. ***Will I be assessed again?***
   - Amazon's commitment to data security and privacy involves regularly updating its security framework to address emerging threats and evolving best practices. Consequently, re-assessments may be initiated based on these updates or other relevant factors. By periodically re-evaluating compliance with our updated framework, we aim to ensure that developers meet our stringent security standards. Therefore, it is possible that you may undergo re-assessment in the future.

5. ***How much will this assessment cost us?***
   - The assessment process is provided at no cost to you and will be conducted by an Amazon Agent. This complimentary service is part of Amazon's commitment to maintaining high standards of data security and privacy across developers and partners.