IBM Application Security on Cloud

This Service Description describes the Cloud Service IBM provides to Client. Client means the company and its authorized users and recipients of the Cloud Service. The applicable Quotation and Proof of Entitlement (PoE) are provided as separate Transaction Documents.

1. Cloud Service

IBM Application Security on Cloud provides a single place to assist the Client in identifying security vulnerabilities (such as SQL Injection, Cross-Site Scripting, and Data Leakage) for a variety of applications. The service includes various types of application security scanning techniques, each of which identifies security issues in that application.

IBM Application Security on Cloud provides the following capabilities:

- Scanning Mobile Applications for security vulnerabilities. This is done via interactive (glassbox) security analysis technologies.
- Scanning production or pre-production, publicly facing or on private network, Web sites for security vulnerabilities. This is done via dynamic (blackbox) security analysis techniques.
- Scanning the dataflows within Web and Desktop applications for security vulnerabilities. This is done via static (whitebox) security analysis techniques.
- Detailed security vulnerability reports that include both high-level summaries of the findings and remediation steps that can be followed by developers.
- Integration with various DevOps platforms.

1.1 IBM Application Analyzer

IBM Application Analyzer can be ordered per Application Instance, per Job (scan), or as a full Instance and allows the following types of scanning:

- **Dynamic Analyzer** – Test pre-production or production websites via DAST techniques
- **Mobile Analyzer** – Test iOS or Android binaries via IAST techniques
- **Static Analyzer** – Test byte - or source-code data flow via SAST techniques

1.2 Set Up Service

IBM Application Security on Cloud Consulting Services is a productized set up service for Application Analyzer. The Service uses IBM consultants to provide guidance and assistance with testing and managing application risk. IBM Application Security on Cloud Consulting Services are purchased as blocks of Engagements that may be expended in the quantities set forth below to request and make use of the following specific services:

a. **Fast Start** [Uses one (1) Engagement unit]

The Fast Start service provides expertise and guidance for using the Application Security on Cloud testing and risk management features. After Client has confirmed successful login to the Application Security on Cloud portal, IBM will facilitate a web conference for up to two (2) hours and two (2) active participants to provide education on basic AppSec on Cloud service configurations and functions including scan types, running scans, reviewing reports and installing associated tools and plug-ins. The Fast Start service is completed after the completion of the (a) client education webinar, (b) installation of applicable tools and plug-ins, and (c) assisted Client to set up and run Client's first scan.

b. **Assessment Review** [Uses two (2) Engagement units]

The Assessment Review service provides assistance reviewing a test result, including understanding and prioritizing the remediation of vulnerabilities in the application. IBM will facilitate a web conference for up to one (1) hour and two (2) active participants to provide an overview of the vulnerabilities found and overall security risk of the application and a detailed discussion into the application security vulnerabilities found including (1) how the vulnerability was tested, (2) how the vulnerabilities were detected, (3) what is the risk of each vulnerability, and (4) provide general fix

recommendations to help remediate the vulnerability. The review will be based exclusively on the test result and will not be a review of the source code itself. Client will review the test result and will identify to IBM the test result for review prior to the web conference. The Assessment Review service is completed after the completion of the web conference

c. **Scan for Me** [Uses four (4) Engagement units]

The Scan for Me service provides an IBM application security expert who will configure and run a scan, validate the results, and conduct a report briefing to review the findings. Client will allow an IBM consultant access to its ASoC environment to configure and run a scan, validate the results, provide recommendations on remediation prioritization, and conduct a report briefing of the results. IBM will facilitate a web conference for up to one (1) hour and two (2) active participants to provide an overview of the vulnerabilities found and overall security risk of the application and a detailed discussion into the application security vulnerabilities found including (1) how the vulnerability was tested, (2) how the vulnerabilities were detected, (3) what is the risk of each vulnerability, and (4) provide general fix recommendations to help remediate the vulnerability. If requested, and up to 30 days after the initial scan, IBM will provide a rescan using the original scan configuration to verify security fixes only, not to test new functionality, validate results and deliver report to the client. The Scan for Me service is completed after the completion of the web conference to review the initial scan results or, if applicable, the completion of the rescan as requested by the Client and delivery of the rescan report to the Client.

d. **Advisor on Demand** [Uses seven (7) Engagement units]

The Advisor on Demand service provides up to twenty (20) hours of an IBM consultant's time that can be used for activities related to the Cloud Service. The IBM consultant will assist with application security specific topics, including, but not limited to, program management, security testing prioritization, remediation strategies, source code analysis and source code repair. IBM will work with Client to understand and create a project schedule with specific Client requirements, including project goals, relevant technologies, desired timelines, expected deliverables, and estimated number of Advisor on Demand service engagements. Client must provide access to necessary applications, systems and documentation required to perform the services. The Advisor on Demand service is completed when up to 20 hours of security expertise has been performed and/or after the project schedule and/or the documented deliverables defined in the project schedule have been delivered to the Client.

e. **Application Penetration Testing** -- three options:

(1) **Compliance/Entry-Level Application Penetration Test**, which includes up to forty (40) hours of Consultant time, and focuses on Single-step logic flaws, and Simpler versions of injection flaws. Uses fifteen (15) Engagement units.

(2) **Standard Application Penetration Test**, which includes up to sixty (60) hours of Consultant time, and expands the focus to include Logic flaws in multi-step work flows, Complex versions of injection flaws and Analysis of complex data types. Uses twenty-one (21) Engagement units.

(3) **Advanced Application Penetration Test**- Up to eighty (80) hours of Consultant time, and expands the focus to include Reverse engineering of compiled executables, Dissection of custom network protocols, In-depth analysis of publically available libraries and frameworks. Uses twenty-seven (27) Engagement units

The application penetration testing service provides an IBM resource to perform testing and exploitation of an application, the delivery of a test report, and a report briefing to explain the findings and associated risks.

IBM will facilitate a project initiation call for up to one (1) hour and two (2) active participants to review Client's environment and organization, including application platform, architecture, frameworks, supporting infrastructure, known security problems or concerns associated with the application, preliminary testing schedule and emergency contact plan.

IBM will conduct the application penetrating testing including, but not limited to: identification of common vulnerabilities such as SQL injection and cross-site scripting, assessment of the strengths and weaknesses of existing security controls such as input validation, authentication, and authorization, check for proper enforcement of business logic, validation of proper use of secure protocols, identification of session handling flaws, and verification of proper security controls on

login, password recovery, password policy, and other user management functions. Findings will be documented in the Application Penetration Test Report. IBM will facilitate a web conference for the report briefing for up to one (1) hour. The Application Penetration Test service is completed when the allotted consultative time has been used, the web conference has been conducted and the final Application Penetration Test Report has been delivered to the Client.

1.2.1 Set Up Services Responsibilities

IBM will:

- provide Set Up Services using Engagement units purchased by the Client and per the term of the Client's order
- have completed a Set Up Service when the completion criteria described in Section 1.2 are completed.

Client agrees:

- to be responsible for all charges associated with all Engagement requests made by Client during the contract term;
- and acknowledges, that purchased Engagement units must be used within the initial contract term and do expire if unused by the contract period end date.
- To initiate a formal request for all Set Up Services at least 30 days prior to the end date of the subscription.

In the performance of any Set Up Service, IBM may request information and reasonable cooperation from Client. Failure to provide requested information or cooperation in a timely manner by the Client may, as determined by IBM, result in Engagement unit charges as required by the services or the delay in performance of the applicable service.

In order for IBM to perform the testing accurately, Client agrees to follow IBM instructions in preparing and maintaining the environment for the testing period.

2. Security Description

This Cloud Service follows IBM's data security and privacy principles for IBM SaaS which are available at www.ibm.com/cloud/data-security and any additional terms provided in this section. Any change to IBM's data security and privacy principals will not degrade the security of the Cloud Service.

This Cloud Service is not designed to any specific security requirements for regulated content, such as personal information or sensitive personal information. Client is responsible to determine if this Cloud Service meets Clients needs with regard to the type of content Client uses in connection with the Cloud Service.

IBM does not operate as a provider of services regulated by the Federal Communications Commission ("FCC") or state regulatory authorities ("State Regulators"), and does not intend to provide any services which are regulated by the FCC or State Regulators. If the FCC or any State Regulator imposes regulatory requirements or obligations on any services provided by IBM hereunder, IBM may: (a) modify, replace, or substitute products at Client's expense, and/or (b) change the way in which such services are provided to Client to avoid the application of such requirements or obligations to IBM (for example, by acting as Client's agent for acquiring such services from a third party common carrier).

3. Technical Support

During the subscription period and after IBM notifies Client that access to the Cloud Service is available, technical support is provided via online forums and as standard support during the period of time in which the Client incurs Pay per Use charges. From within this Cloud Service, Clients can submit a support ticket or open a chat session for assistance. IBM will make available the IBM Software as a Service Support Handbook which provides technical support contact information and other information and processes.

Severity	Severity Definition	Response Time Objectives	Response Time Coverage

1	Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.	Within 1 hour	24x7
2	Significant business impact: A service business feature or function of the service is severely restricted in its use or Client is in jeopardy of missing business deadlines.	Within 2 business hours	M-F business hours
3	Minor business impact: Indicates the service or functionality is usable and it is not a critical impact on operations.	Within 4 business hours	M-F business hours
4	Minimal business impact: An inquiry or non-technical request	Within 1 business day	M-F business hours

3.1 Access to Client Data

IBM will be able to access Client data for the purpose of diagnosing issues with the service, and facilitating scans of Client's application by the service. IBM will access the data only for the purposes of fixing defects or to provide support for IBM products or services.

4. Entitlement and Billing Information

4.1 Charge Metrics

The Cloud Service is available under the charge metrics specified in the Transaction Document:

a. Job is a unit of measure by which the Cloud Service can be obtained. A Job is an object within the Cloud Service that cannot be further divided and represents a computing process including all its sub-processes. Sufficient entitlements must be obtained to cover the total number of Jobs which are processed or managed by the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.

b. Application Instance is a unit of measure by which the Cloud Service can be obtained. An Application Instance entitlement is required for each instance of an Application connected to the Cloud Service. If an Application has multiple components, each of which serves a distinct purpose and/or user base, and each of which can be connected to or managed by the Cloud Service, each such component is considered a separate Application. Additionally, test, development, staging, and production environments for an Application are each considered to be separate instances of the Application and each must have an entitlement. Multiple Application Instances in a single environment are each considered to be separate instances of the Application and each must have an entitlement. Sufficient Entitlements must be obtained to cover the number of Application Instances connected to the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.

   For this Cloud Service, Application Instances are consecutive scans of a single application further defined as follows:

   - For Dynamic Testing: a web site addressable via public or private URL. Each application Instance entitles a site of up to 5,000 pages in a single domain.
   - For Static Testing: a unit of code built for a single executable environment. Each Application Instance entitles scanning units of code up to 1,000,000 lines.
   - For Mobile Testing: a unit of binary code that can be executed on a mobile device. Each different mobile platform (e.g., iOS and Android) constitute different application instances.

c. Instance is a unit of measure by which the Cloud Service can be obtained. An Instance is access to a specific configuration of the Cloud Service. Sufficient entitlements must be obtained for each Instance of the Cloud Service made available to access and use during the measurement period specified in Client's Proof of Entitlement (PoE) or Transaction Document.

   For each Instance entitlement there is no limit on the number of Jobs performed or Application Instances (Applications connected), provided, however, that no more than 30 Jobs can be running at any given time.

d. Engagement is a unit of measure by which the services can be obtained. An Engagement consists of professional and/or training services related to the Cloud Service. Sufficient entitlements must be obtained to cover each Engagement.

4.2 Partial Month Charges

A partial month charge as specified in the Transaction Document may be assessed on a pro-rated basis.

4.3 Overage Charges

If actual usage of the Cloud Service during the measurement period exceeds the entitlement specified in the PoE, Client will be charged for the overage as specified in the Transaction Document.

4.4 Set Up Charges

Client will be charged for set up as specified in the Transaction Document.

5. Term and Renewal Options

The term of the Cloud Service begins on the date IBM notifies Client of their access to the Cloud Service, as documented in the PoE. The PoE will specify whether the Cloud Service renews automatically, proceeds on a continuous use basis, or terminates at the end of the term.

For automatic renewal, unless Client provides written notice not to renew at least 30 days prior to the term expiration date, the Cloud Service will automatically renew for the term specified in the PoE.

For continuous use, the Cloud Service will continue to be available on a month to month basis until Client provides 30 days written notice of termination. The Cloud Service will remain available to the end of the calendar month after such 30 day period.

6. Additional Terms

Security scans may not identify all security risks in an application, nor are they designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life support systems, nuclear facilities, or any other applications in which failure to identify security risks could lead to death, personal injury, or property damage. Security scans are not warranted to operate uninterrupted or error free.

The Cloud Service can be used to help Client meet compliance obligations, which may be based on laws, regulations, standards or practices. Any directions, suggested usage, or guidance provided by the Cloud Service does not constitute legal, accounting, or other professional advice, and Client is cautioned to obtain its own legal or other expert counsel. Client is solely responsible for ensuring that Client and Client's activities, applications and systems comply with all applicable laws, regulations, standards and practices. Use of this Cloud Service does not guarantee compliance with any law, regulation, standard or practice.

The Cloud Service performs invasive and non-invasive tests on the website and web or mobile application Client chooses to scan. Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. Client authorizes IBM to perform the Services as described herein and acknowledges that the Services constitute authorized access to Client's computer systems. IBM may disclose this grant of authority to a third party if deemed necessary to perform the Services.

The testing entails certain risks, including without limitation the following:

a. Client's computer systems while running applications under test may hang or crash, resulting in temporary system unavailability or loss of data;

b. the performance and throughput of Client's systems, as well as the performance and throughput of associated routers and firewalls, may be temporarily degraded during testing;

c. excessive amounts of log messages may be generated, resulting in excessive log file disk space consumption;

d. data may be changed or deleted as a result of probing vulnerabilities;

e. alarms may be triggered by intrusion detection systems;

f. emails may be triggered by the email function of the web application being tested;

g. the Cloud Service may intercept the traffic of the monitored network for the purpose of looking for events.

Any service level agreement rights or remedies provided by IBM and relating to the websites or applications subject to testing will be waived during any testing activity.

In the event that Client inputs authenticated log-in credentials for the application under test into the Cloud Service, Client should only input such credentials for test accounts and not for production users. Use of production user credentials may result in personal data being transmitted via the Cloud Service.

The Cloud Service may be configured to scan production web applications. When Client sets the scan type as "production," the service is designed to perform scans in a manner that reduces the risks listed above; however, in certain situations the Cloud Service may lead to performance degradation or instability within the tested production sites and infrastructure. IBM makes no warranties or representations with respect to the suitability of using the Cloud Service to scan production sites

IT IS CLIENT'S RESPONSIBILITY TO DETERMINE IF THE CLOUD SERVICE IS APPROPRIATE OR SAFE FOR CLIENT'S WEBSITE, WEB APPLICATION, MOBILE APPLICATION OR TECHNICAL ENVIRONMENT.

The Cloud Service is designed to identify a variety of potential security and compliance issues in mobile and web applications and web services. It does not test all vulnerabilities or compliance risks, nor does it act as a barrier to security attacks. Security threats, regulations and standards continually change, and the Cloud Service may not reflect all such changes. The security and compliance of Client's web application, systems and employees, and any remedial actions, are Client's responsibility alone. It is solely within Client's discretion to use or not use any of the information provided by the Cloud Service.

Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. CLIENT IS RESPONSIBLE FOR ENSURING THAT CLIENT DOES NOT USE THE CLOUD SERVICE TO SCAN ANY WEBSITES AND/OR APPLICATIONS OTHER THAN WEBSITES AND/OR APPLICATIONS OWNED BY CLIENT OR THOSE THAT CLIENT HAS THE RIGHT AND AUTHORITY TO SCAN.

For the purpose of clarity, Client content described in the Data Protection section of the Cloud Service Agreement is also deemed to include data that may become accessible to IBM during Application Penetration Testing.

6.1 Systems Owned by a Third Party

For systems (which for purposes of this provision includes but is not limited to applications and IP addresses) owned by a third party that will be the subject of testing hereunder, Client agrees:

a. that prior to IBM initiating testing on a third party system, Client will obtain a signed letter from the owner of each system authorizing IBM to provide the Services on that system, and indicating the owner's acceptance of the conditions set forth in the section entitled "Permission to Perform Testing" and to provide IBM with a copy of such authorization;

b. to be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these systems by IBM's remote testing to the system owner, and

c. to arrange for and facilitate the exchange of information between the system owner and IBM as deemed necessary by IBM.

Client agrees:

- to inform IBM immediately whenever there is a change in ownership of any system that is the subject of the testing hereunder;
- not to disclose the deliverables, or the fact that IBM performed the Services, outside Client's Enterprise without IBM's prior written consent; and
- to indemnify IBM in full for any losses or liability IBM incurs due to third party claims arising out of Client's failure to comply with the requirements of this section entitled, "Systems Owned by a Third Party" and for any third party subpoenas or claims brought against IBM or IBM's subcontractors or agents arising out of (a) testing the security risks, exposures or vulnerabilities of the systems that are the subject of testing hereunder, (b) providing the results of such testing to Client, or (c) Client's use or disclosure of such results.

6.2 Cookies

Client is aware and agrees that IBM may, as part of the normal operation and support of the Cloud Service, collect personal information from Client (Client's employees and contractors) related to the use of the Cloud Service, through tracking and other technologies. IBM does so to gather usage statistics and information about effectiveness of our Cloud Service for the purpose of improving user experience and/or tailoring interactions with Client. Client confirms that it will obtain or have obtained consent to allow IBM to process the collected personal information for the above purpose within IBM, other IBM companies and

their subcontractors, wherever we and our subcontractors do business, in compliance with applicable law. IBM will comply with requests from Client's employees and contractors to access, update, correct or delete their collected personal information.

As part of the Cloud Service, that includes reporting activities, IBM will prepare and maintain de-identified and/or aggregate information collected from the Cloud Service (called "Security Data"). The Security Data will not identify the Client, or an individual except as provided in (d) below. Client herein additionally agrees that IBM may use and/or copy the Security Data only for the following purposes:

a. publishing and/or distributing the Security Data (e.g., in compilations and/or analyses related to cybersecurity);

b. developing or enhancing products or services;

c. conducting research internally or with third parties; and

d. lawful sharing of confirmed third party perpetrator information.

6.3 Enabling Software

This Cloud Service includes enabling software, which may be used only in connection with Client's use of the Cloud Service and only for the Cloud Service term.