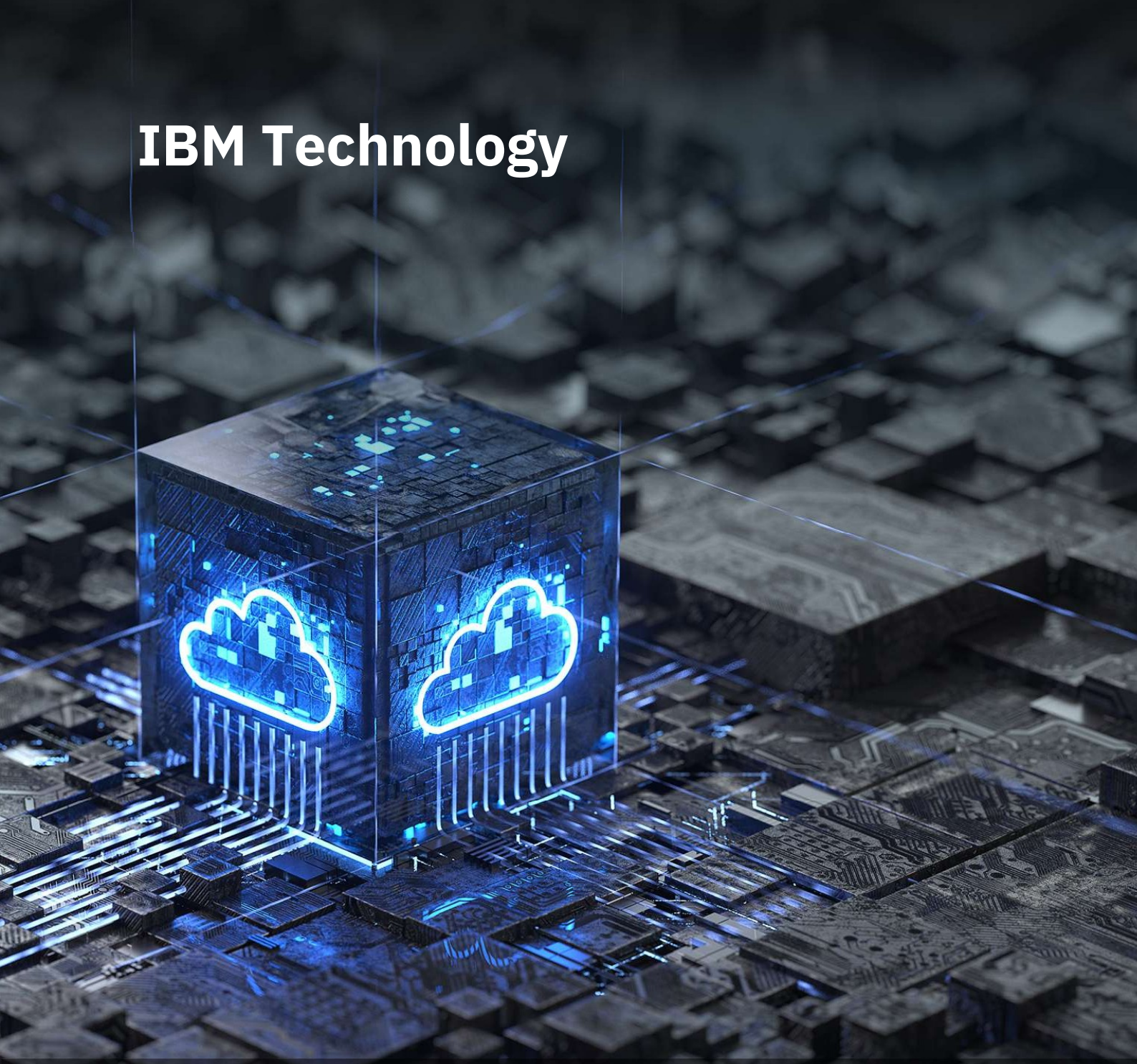
IBM Technology



G-Cloud 15
IBM – Verify

Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

IBM Verify

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at http://www.ibm.com/terms/csa (or equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

IBM Verify provides Single Sign-On (SSO), multi-factor authentication (MFA) and identity lifecycle controls for internal (workforce) and external (customer) user types. Client Instances have a maximum aggregated transaction rate limit of 400 Transactions per second (TPS) for each Production Instance and 100 TPS for each Non-Production Instance. Scenarios, such as user login and MFA, performed by this service may consist of multiple transactions.

Performance and load testing on any Client instance is permitted only when the Client submits a request via a support ticket at least one week prior to the planned testing period and IBM confirms in writing the test time and planned traffic volume. IBM will advise Client of the maximum aggregated transaction rate limit ("Test Rate Limit") applicable during testing as part of the written confirmation. The Test Rate Limit will not be less than the maximum aggregated transaction rate limit set out in a Transaction Document or Client's maximum growth projections as previously disclosed to IBM for the test. IBM reserves the right to not allow performance and load testing during the requested period, and in such event, IBM will provide an alternative test time. Notwithstanding anything to the contrary in this section, IBM is not obligated to permit the performance and load testing if the parties cannot agree on the parameters or other details pertaining to the proposed performance and load testing.

The data obtained from Client's performance and load testing (collectively "Testing Data") is IBM confidential information (governed under s. 5.3 below) and can only be used for Client's internal testing and validation purposes. Client cannot disclose Testing Data without IBM's prior written consent.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Verify (SaaS)

IBM Verify helps Clients secure user productivity with cloud-delivered, Single Sign-On (SSO), multi-factor authentication, lifecycle management, adaptive authentication, and identity governance under a single part number. This Cloud Service also supports access to thousands of popular cloud service applications, and in-house applications, with hundreds of pre-built templates for faster integration.

- Single Sign-On

  This Cloud Service delivers Single Sign-On (SSO) via SAML and Open ID Connect (OIDC), Authentication as a Service for cloud-based API authorization, an application launchpad, administrator reporting and an analytics dashboard. This Cloud Service connects users to applications using modern standards-based authentication and federation protocols, including hundreds of connectors to common applications. This Cloud Service includes the IBM Verify Application Gateway software program, as enabling software, to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications. It also tightly integrates with the separately licensed, on-premises IBM Verify Identity Access software program.

- Multi-Factor Authentication

  This Cloud Service provides multi-factor authentication for applications protected by IBM Verify Identity Access on prem, or via direct API invocation, and for other enforcement points including RADIUS clients, Unix/Linux PAM servers and Windows servers to verify identities when accessing a digital service. Second factors enabled by the Cloud Service include, but are not limited to, email, SMS and voice call, time based one-time passwords, and mobile biometrics powered by the IBM Verify Authenticator App for Mobile (iOS and Android). The SMS and voice call factors are not included as part of the Cloud Service and can be added by obtaining the IBM Verify SMS and Voice One-time Password optional add-on service. This Cloud Service integrates with the separately

licensed, on-premises IBM Verify Identity Access software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications.

- Adaptive Access

  This Cloud Service uses a combination of Threat Intelligence and Artificial Intelligence (AI) to help organizations accurately differentiate between malicious and true users, when user is trying to access an application protected by the service. The service consumes insights on users, their devices, and behavior patterns to determine in real-time a risk-mitigating action: allow access, enforce authentication, or block access. The service uses hundreds of data points and contextual information collected from the end-user's device to fingerprint the device and calculate a holistic risk level of the session. Risk-based access rules defined in the access policy uses the session risk level with additional parameters for determining the system's action. This service is tightly connected with the Verify administrator reports, access policy rules editor and the multi-factor authentication service.

- Lifecycle Management and Governance

  This Cloud Service tightly integrates with the separately licensed, on-premises IBM Verify Identity Governance Enterprise software program, to provide a solution for Clients to support their line-of-business demands for identity governance spanning both their on-premises and cloud applications. This Cloud Service provides organizations advanced identity lifecycle management capabilities within the cloud that includes account synchronization, application access request workflow, access certification, provisioning to cloud and on-premises applications.

1.1.2 IBM Verify Dedicated

IBM Verify Dedicated provides a highly available cloud instance for workforce, consumer, citizen, and classroom enterprises that provides single sign on, multi-factor authentication and lifecycle management with dedicated transaction rates that exceed the maximum aggregated transaction rate limit of 400 TPS for Production Instances, with the dedicated transaction rate to be specified in a transaction document.

1.1.3 IBM Verify Hybrid

This Cloud Service delivers flexibility through its entitlement to both on-premises and cloud solutions to let organizations approach hybrid deployments and cloud migration appropriately.

Verify Hybrid is a Dual Entitlement offering that provides simultaneous use of the Cloud Services and use of the identified Programs in a Client computing environment. The identified Programs are IBM Verify Identity Access Enterprise Edition, IBM Verify Identity Governance Enterprise Edition and IBM Directory Suite Enterprise Edition which may be used simultaneously with IBM Verify (SaaS) Single Sign-On, Multi-Factor Authentication and Lifecycle Management and Governance Cloud Services.

1.1.4 IBM Cloud Identity Connect

This Cloud Service delivers Single Sign-On (SSO) and Open ID Connect (OIDC), Authentication as a Service for cloud-based API authorization, an application launchpad, administrator reporting and an analytics dashboard. This Cloud Service connects users to applications using modern standards-based authentication and federation protocols, including hundreds of connectors to common applications. This Cloud Service tightly integrates with the on-premises IBM Verify Identity Access software program, which is included as enabling software, to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications.

1.1.5 IBM Cloud Identity Connect for ISAM

This Cloud Service tightly integrates with the on-premises IBM Verify Identity Access software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications. This Cloud Service requires the Client to have an active Software Subscription and Support (S&S) entitlement for the IBM Verify Identity Access program, and the S&S must remain active for the duration of Client's Cloud Service subscription. Client's entitlement to this Cloud Service must be equivalent to the Client's on-premises IBM Verify Identity Access license entitlement. Discontinuation of Client's S&S will also discontinue this Cloud Service. Access to the enabling software defined in Section 5.1 is not included with this Cloud Service.

1.1.6 IBM Cloud Identity Essentials

This Cloud Service provides Clients with Single Sign-On (SSO) and Multi-Factor Authentication (MFA) capabilities to the various IBM and public cloud applications they are using. This Cloud Service can be coupled with IBM MaaS360 to provide additional levels of security controls, such as conditional access.

1.1.7 IBM Cloud Identity Verify

This Cloud Service provides multi-factor authentication for applications protected by Cloud Identity Connect, or via direct API invocation, and for other enforcement points including RADIUS clients, Unix/Linux PAM servers and Windows servers in order to verify their identities when accessing a digital service. This includes mechanisms such as email, SMS and time based (software token) one-time passwords, and push based mobile biometrics authentication powered by IBM Verify. This Cloud Service integrates with the on-premises IBM Verify Identity Access software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications. It is available standalone, or to compliment Cloud Identity Connect, Cloud Identity Connect for IBM Verify Identity Access and Cloud Identity Essentials.

1.1.8 IBM Cloud Identity Govern

This Cloud Service tightly integrates with the separately licensed, on-premises IBM Verify Identity Governance Enterprise software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications. This Cloud Service provides organizations advanced identity lifecycle management capabilities within the cloud that includes application access request workflow.

1.1.9 IBM Cloud Identity Connect and Verify

This Cloud Service provides Client with the functionality of IBM Cloud Identity Connect and IBM Cloud Identity Verify as a single offering.

1.1.10 IBM Cloud Identity Adaptive Access

This Cloud Service uses Artificial Intelligence (AI)-powered contextual insights on users, their devices, and behavior patterns to help organizations enforce the correct authentication policies.

1.1.11 IBM Cloud Identity Connect Verify and Govern

This Cloud Service provides Client with the functionality of IBM Cloud Identity Connect, IBM Cloud Identity Verify, and IBM Cloud Identity Govern as a single offering.

1.2 Optional Services

1.2.1 IBM Verify Non-Production

IBM Verify Non-Production Environment on Cloud is a separate instance of the IBM Verify platform that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces. This Cloud Service has the option to include an availability service level agreement (SLA), subject to the terms in Section 3 Service Levels and Technical Support. This Cloud Service has a maximum aggregated transaction rate limit of 100 Transactions per second.

1.2.2 IBM Verify Vanity Domain

A vanity domain (one domain or sub-domain) allows for the Client to use a domain owned by, and more relevant to their organization, rather than using the default tenant domain that is provided by the platform out of the box. An SSL certificate will be maintained by IBM for the single domain and will be renewed on an annual basis.

1.2.3 IBM Verify Hosted Application Gateway

The application gateway provides an IBM managed and hosted light-weight appliance for Clients looking to support non-standard, or legacy, based single sign-on mechanisms. These mechanisms include LTPA and HTTP header-based authentication. Ongoing monitoring and maintenance are managed by IBM.

1.2.4 IBM Verify SMS and Voice One-time Password

This optional service provides voice call and SMS delivered one-time passwords, as a second factor authentication mechanism.

1.2.5 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud is a separate instance of the IBM Cloud Identity platform that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces. This Cloud Service has the option to include an availability service level agreement (SLA), subject to the terms in Section 3 Service Levels and Technical Support. This Cloud Service has a maximum aggregated transaction rate limit of 100 Transactions per second.

1.2.6 IBM Cloud Identity Vanity Domain

A vanity domain (one domain) allows for the Client to use a domain owned by, and more relevant to their organization, rather than using the default tenant domain that is provided by the platform out of the box. An SSL certificate will be maintained by IBM for this domain and will be renewed on an annual basis.

1.2.7 IBM Cloud Identity Application Gateway Hosted

The application gateway provides an IBM managed and hosted light-weight appliance for Clients looking to support non-standard, or legacy, based authentication mechanisms. These mechanisms include LTPA and HTTP header-based authentication. Ongoing monitoring and maintenance is managed by IBM.

1.3 Acceleration Services

Acceleration Services are expert services, as described in this SD, and are provided remotely to Client. For the purpose of this SD, if Client's base agreement references Cloud Services, then all such references apply to Acceleration Services, as applicable.

These remotely delivered services, for purposes of this Service Description, are referred to as the "Service". The Service provides Client access to subject matter expertise (SME) resources and supporting information for the IBM Verify product family.

Through coaching, mentoring and knowledge transfer, the Service is designed to aid Client in the construction and management of business solutions built using Verify Software products. Client must have an active entitlement to Verify virtual or physical appliance product. The Service is applicable to generally available Verify products, not "deprecated", "experimental" or "beta" products.

A list of supported product families can be viewed at the following webpage:
https://www.ibm.com/security/security-expert-labs

The Service is delivered in English language only, unless mutually agreed with Client.

The Service does not replace the role of the IBM Support organization which should continue to be the point of contact for technical problems.

1.3.1 IBM Expert Labs Assess Verify (10 hours)

This Service provides up to ten (10) hours in one or more of the following focus areas:

- A trusted advisor to help organizations achieve benefits and value from their Verify investment.
- Enhancements to the organization's capability to help develop a broad range of skills that span full process implementation of a Verify subscription.
- Regular check points during the implementation project to address challenges or architectural design decisions.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

IBM Security Verify:

www.ibm.com/terms/?id=735E5650E26711E69CCD7F0385C6524D

During service provisioning of IBM Verify, Client may select preferred region for Hosting Processing Activities from this list:

- Australia
- Canada

- Europe Region
- Japan
- United States

IBM Common Service Mesh (IBM Covered Model):

https://www.ibm.com/terms/?id=503882A8505045C1802C09E0B315F6CC

IBM Common Service Mesh is a common service that enables the generative AI functionality contained in the Cloud Service.

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month, and is specific to the region impacted and number of subscribed users in the region. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.99%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.1.1 Other Information about this SLA

During the first sixty (60) days of Client's term ("Burn-In Period"), Client shall not be entitled to any credit due to failure of the Cloud Service environment to achieve the minimum 99.99% Uptime Percentage under this Agreement. If prior-to or during the Burn-In Period IBM identifies existing Client configurations, policies, data, or code ("Pre-Existing Components") intended to be migrated to the Cloud Service that would prohibit the Cloud Service from successfully achieving the Uptime Percentage within this Agreement, IBM shall reserve the right to notify Client of such Pre-Existing Components and exempt them at IBM's sole discretion, from the provisions of the SLA. Should IBM notify Client of any exempted Pre-Existing Components, IBM shall be responsible for presenting to Client a remediation plan, to the extent possible, which enables such exempted components to meet the Uptime Percentage of this Agreement. Client shall be solely responsible for the cost of any such remediation unless otherwise agreed-upon by both parties.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at https://www.ibm.com/support/home/pages/support-guide/.

3.2.1 Optional Support Offerings

Additional support options are available for this Cloud Service. If Client selects to order an optional support offering, the terms defined in the Optional Support Offerings Service Description at https://www.ibm.com/terms/?id=i126-9789 will apply to the support offering specified in Client's TD.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Event is an occurrence of a specific event that is processed by or related to the use of the Cloud Services.

- For Verify SMS and Voice One-time Password, an Event is a voice call or SMS delivered one-time password. SMS sent for user management operations are not considered in this calculation.
- For IBM Verify (SaaS), IBM Verify Dedicated, IBM Verify Hybrid, and Cloud Identity Connect, an Event is an http request against the Cloud Service.
- For IBM Verify (SaaS), IBM Verify Dedicated, IBM Verify Hybrid, and Cloud Identity Verify, an Event is any multi-factor method being invoked via the Cloud Service.

- Authorized User is a unique user authorized to access to the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means.
- Employee is a unique person employed in or otherwise paid by or acting on behalf of Client's Enterprise, whether or not given access to the Cloud Services.
- Eligible Participant is an individual or entity eligible to participate in any service delivery program managed or tracked by the Cloud Services.
- Instance is each access to specific configuration of the Cloud Services.
- Resource Unit is an independent measure of a resource managed by, processed by, or related to the use of the Cloud Service.
  - Graduated Tiers is a cumulative pricing model, the Client is required to step through the tiers by purchasing the quantities in Tier 1, then Tier 2, etc.
  - Monthly Active User is a unique person who accesses the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means measured monthly.
  - Usage of each functional capability requires the specified number of Resource Unit entitlements to this Cloud Service subscription:

Maximum Monthly Active Users:

		Functional Capability in weighted Resource Units required per Active User		
Graduated Tier	**Maximum Monthly Active Users**	**Single Sign-On**	**Multi-factor Authentication**	**Adaptive Access**
1	500	0.1	0.1	0.1
2	5,000	0.08	0.08	0.08
3	10,000	0.06	0.06	0.06
4	100,000	0.008	0.008	0.008
5	500,000	0.0025	0.0025	0.0025
6	1,000,000	0.002	0.002	0.002
7	5,000,000	0.0015	0.0015	0.0015
8	10,000,000	0.0015	0.0015	0.0015
9	50,000,000	0.001	0.001	0.001
10	999,999,999	0.0005	0.0005	0.0005

Maximum Total Users:

		Functional Capability in weighted Resource Units required per Total User
Graduated Tier	**Maximum Total Users**	**Lifecycle Management and Governance**
1	500	0.29
2	5,000	0.075

		Functional Capability in weighted Resource Units required per Total User
Graduated Tier	Maximum Total Users	Lifecycle Management and Governance
3	10,000	0.05
4	100,000	0.005
5	500,000	0.002
6	1,000,000	0.001
7	5,000,000	0.0005
8	10,000,000	0.0002
9	50,000,000	0.0001
10	999,999,999	0.0001

Note: All calculations will be rounded up to a whole number.

4.2 Remote Services Charges

A remote service will expire 90 days from purchase regardless of whether the remote service has been used.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at https://www.ibm.com/acs apply.

5.1 Enabling Software

Enabling Software is provided to Client under the following terms:

Enabling Software	Applicable License Terms (if any)
IBM Verify Antenna	https://www.ibm.com/terms/?id=L-RVFP-9ZCQEW
IBM Verify Bridge	https://www.ibm.com/terms/?id=L-DDVG-SXWNMK
IBM Verify Authenticator App for Mobile	https://www.ibm.com/terms/?id=i125-5589
IBM Verify SDK (iOS)	
IBM Verify SDK (Android)	
IBM Verify SDK for JavaScript	
IBM Verify Bridge for Directory Sync	https://www.ibm.com/terms/?id=L-PLRN-678SAZ
IBM Application Gateway	https://www.ibm.com/terms/?id=L-SVRZ-CLFGHV
IBM Verify Gateway for Windows Login	https://www.ibm.com/terms/?id=L-ZALG-B7F9GL
IBM Verify Gateway for AIX PAM	https://www.ibm.com/terms/?id=L-LKMK-TRZC7Z
IBM Verify Gateway for Linux PAM	https://www.ibm.com/terms/?id=L-ELDJ-JK7M9F
IBM Verify Gateway for RADIUS	https://www.ibm.com/terms/?id=L-CNEM-X5UCHT
IBM Verify Identity Governance Infrastructure Adapters (Class A)	https://www.ibm.com/terms/?id=L-UDUG-X3CFM6
IBM Verify Identity Governance Application Adapters (Class B)	https://www.ibm.com/terms/?id=L-NHKM-NPLA8A
IBM Verify Directory Integrator	https://www.ibm.com/terms/?id=L-CNWH-KN4EVN

The following enabling software may only be used with the IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify, and IBM Cloud Identity Connect Verify and Govern Cloud Services:

Enabling Software	Applicable License Terms (if any)

IBM Verify Identity Access Virtual Enterprise Edition	**Container:** https://www.ibm.com/terms/?id=L-UGYM-JBJAL3 **Software:** https://www.ibm.com/terms/?id=L-MAZZ-49RVWE

5.2 Client Reference

Client agrees IBM may publicly refer to Client as a subscriber to the Cloud Services in a publicity or marketing communication.

5.3 Confidentiality

Testing Data, as well as any information or materials created, in any form or format, using the Testing Data, or any feedback about the Testing Data Client provides to IBM in any form or format, is considered to be IBM confidential information ("Information").

Client will use the Information only for the purpose set forth in this Service Description and for the benefit of IBM, and will use reasonable care to avoid disclosure of the Information other than to Client's:

a. employees and employees of any legal entity that it controls, controls it, or with which it is under common control, who have a need to know. Control means to own or control, directly or indirectly, over 50% of voting shares; or

b. subcontractors, financial and legal advisors, and then only to those who have a need to know.

Before disclosure to any party in (a) or (b), Client will have a written agreement with such party sufficient to require that party to treat Information substantially the same as described in this Agreement.

If required to disclose Information by law or court order, Client will endeavor to give IBM prompt notice to allow IBM a reasonable opportunity to obtain a protective order.

Client may disclose, disseminate, and use Information that is already in its possession without obligation of confidentiality, developed independently, obtained from a source other than IBM without obligation of confidentiality, publicly available when received or subsequently becomes publicly available through no fault of the Client, or disclosed by IBM to another without obligation of confidentiality. Client's obligations with respect to the Information will continue for a period of five years from its disclosure.

Notwithstanding the existence of any confidentiality or other agreement Client may have with IBM pertaining to confidential information, the preceding paragraphs govern with respect to the Testing Data.

5.4 Output IP Indemnity

IBM's obligation to protect Client against third party claims as set forth in the Cloud Services Agreement includes third party claims that the result generated by the Covered Model in response to a Client's prompt or other input (collectively, "Output") infringes that third party's patent or copyright provided that (in addition to the exclusions and Client obligations provided in the relevant base agreement):

a. Client has a paid subscription to the Cloud Service at the time Client generates the Output.

b. Client enables all available filters and logging features recommended by IBM in the product documentation or delivered with the Covered Model or in the Cloud Service, and Client supplies information collected by such filters and features as requested by IBM in connection with a third party claim;

c. the Output at issue was generated in connection with an Indemnified Use Case;

d. Client takes mitigating actions reasonably requested by IBM, which may include ceasing use of the allegedly infringing Output; and

e. Client had no reasonable basis to know that the Content or Output was infringing or likely to cause an infringement.

"**Covered Model**" means an IBM developed generative model provided with the Cloud Service ("IBM Covered Model").

"**Indemnified Use Cases**" means use within Client's enterprise (a) of an IBM Covered Model in a manner consistent with such model's intended use as described in its published Model Information or other Transaction Documents (such as license information or program specifications).

Except for IBM's obligation set out above relating to third party claims, Client is solely responsible for Output generated by the Cloud Service.

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content or that otherwise identify Client. IBM may however use Content and other information that result from Content as part of the Cloud Service for the purpose of managing and improving the Cloud Service. IBM may share threat identifiers and other security information embedded in Client personal data for threat detection and protection.