

# IBM Cloud Services Agreement

---

## IBM Cloud Service Description: IBM OpenPages GRC on Cloud

The following is the Service Description for your Order:

### 1. Cloud Service

The Cloud Service offering, is described below and is specified in an Order Document for the selected entitled offerings. The Order Document will consist of the Quotation that is provided and the Proof of Entitlement (PoE) you will receive confirming the start date and term of the Cloud Services and when invoicing will commence.

#### 1.1 IBM OpenPages GRC on Cloud

IBM OpenPages GRC on Cloud (a required component) offers a standard configuration for Operational Risk Management providing the ability to identify, manage, monitor, and report on risk and compliance initiatives enterprise wide. It can be used to combine all risk data, including risk and control self assessments (RCSA), loss events, scenario analysis, external losses, and key risk indicators (KRI) into a single integrated module.

The Operational Risk Management capabilities are:

- Key features:
  - (1) Enables identification, measurement, and mitigation of risks.
  - (2) Enables testing and documentation of internal controls.
- Loss events, which enables the following activities:
  - (1) Tracking, assessing, and managing both internal and external events that could result in operational loss.
  - (2) Managing multiple impact events and recoveries that are associated with operational losses.
- External loss events provide the ability to import loss data from IBM Algo FIRST, Operational Risk data eXchange Association (ORX), and Operational Risk Consortium (ORIC) loss databases (separate subscription required) into IBM OpenPages Operational Risk Management for scenario analysis, benchmarking, and reports generation. You can also export loss data to analytic tools or capital allocation applications.
- KRIs, which can be used to track performance metrics to potentially show the presence or state of a risk condition or trend.
- Scenario analysis, which is an assessment technique that can be used to identify and measure specific kinds of risks, in particular, low frequency, high-severity events.
- Reporting, monitoring, and analytics.
- IBM SoftLayer cloud implementation.

#### 1.2 IBM OpenPages GRC Non-Production Instance on Cloud

IBM OpenPages GRC Non-Production Instance on Cloud provides a Non-Production instance of the Cloud Service for internal development and testing activities.

#### 1.3 IBM OpenPages GRC Data Storage on Cloud

IBM OpenPages GRC Data Storage on Cloud (a required component) provides for the storage of GRC data for your instance of the Cloud Service. Storage will be sold in allotments of 150 Gigabytes.

#### 1.4 IBM OpenPages GRC Administrator User on Cloud

IBM OpenPages GRC Administrator User on Cloud (at least one is required) users are permitted to access all administrative functions as well as the Operational Risk Management capabilities of the Cloud Service.

#### 1.5 IBM OpenPages Operational Risk Management User on Cloud

IBM OpenPages Operational Risk Management User on Cloud users are permitted only to interact with the Operational Risk Management capabilities described above.

## **1.6 IBM OpenPages GRC Operational Risk Management Jump Start on Cloud**

IBM OpenPages GRC Operational Risk Management Jump Start on Cloud (a required component) provides services for the initial implementation of the Cloud Service and includes initial coaching and assistance for project planning, maintenance, administration and review of proven practices.

## **2. Security Description**

### **2.1 Security Policies**

IBM maintains privacy and security policies that are communicated to IBM employees. IBM requires privacy and security training to personnel who support IBM data centers. We have an information security team. IBM security policies and standards are reviewed and re-evaluated annually. IBM security incidents are handled in accordance with a comprehensive incident response procedure.

### **2.2 Access Control**

Access to client data, if required, is allowed only by authorized IBM support representatives according to principles of segregation of duties. IBM staff use two-factor authentication to an intermediate "gateway" management host. All connections are encrypted channels when accessing client data. All access to client data and transfer of data into or out of the hosting environment is logged. WIFI use is prohibited within the IBM data centers that support this Cloud Service.

### **2.3 Service Integrity and Availability**

Modifications to operating systems and application software are governed by IBM's change management process. Changes to firewall rules are also governed by the change management process and are reviewed by the IBM security staff before implementation. IBM monitors the data center 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators and third party vendors to help detect and resolve potential system security exposures. Malware detection (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) systems are used in all IBM data centers. IBM's data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

### **2.4 Activity Logging**

IBM maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time to central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to detect anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

### **2.5 Physical Security**

IBM maintains physical security standards designed to restrict unauthorized physical access to IBM data centers. Only limited access points exist into the data centers, which are controlled by two-factor authentication and monitored by surveillance cameras. Access is allowed only to authorized staff that have approved access. Operations staff verifies the approval and issues an access badge granting the necessary access. Employees issued such badges must surrender other access badges and can only possess the data center access badge for the duration of their activity. Usage of badges is logged. Non-IBM visitors are registered upon entering on premises and are escorted when they are on the premises. Delivery areas and loading docks and other points where unauthorized persons may enter the premises are controlled and isolated.

### **2.6 Compliance**

IBM performs industry standard SSAE 16 audits (or their equivalent) annually in production data centers. IBM reviews security and privacy-related activities for compliance with IBM's business requirements. Assessments and audits are conducted regularly by IBM to confirm compliance with its information security policies. IBM employees and vendor employees complete workforce security and awareness training annually. Personnel are reminded of their job objectives and their responsibility to meet ethical business conduct, confidentiality, and IBM's security obligations annually.

### 3. Service Level Commitment

IBM provides the following availability service level agreement (“SLA”) for the Cloud Service. You understand that the SLA does not constitute a warranty to you.

#### 3.1 Definitions

- a. "Availability Credit" means the remedy IBM will provide for a validated Claim. The Availability Credit will be applied in the form of a credit or discount against a future invoice of subscription charges for the Cloud Service.
- b. "Claim" means a claim you submit to IBM pursuant to the SLA that a Service Level has not been met during a Contracted Month.
- c. "Contracted Month" means each full month during the term measured from 12:00 a.m. Eastern US time on the first day of the month through 11:59 p.m. Eastern US time on the last day of the month.
- d. "Downtime" means a period of time during which production system processing for the Cloud Service has stopped and your users are unable to use all aspects of the Cloud Service for which they have permissions. Downtime does not include the period of time when the Cloud Service is not available because of:
  - (1) a scheduled or announced maintenance outage;
  - (2) Events or causes beyond IBM's control (e.g., natural disaster, internet outages, emergency maintenance, etc.);
  - (3) problems with your applications, equipment or data, or a third party's applications, equipment or data;
  - (4) your failure to adhere to required system configurations and supported platforms for accessing the Cloud Service; or
  - (5) IBM's compliance with any designs, specifications, or instructions that you provide to IBM or a third party provides to IBM on your behalf.
- e. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a Service Level.
- f. "Service Level" means the standard set forth below by which IBM measures the level of service it provides in this SLA.

#### 3.2 Availability Credits

- a. To submit a Claim, you must log a Severity 1 support ticket (as defined below in the Technical Support section) for each Event with the IBM technical support help desk, within twenty-four (24) hours of your first becoming aware that the Event has impacted your use of the Cloud Service. You must provide all necessary information about the Event and reasonably assist IBM with the diagnosis and resolution of the Event.
- b. You must submit your Claim for an Availability Credit no later than three (3) business days after the end of the Contracted Month in which the Claim arose.
- c. Availability Credits are based on the duration of the Downtime measured from the time you report that you were first impacted by the Downtime. For each valid Claim, IBM will apply the highest applicable Availability Credit based on the achieved Service Level during each Contracted Month, as shown in the table below. IBM will not be liable for multiple Availability Credits for the same Event in the same Contracted Month.
- d. The total Availability Credits awarded with respect to any Contracted Month shall not, under any circumstance, exceed 10 percent (10%) of one twelfth (1/12<sup>th</sup>) of the annual charge paid by you to IBM for the Cloud Service.

#### 3.3 Service Levels

Availability of the Cloud Service during a Contracted Month

Availability during a Contracted Month	Availability Credit (% of Monthly Subscription Fee for Contracted Month that is the subject of a Claim)
< 98%	2%

< 97%	5%
< 93%	10%

Availability, expressed as a percentage, is calculated as: (a) the total number of minutes in a Contracted Month minus (b) the total number of minutes of Downtime in a Contracted Month, divided by (c) the total number of minutes in a Contracted Month.

Example: 900 minutes total Downtime during Contracted Month

43,200 total minutes in a 30 day Contracted Month – 900 minutes Downtime = 42,300 minutes	
<hr/> 43,200 total minutes	= 2% Availability Credit for 97.9% Achieved Service Level

### 3.4 Other information about this SLA

This SLA is made available only to IBM's clients and does not apply to claims made by your users, guests, participants and permitted invitees of the Cloud Service or to any beta or trial services that IBM provides. The SLA only applies to the Cloud Services that are in production use. It does not apply to non-production environments, including but not limited to test, disaster recovery, quality assurance, or development.

## 4. Entitlement and Billing Information

### 4.1 Charge Metrics

The Cloud Services are made available under one of the following charge metrics as specified in the Order Document:

- a. Authorized User is a unit of measure by which the Cloud Service can be obtained. You must obtain separate, dedicated entitlements for each unique Authorized User given access to the Cloud Service in any manner directly or indirectly (for example: via a multiplexing program, device, or application server) through any means. Sufficient entitlements must be obtained to cover the number of Authorized Users given access to the Cloud Service during the measurement period specified in the Order Document.
- b. 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.
- c. Gigabyte is a unit of measure by which the Cloud Service can be obtained. A Gigabyte is defined as 2 to the 30<sup>th</sup> power bytes of data (1,073,741,824 bytes). Sufficient entitlements must be obtained to cover the total number of Gigabytes processed by the Cloud Service during the measurement period specified in the Order Document.
- d. 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 the Order Document.

### 4.2 Charges and Billing

The amount payable for the Cloud Service is specified in an Order Document.

### 4.3 Set-Up Charges

Standard set-up services and their applicable charges are provided through the IBM OpenPages Operational Risk Management Jump Start on Cloud offering.

If you require additional configuration or services, you must engage IBM's OpenPages GRC on Cloud services via a supplemental Statement of Work.

#### **4.4 Partial Month Charges**

The partial month charge is a pro-rated daily rate. The partial month charges are calculated based on the remaining days of the partial month starting on the date you are notified by IBM that your access to the Cloud Service offering is available.

#### **4.5 Overage Charges**

If your actual usage of the Cloud Service during the measurement period exceeds the entitlement stated on the PoE portion of the Order Document, then you will be invoiced for the overage, as set forth in the Order Document.

### **5. Term and Renewal Options**

#### **5.1 Term**

The term of the Cloud Service begins on the date that IBM notifies you that you have access to the Cloud Service, as described in the Order Document. The PoE portion of the Order Document will confirm the exact date of the start and end of the term. You are permitted to increase your level of use of the Cloud Service during the term by contacting IBM or your IBM Business Partner. We will confirm the increased level of usage in the Order Document.

#### **5.2 Cloud Services Term Renewal Options**

Your Order Document will set forth whether the Cloud Service will renew at the end of the term, by designating the term as one of the following:

##### **5.2.1 Automatic Renewal**

If your Order Document states that your renewal is automatic, you may terminate the expiring Cloud Service term by written request, at least ninety (90) days prior to the expiration date of the term that is set forth in the Order Document. If IBM or your IBM Business Partner does not receive such termination notice by the expiration date, the expiring term will be automatically renewed for either a one year term or the same duration as the original term as set forth in the PoE.

##### **5.2.2 Continuous Billing**

When the Order Document states that your billing is continuous, you will continue to have access to the Cloud Service following the end of your term and will be billed for the usage of the Cloud Service on a continuous basis. To discontinue use of the Cloud Service and stop the continuous billing process, you must provide IBM or your IBM Business Partner with ninety (90) days written notice requesting that your Cloud Service be cancelled. Upon cancellation of your access, you will be billed for any outstanding access charges through the month in which the cancellation took effect.

##### **5.2.3 Renewal Required**

When the Order Document states that your renewal type is "terminate", the Cloud Service will terminate at the end of the term and your access to the Cloud Service will be removed. To continue to use the Cloud Service beyond the end date, you must place an order with your IBM sales representative or IBM Business Partner to purchase a new subscription term.

### **6. Technical Support**

During the term of the Cloud Service, technical support is provided for the Cloud Service as set forth at [http://www-01.ibm.com/software/support/acceleratedvalue/SaaS\\_Handbook\\_V18.pdf](http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf) or a subsequent URL provided by IBM. Technical support is included with the Cloud Service and is not available as a separate offering.

### **7. Safe Harbor Compliance**

IBM has not determined compliance of this Cloud Service with the US-EU and US-Swiss Safe Harbor Frameworks.

### **8. Additional Information**

#### **8.1 Data Collection**

You are aware and agree that IBM may, as part of the normal operation and support of the Cloud Service, collect personal information from you (your 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 you. You confirm that you 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 your employees and contractors to access, update, correct or delete their collected personal information.

## **8.2 Derived Benefit Locations**

Where applicable, taxes are based upon the location(s) you identify as receiving benefit of the Cloud Services. IBM will apply taxes based upon the business address listed when ordering a Cloud Service as the primary benefit location unless you provide additional information to IBM. You are responsible for keeping such information current and providing any changes to IBM.

## **8.3 Non-Production Limitation**

If the Cloud Service is designated as "Non-Production", it can only be used 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. You are not authorized to use any part of the Cloud Service for any other purposes without acquiring the appropriate production entitlements.

## **8.4 No Guaranty of Compliance**

The Cloud Service can be used to help you 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 you are cautioned to obtain its own legal or other expert counsel. You are solely responsible for ensuring that you and your activities comply with all applicable laws, regulations, standards and practices. Use of the Cloud Service does not guarantee compliance with any law, regulation, standard or practice.

You further acknowledge that the Cloud Service is a tool for assisting you and not a substitute for the skill, judgment and experience of your management and employees in giving advice to third parties and in making investment and other business and risk management decisions. You are responsible for the results obtained from the use of the Cloud Service.

## **8.5 Links to Third Party Websites or Other Services.**

If you or Cloud Service User transmits Content to or from a third party website or other service that is linked to or made accessible by the Cloud Service, you and the Cloud Service User provide IBM with the consent to enable any such transmission of Content, but such interaction is solely between you and the third party website or service. IBM makes no warranties or representations about such third party sites, services or data, and shall have no liability for such third party sites, services or data quality.

## **8.6 Restrictions on Use for the Benefit of a Third Party**

You may not use the Cloud Service or any component thereof, including without limitation output data and reports produced by the Cloud Service to provide service bureau, hosting services, or any sort of commercial information technology services to third parties, unless otherwise agreed to in writing by IBM.

## **8.7 No Personal Health Information**

The Cloud Service is not designed to comply with HIPAA and may not be used for the transmission or storage of any Personal Health Information.