IBM Cognos Controller 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 provided Quotation and the Proof of Entitlement (PoE) which confirms the start date and term of the Cloud Services. Invoicing will commence following provisioning of the Cloud Service.

1.1 IBM Cognos Controller User on Cloud

IBM Cognos Controller is financial consolidation software that supports the close, consolidate and report process. The offering allows users to deliver financial results, create financial and management reports, and provides an enterprise view of key financial ratios and metrics.

IBM Cognos Controller User on Cloud can consolidate, report against, and administer the system

1.2 IBM Cognos Controller Jump Start on Cloud

IBM Cognos Controller Jump Start on Cloud remote service includes up to 80 hours of coaching and assistance including facilitated identification of an initial IBM Cognos Controller on Cloud (CCoC) use case, coaching on project planning and initiation of IBM CCoC implementation, coaching on proven practices for creating IBM CCoC reports, and coaching on maintenance and administration of IBM CCoC Service are purchased per Engagement and expire 90 days from purchase regardless of whether all hours have been used.

1.3 IBM Cognos Controller Additional Non-Production Instance

This offering adds additional Non-Production instances of IBM Cognos Controller. It can only be used as part of the Client's non-production activities, including but not limited to testing, performance tuning, fault diagnosis, benchmarking, staging, quality assurance activity and/or developing internally used additions or extensions to the offering using published application programming interfaces.

2. Security Description

2.1 Security Policies

IBM has an information security team and also maintains privacy and security policies that are communicated to IBM employees. IBM requires privacy and security training to personnel who support IBM data centers. 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 certifies its privacy practices annually as consistent with the U.S. Department of Commerce's Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement. 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. "Authorized Contact" means the individual(s) you have specified to IBM who is authorized to submit Claims under this SLA.

b. "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.

c. "Claim" means a claim you submit to IBM pursuant to the SLA that a Service Level has not been met during a Contracted Month.

d. "Client" means an entity subscribing for the Service directly from IBM which is not in default of any material obligations, including payment obligations, under its contract with IBM for the Service.

e. "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.

f. "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.

g. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a Service Level.

h. "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 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 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 ($1/12^{th}$) 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)**
99% - 99.75%	2%
95% - 98.99%	5%
Less than 95.0%	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: 476 minutes total Downtime during Contracted Month

43,200 total minutes in a 30 day Contracted Month -- 476 minutes Downtime = 42,724 minutes _____ 43,200 total minutes in a 30 day Contracted Month	= 5% Availability Credit for 98.9% Availability during the Contracted Month

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. 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.

b. Authorized User is a unit of measure by which the Cloud Service may be obtained. An Authorized User is a unique person who is given access to Cloud Service. You must obtain separate, dedicated entitlements for each Authorized User accessing the Cloud Service offering in any manner directly or indirectly (for example: via a multiplexing program, device, or application server) through any means during the measurement period specified in the Order Document. An entitlement for an Authorized User is unique to that Authorized User and may not be shared, nor may it be reassigned other than for the permanent transfer of the Authorized User entitlement to another person. For the purposes of the Cloud Service, you may provide access to users outside of its enterprise. Such users shall be deemed to be Authorized Users and be entitled appropriately.

c. 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 Charges and Billing

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

4.3 Set-Up Charges

Set-up charges will be specified in an Order Document.

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 On Demand Charges

On-Demand options included in the Order Document will not be invoiced until you request activation of the On-Demand part. When activated, you will be invoiced according to the rate 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 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 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

Technical support for the Cloud Service is available during the subscription period.

Regular Phone and Email Support Hours of Operation are as follows:

Support Ticket or E-Mail: Anytime, tickets processed according to assigned severity levels. Severity levels between 2 to 4 will be handled during business hours.
Phone: Monday-Friday, 9am – 5pm local hours (excluding IBM company observed holidays).

After Hours Support:

After Hours Support (outside of the regular operating hours stated above) is available only for Severity 1 issues on business days, weekends, and holidays.

Support Hotline: 1-877-465-5444.

Email: vsupport@ca.ibm.com
For logging a ticket via email, clients must use the interim Varicent/IBM address.

Support web portal: • http://support.varicent.com

Please see the attached link for the technical support guide:
http://www-1.ibm.com/software/analytics/varicent/customercenter/saas.html.

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 you are 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

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 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.

8.2 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.

8.3 Cookies

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.

8.4 Disaster Recovery and Content Backup

This Cloud Service also includes the following disaster recovery and content backup services:

In the event that a catastrophic condition arises, catastrophic being defined as "Force Majeure" meaning acts of God, terrorism, labor action, fire, flood, earthquake, riot, war, governmental acts, orders or restrictions, viruses, denial of service attacks and other malicious conduct, utility and network connectivity failures, or any other cause of Cloud Service unavailability that was outside IBM's reasonable control, IBM will work to restore your access to the Cloud Service as follows:

a) Standard Option - IBM shall provide the hardware, software and network infrastructure in IBM's data-center network that will enable Customer to resume access to the IBM SaaS within 14 days.

b) Premium Option - IBM shall provide the hardware, software and network infrastructure in IBM's data-center network that will enable Customer to resume access to the IBM SaaS within 5 days.

The environment will be restored using the most recent Content backup, as described below, with no more than 24 hours of Content loss of the restored Content data set.

Backups are taken daily and copied to an off-site location in the event of a Force Majeure event in the primary location. IBM retains backups on a rolling basis: Every 7 days, a full database backup is taken and each subsequent day within the week a comparative differential backup is taken. IBM will retain the last 7 days of daily differential backups and the previous 4 full backups (covering a span of 28 days of activity). As a new full backup is created, the oldest version is discarded. Backups are encrypted at rest on a disk-based backup system and during transmission to the offsite location.