

IBM Financial Crimes Insight

Nella presente Descrizione dei Servizi viene illustrato il Servizio Cloud. I documenti d'ordine applicabili riportano prezzi e dettagli aggiuntivi sull'ordine del Cliente.

1. Servizio in Cloud

1.1 Offerte

Il Cliente può selezionare le seguenti offerte disponibili:

1.1.1 IBM Financial Crimes Insight

Questo Servizio Cloud offre un'infrastruttura comune ed una serie di servizi comuni su cui sono costruite le offerte Financial Crimes Insights. IBM Financial Crimes Insight assicura l'integrazione necessaria tra componenti di contrasto ai crimini finanziari permettendo ai clienti di trarre vantaggio da tale integrazione.

IBM Financial Crimes Insight è un componente richiesto che fornisce l'Istanza del Servizio Cloud.

1.1.2 IBM Financial Crimes Insight Non-Production

Questo Servizio Cloud consente al Cliente di accedere alla funzionalità IBM Financial Crimes Insight Non-Production come offerta cloud.

1.1.3 IBM Financial Crimes Insight BYOL

Questo Servizio Cloud consente al Cliente di accedere alla funzionalità IBM Financial Crimes Insight come offerta cloud. Le offerte Bring your own licenses (BYOL) richiedono che il Cliente abbia precedentemente acquistato le titolarità di licenza appropriate per il Programma IBM associato. Il Programma IBM richiesto dall'offerta IBM Financial Crimes Insight BYOL è IBM Cloud Pak for Data Financial Crimes Insight.

1.1.4 IBM Financial Crimes Insight Non-Production BYOL

Questo Servizio Cloud consente al Cliente di accedere alla funzionalità IBM Financial Crimes Insight Non-Production come offerta cloud. Le offerte Bring your own licenses (BYOL) richiedono che il Cliente abbia precedentemente acquistato le titolarità di licenza appropriate per il Programma IBM associato. Il Programma IBM richiesto dall'offerta IBM Financial Crimes Insight Non-Production BYOL è IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment.

1.1.5 IBM Financial Crimes Insight for Entity Research Negative News API

Questo Servizio Cloud utilizza la tecnologia di cognitive computing e le analisi avanzate per cercare, analizzare ed assegnare una priorità alle notizie e ai media non strutturati allo scopo di scoprire il potenziale rischio legato ai crimini finanziari di un'entità, fornendo in output un elenco di articoli filtrati e ordinati per rilevanza. L'offerta viene fornita come API che può essere richiamata dalle organizzazioni o incorporata nei flussi di lavoro e nei processi.

1.1.6 IBM Financial Crimes Insight for Entity Research Enrichment API

Questo Servizio Cloud utilizza la tecnologia di cognitive computing per aggregare i dati provenienti da fonti strutturate che aiutano le organizzazioni a comprendere meglio un'entità, mantenendo aggiornati i registri dell'entità o dei clienti ed evidenziando la potenziale esposizione di un'entità al rischio di crimine finanziario. Le entità possono includere clienti, controparti o fornitori. L'offerta viene fornita come API che può essere richiamata dalle organizzazioni o incorporata nei flussi di lavoro e nei processi.

1.2 Servizi Opzionali

Oltre ad abbonarsi a IBM Financial Crimes Insight o IBM Financial Crimes Insight Non-Production, i Clienti dovranno anche abbonarsi ad uno dei seguenti Servizi Cloud:

1.2.1 IBM Financial Crimes Insight for Anti-Money Laundering

IBM Financial Crimes Insight for Anti-Money Laundering (FCI for AML) applica i propri livelli di analisi avanzata per monitorare l'attività finanziaria e aiutare il Cliente ad identificare la propensione delle entità a riciclare denaro. Attraverso l'utilizzo di dati demografici, comportamentali e di relazione, FCI for AML

assiste il cliente nel processo di revisione dei rischi noti, incrementando inoltre la copertura dei rischi tramite la fornitura di approfondimenti sui rischi nascosti.

1.2.2 IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring

Questo Servizio Cloud utilizza i dati di casi storici, l'aggregazione dei dati di evidenza contestuale e le funzionalità di machine learning con l'obiettivo di razionalizzare il processo di triage delle segnalazioni, riducendo i falsi positivi, accelerando la gestione della segnalazione e migliorando il processo decisionale grazie ad una migliore conoscenza dell'entità del rischio. Il servizio è un componente aggiuntivo che si inserisce tra il monitoraggio delle transazioni esistenti del Cliente e i sistemi di gestione dei casi.

1.2.3 IBM Financial Crimes Insight for Alert Triage – Transaction List Screening

Questo Servizio Cloud migliora i sistemi esistenti di screening delle sanzioni, analizzando le transazioni segnalate, utilizzando una pipeline configurabile, estendibile, basata su API. I dati della transazione vengono ripuliti, analizzati e messi in discussione, quindi elaborati attraverso tecniche di euristica e cognitive computing. I risultati vengono utilizzati per assegnare punteggi alle corrispondenze, identificare falsi positivi e restituire informazioni dettagliate e personalizzabili.

1.2.4 IBM Financial Crimes Insight for Entity Research

Questo Servizio Cloud utilizza la tecnologia di calcolo cognitiva per la visualizzazione, l'estrazione e il collegamento di contenuti rilevanti da fonti di dati strutturati e non strutturati con l'obiettivo di migliorare la conoscenza delle entità o dei rischi legati all'intraprendere rapporti commerciali con esse, e ridurre il tempo necessario per completare le attività Know Your Customer (KYC). La soluzione aiuta ad automatizzare e standardizzare la ricerca e l'analisi di informazioni relative al cliente tramite l'aggregazione di una varietà di sorgenti dati. L'obiettivo del servizio è il miglioramento della qualità dei record KYC in aggiunta ad una migliore 'esperienza cliente mediante la semplificazione e l'arricchimento del processo di ricerca e dell'attività di "due diligence".

Il Cliente può selezionare tra le seguenti opzioni di titolarità:

- IBM Financial Crimes Insight for Entity Research – Enterprise – ciascun Evento consente di indagare su più di 5 parti correlate.
- IBM Financial Crimes Insight for Entity Research – Advanced – ciascun Evento consente di indagare su un massimo di 5 parti correlate.
- IBM Financial Crimes Insight for Entity Research – Basic – ciascun Evento consente di indagare su un massimo di 2 parti correlate.

Una parte correlata è una qualsiasi entità (organizzazione o individuo) su cui indagare come parte di un'Indagine Principale come descritto nell'Articolo 4.1. In genere, questa può essere rappresentata da firmatari, funzionari, proprietari beneficiari definitivi, organizzazioni principali o sussidiarie autorizzate. A scanso di equivoci, se una parte correlata è un'entità che richiede un'indagine sui propri membri singoli o associati, anche questi verranno come parte correlata.

1.2.5 IBM Financial Crimes Insight for Entity Research with Material Change

Questo Servizio Cloud utilizza la tecnologia di calcolo cognitiva per la visualizzazione, l'estrazione e il collegamento di contenuti rilevanti da fonti di dati strutturati e non strutturati con l'obiettivo di migliorare la conoscenza delle entità o dei rischi legati all'intraprendere rapporti commerciali con esse, e ridurre il tempo necessario per completare le attività Know Your Customer (KYC). La soluzione aiuta ad automatizzare e standardizzare la ricerca e l'analisi di informazioni relative al cliente tramite l'aggregazione di una varietà di sorgenti dati. L'obiettivo del servizio è il miglioramento della qualità dei record KYC in aggiunta ad una migliore 'esperienza cliente mediante la semplificazione e l'arricchimento del processo di ricerca e dell'attività di "due diligence". Ciò include la funzionalità di Modifica Materiale, che consente di monitorare le entità in base ad una pianificazione per risalire ad eventuali differenze materiali da segnalare all'analista perché le controlli.

Il Cliente può selezionare tra le seguenti opzioni di titolarità:

- IBM Financial Crimes Insight for Entity Research – Enterprise – ciascun Evento consente di indagare su più di 5 parti correlate.
- IBM Financial Crimes Insight for Entity Research – Advanced – ciascun Evento consente di indagare su un massimo di 5 parti correlate.
- IBM Financial Crimes Insight for Entity Research – Basic – ciascun Evento consente di indagare su un massimo di 2 parti correlate.

Una parte correlata è una qualsiasi entità (organizzazione o individuo) su cui indagare come parte di un'indagine Principale come descritto nell'Articolo 4.1. In genere, questa può essere rappresentata da firmatari, funzionari, proprietari beneficiari definitivi, organizzazioni principali o sussidiarie autorizzate. A scanso di equivoci, se una parte correlata è un'entità che richiede un'indagine sui propri membri singoli o associati, anche questi varranno come parte correlata.

1.2.6 IBM Financial Crimes Insight for Claims Fraud – Property and Casualty

Questo Servizio Cloud aiuta le organizzazioni ad analizzare i dati per rilevare i rischi derivanti da reclami fraudolenti presentati dai propri clienti, da fornitori di servizi medici o altre entità e per gestire l'intero ciclo di vita dell'indagine e riferire sui risultati.

1.2.7 IBM Financial Crimes Insight for Claims Fraud – Investigation

Questo Servizio Cloud aiuta le organizzazioni a gestire l'intero ciclo di vita dell'indagine delle attività sospette e delle potenziali frodi.

1.2.8 IBM Electronic Communication Surveillance Analytics on Cloud

Questo Servizio Cloud è uno strumento che assiste gli organismi dei servizi finanziari nell'analisi e nel monitoraggio dei dati delle interazioni degli operatori commerciali su più canali al fine di rilevare diversi modelli di comunicazioni sospette. Lo strumento aiuta a rilevare diversi modelli di comportamenti illeciti riguardanti l'abuso e la manipolazione del mercato. Lo strumento utilizza la funzionalità di elaborazione del linguaggio naturale per comprendere le informazioni del testo e per distinguere i termini ambigui in base al contesto. Lo strumento utilizza inoltre le funzionalità di analisi dei sentimenti e delle emozioni che possono essere utilizzati per analizzare le comunicazioni. Queste funzionalità non sono state progettate per essere usate a, né tanto meno dedurre tratti della personalità delle persone. L'analisi alimenta il motore di ragionamento complessivo consentendo di collegare vari approfondimenti e fornire la stima dei rischi ai responsabili della conformità.

1.2.9 IBM Voice Surveillance Analytics on Cloud

Questo Servizio Cloud è uno strumento che aiuta gli istituti di servizi finanziari ad analizzare e monitorare le comunicazioni vocali dei dipendenti su più canali per rilevare attività sospette. Lo strumento utilizza la tecnologia di riconoscimento vocale per convertire la voce umana in parola scritta utilizzando l'apprendimento macchina per rilevare la grammatica e la struttura del linguaggio. Collega l'output del riconoscimento vocale (speech-to-text) con i metadati di tipo 'rich' generati dal sistema di telefonia e applica al testo la funzionalità 'speaker diarisation', al fine di consentire una ricerca rapida e semplice e la riproduzione di conversazioni vocali di interesse. L'output del riconoscimento vocale insieme ai metadati vengono messi a disposizione del Cliente in un formato ben definito. Come opzioni aggiuntive, lo strumento può utilizzare l'elaborazione del linguaggio naturale per estrarre i metadati semantici dall'analisi linguistica e del contenuto per rilevare gli argomenti, i toni, i sentimenti e le emozioni. Queste funzionalità non sono state progettate per essere usate a, né tanto meno dedurre tratti della personalità delle persone. Tutta la conversione del riconoscimento vocale viene eseguita "in memoria" per ridurre lo storage di file duplicati e delle trascrizioni e, dopo l'elaborazione, i dati vocali non vengono memorizzati nel Cloud.

1.2.10 IBM Complaints Analytics on Cloud

Questo Servizio Cloud consente alle organizzazioni di identificare, aggregare e classificare i reclami, le segnalazioni e altre attività. Fornisce approfondimenti su questioni emergenti per indirizzare le crescenti aspettative normative. Lo strumento utilizza l'analitica avanzata per identificare e analizzare reclami che altrimenti verrebbero ignorati dai sistemi tradizionali. Può importare dati strutturati e non strutturati come, ad esempio, i dati del Cliente, le email, le note di servizio, i reclami sui social media e le registrazioni vocali. Successivamente utilizza le capacità cognitive per aggregare e arricchire i dati dei reclami per identificare i rischi sistemici. Applica, inoltre, la segmentazione dinamica e la profilatura delle serie temporali per monitorare e anticipare i cambiamenti e le tendenze.

Al fine di utilizzare IBM Complaints Analytics on Cloud, il Cliente deve sottoscrivere l'abbonamento a IBM Electronic Communication Surveillance Analytics on Cloud oppure a IBM Voice Surveillance Analytics on Cloud.

1.2.11 IBM Electronic Communication Surveillance Analytics on Cloud BYOL

Questo Servizio Cloud consente al Cliente di accedere alla funzionalità IBM Electronic Communication Surveillance Analytics on Cloud come offerta cloud. Le offerte Bring your own licenses (BYOL) richiedono

che il Cliente abbia precedentemente acquistato le titolarità di licenza appropriate per il Programma IBM associato. Il Programma IBM richiesto da questa offerta IBM Electronic Communication Surveillance Analytics on Cloud BYOL è IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication.

1.2.12 IBM Voice Surveillance Analytics on Cloud BYOL

Questo Servizio Cloud consente al Cliente di accedere alla funzionalità IBM Voice Surveillance Analytics on Cloud come offerta cloud. Le offerte Bring your own licenses (BYOL) richiedono che il Cliente abbia precedentemente acquistato le titolarità di licenza appropriate per il Programma IBM associato. Il Programma IBM richiesto da questa offerta IBM Voice Surveillance Analytics on Cloud BYOL è IBM Financial Crimes Insight for Conduct Surveillance Software – Voice.

1.2.13 IBM Complaints Analytics on Cloud BYOL

Questo Servizio Cloud consente al Cliente di accedere alla funzionalità IBM Complaints Analytics come offerta cloud. Le offerte Bring your own licenses (BYOL) richiedono che il Cliente abbia precedentemente acquistato le titolarità di licenza appropriate per il Programma IBM associato. Il Programma IBM richiesto dall'offerta IBM Complaints Analytics on Cloud BYOL è IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics.

1.3 Servizi di accelerazione

1.3.1 IBM Financial Crimes Insight Set-up

I seguenti servizi di set-up sono richiesti affinché vengano forniti al Cliente per l'utilizzo del Servizio Cloud corrispondente:

- IBM Financial Crimes Insight for Anti-Money Laundering Set-up
- IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring Set-up
- IBM Financial Crimes Insight for Alert Triage – Transaction List Screening Set-up
- IBM Financial Crimes Insight for Entity Research – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research – Basic Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Basic Set-up
- IBM Financial Crimes Insight for Entity Research Negative News API Set-up
- IBM Financial Crimes Insight for Entity Research Enrichment API Set-up
- IBM Financial Crimes Insight for Claims Fraud – Property and Casualty Set-up
- IBM Financial Crimes Insight for Claims Fraud – Investigation Set-up
- IBM Surveillance Insight for Financial Services on Cloud Set-up

2. Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)

Il Supplemento al Trattamento dei Dati Personali (DPA o Data Processing Addendum) di IBM, disponibile alla pagina web <http://ibm.com/dpa> e le Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Sheet o Appendice DPA) nei seguenti link forniscono ulteriori informazioni sulla protezione dei dati per i Servizi Cloud e per le opzioni relative ai tipi di Contenuto che potrebbe essere trattato, per le attività di trattamento interessate, le funzionalità per la protezione dei dati e le specifiche sulla conservazione e restituzione del Contenuto. Il DPA si applica ai dati personali presenti nel Contenuto, nella misura in cui si applichino i) il Regolamento Europeo in materia di Protezione dei Dati Personali (European General Data Protection Regulation, EU/2016/679, GDPR); o ii) altre leggi sulla protezione dei dati riportate alla pagina <http://www.ibm.com/dpa/dpl>.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=14BD7780D65B11E99EAF519926DF897>

3. Livelli di Servizio e Supporto Tecnico

3.1 Service Level Agreement ("SLA")

IBM fornisce al Cliente il seguente Service Level Agreement ("SLA"). IBM applicherà il Rimborso più elevato applicabile sulla base della disponibilità cumulativa del Servizio Cloud raggiunta, come mostrato nella tabella seguente. La percentuale di disponibilità viene calcolata nel seguente modo: il numero totale di minuti nel mese contrattuale, meno il numero totale di minuti di Inattività del Servizio nel mese contrattuale, diviso per il numero totale di minuti nel mese contrattuale. La definizione di Inattività del Servizio, il processo di reclamo e le modalità per contattare IBM in relazione ai problemi di disponibilità del servizio sono riportati nel manuale di supporto al Servizio Cloud di IBM all'indirizzo https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilità	Credito (% della quota di abbonamento mensile*)
Inferiore al 99,9%	2%
Inferiore al 99,0%	5%
Inferiore al 95,0%	10%

* La quota di abbonamento rappresenta il prezzo contrattuale per il mese soggetto al reclamo.

3.2 Supporto tecnico

Il supporto tecnico per il Servizio Cloud, inclusi i dettagli di contatto di assistenza, i livelli di gravità, le ore di disponibilità del supporto, i tempi di risposta e altre informazioni e processi relativi al supporto, possono essere consultati selezionando il Servizio Cloud nella guida di supporto IBM disponibile alla pagina <https://www.ibm.com/support/home/pages/support-guide/>.

4. Corrispettivi

4.1 Calcolo dei Corrispettivi

Le metriche dei corrispettivi per il Servizio Cloud sono specificate nel Documento d'Ordine.

Al presente Servizio Cloud si applica il seguente calcolo dei corrispettivi:

- Per Impegno si intende un servizio professionale o di formazione correlato ai Servizi Cloud.
- Per Istanza si intende ogni accesso ad una configurazione specifica dei Servizi Cloud.
- Un Evento rappresenta il verificarsi di un evento specifico che viene elaborato o relativo all'utilizzo dei Servizi Cloud.
 - Per IBM Financial Crimes Insight for Anti-Money Laundering, un Evento è rappresentato da 10 milioni di transazioni finanziarie in un mese di calendario.
 - Per IBM Financial Crimes Insight for Claims Fraud – Property and Casualty e IBM Financial Crimes Insight for Claims – Investigation, un Evento rappresenta un ricorrenza di un Reclamo. Un Reclamo è un insieme di istruzioni relative ad una richiesta formale fatta ad un'organizzazione per la copertura o il risarcimento per una perdita o un evento coperti.
 - Per IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring, un Evento è rappresentato da un singolo avviso/evento inserito nel Servizio Cloud dal sistema originario in un mese di calendario. Solitamente il sistema di origine è un sistema di monitoraggio della transazione o un sistema di Case Management.
 - Per IBM Financial Crimes Insight for Alert Triage – Transaction List Screening, un Evento è rappresentato da un massimo di 1.000 eventi singoli inseriti nel Servizio Cloud dal sistema originario, in un mese di calendario. Solitamente il sistema di origine è un sistema di monitoraggio della transazione o un sistema di Case Management.
 - Per IBM Financial Crimes Insight for Entity Research e IBM Financial Crimes Insight for Entity Research with Material Change, un Evento è rappresentato da qualsiasi indagine principale gestita dal Servizio Cloud, incluse le ricerche identiche ripetute, in un mese solare. Un'indagine principale è qualsiasi record non collegato come child ad un altro controllo. Un child è una parte correlata (come descritto nell'Articolo 1.2.5) che non sarebbe altrimenti soggetta a un'indagine principale.

- Si definisce Partecipante Eleggibile, qualsiasi persona fisica o giuridica idonea a partecipare a qualsiasi programma di erogazione del servizio, gestito o tracciato mediante i Servizi Cloud.
- Un Elemento è la ricorrenza di un elemento specifico che viene elaborato, gestito o che è relativo all'uso del Servizio Cloud.
 - Per IBM Voice Surveillance Analytics on Cloud, un Elemento è un'ora di un Flusso Vocale (Voice Stream) elaborato dal Servizio Cloud durante un giorno solare. Un Flusso Vocale è la cattura di una comunicazione audio sia in tempo reale che in formato registrato.
- Una chiamata API è rappresentata da una richiesta ai Servizi Cloud attraverso un'interfaccia programmabile.
- "Entity ID" è un identificativo univoco riferito a qualsiasi entità rappresentata all'interno dei Servizi Cloud.

5. Ulteriori condizioni

Agli Accordi per i Servizi Cloud (o agli accordi equivalenti per il cloud di base), stipulati prima del 1 gennaio 2019, si applicano le condizioni riportate alla pagina web <https://www.ibm.com/acs>.

5.1 Programmi di Supporto

IBM Financial Crimes Insight e IBM Financial Crimes Insight Non-Production includono l'accesso a determinati programmi ("Programmi di Supporto") distribuiti nell'ambiente Cloud. Il Cliente può utilizzare questi Programmi di Supporto esclusivamente allo scopo di contrastare o eventualmente intraprendere azioni intese a identificare e/o inibire frodi, reati finanziari e pagamenti impropri.

5.1.1 Limitazioni d'uso – Specifiche per determinati Programmi di Supporto

I seguenti programmi di supporto sono disponibili con le seguenti limitazioni:

- IBM Watson Studio – Entitlement: 5 Concurrent Users
- IBM Watson Machine Learning – Entitlement: 50 Models
- IBM Openscale – Entitlement: 50 Models
- IBM SPSS Modeler Premium – Entitlement: 4 Authorized Users
- IBM SPSS Statistics Standard – Entitlement: 4 Authorized Users
- Watson Explorer Advanced Edition – Entitlement: per X Gigabytes secondo quanto di seguito definito.

Il Cliente è autorizzato ad analizzare:

- tutto il contenuto archiviato nel repository del Servizio Cloud da utilizzare con Raccolte Non Analitiche;
- fino a 10 Gigabyte di Contenuti non archiviati nel repository del Servizio Cloud da utilizzare con Raccolte Non Analitiche.
- 100 Gigabyte di Contenuti archiviati nel repository del Servizio Cloud da utilizzare con Raccolte Analitiche.

Le Raccolte Analitiche si riferiscono alle raccolte create nella console di amministrazione delle annotazioni di Watson Explorer o create nella console di amministrazione di Watson Explorer Content Analytics o tramite l'API come tipo "Analisi dei contenuti" o "Analisi".

Le Raccolte Non Analitiche includono tutti gli altri contenuti analizzati dal Servizio Cloud del programma.

- IBM InfoSphere DataStage – IBM InfoSphere DataStage and QualityStage Designer Entitlement: 2 Authorized Users
- IBM Operational Decision Manager – Entitlement: 1 million Monthly Rules Decisions and 1 thousand Monthly Managed Decision Artifacts

Definizione della titolarità

- a. "Utente Concurrent" è una persona che accede al Programma di Supporto in un qualsiasi momento. Indipendentemente dal fatto che la persona acceda simultaneamente al Programma di Supporto più volte, tale persona viene considerata come un unico Utente "Concurrent".

- b. Il Modello è rappresentato da un modello matematico o un algoritmo relativo ai dati sottostanti o al processo di generazione dei dati utilizzato per simulare, spiegare e fare previsioni nel Programma di Supporto.
- c. Un Utente Autorizzato è una persona specifica cui è stato fornito l'accesso al Programma di Supporto in qualsiasi modo, direttamente o indirettamente (ad esempio, tramite un programma multiplexing, dispositivo o server applicativo) con qualsiasi mezzo.
- d. Un Gigabyte (GB) è uguale a 2 byte elevati alla ventesima potenza di dati elaborati, analizzati, utilizzati, archiviati o configurati nel Programma di Supporto.
- e. Una Decisione su Regole Mensile è il risultato della chiamata di un insieme di regole da un server di esecuzione delle regole in esecuzione nel Programma di Supporto o da questi gestito, in un qualsiasi mese di calendario.
- f. Le Risorse Decisionali Gestite mensili sono un oggetto gestito dal Programma di Supporto in un qualsiasi mese di calendario.

5.2 Condizioni applicabili a IBM Financial Crimes Insight BYOL

Le offerte Bring your own licenses (BYOL) richiedono che il Cliente abbia precedentemente acquistato le titolarità di licenza appropriate per il Programma IBM associato specificato nella seguente Tabella. Le titolarità del Cliente per le offerte BYOL SaaS non possono superare le titolarità del Cliente per il programma IBM associato, secondo i rapporti specificati di seguito.

L'offerta BYOL non comprende il servizio Subscription and Support (S&S) per il Programma IBM associato. Il Cliente dichiara di aver acquistato (1) le titolarità di licenza e (2) il servizio S&S applicabili per il Programma IBM associato. Durante il periodo di abbonamento all'offerta BYOL, il Cliente deve tenere aggiornato il servizio S&S per le titolarità del Programma IBM utilizzate insieme alle titolarità dell'offerta BYOL. Qualora la licenza del Cliente per l'utilizzo del Programma IBM associato o il servizio S&S del Cliente per il programma IBM associato vengano sospesi, cesserà anche il diritto del Cliente all'utilizzo dell'offerta BYOL.

Il Cliente può continuare a utilizzare le titolarità associate al programma IBM che sono applicate all'utilizzo dell'offerta BYOL per distribuire il programma IBM associato in concomitanza con l'utilizzo da parte del Cliente dell'offerta BYOL per il seguente periodo (il "periodo di Utilizzo simultaneo"): per i Clienti con una durata di abbonamento inferiore a 3 (tre), non più di novanta (90) giorni dopo l'inizio dell'abbonamento iniziale del Cliente dell'offerta BYOL; per i Clienti con una durata di abbonamento superiore a 3 (tre) anni, non più di un (1) anno dall'inizio dell'abbonamento iniziale del Cliente all'offerta BYOL. Al termine del periodo di Utilizzo Simultaneo e per la durata dell'uso dell'offerta BYOL da parte del Cliente, le titolarità del Cliente per il programma IBM associato, applicate all'utilizzo dell'offerta BYOL, vengono sospese e il Cliente non potrà più utilizzare tali titolarità per implementare il programma IBM associato (soggetto ad eventuali eccezioni dichiarate).

La seguente tabella specifica il rapporto delle titolarità con il Programma IBM associato, richiesto per l'utilizzo dell'offerta BYOL in base alla titolarità corrispondente dichiarata. Una volta che il Cliente ha ottenuto l'offerta BYOL e per la durata dell'uso dell'offerta BYOL da parte del Cliente, le titolarità del Cliente per il Programma IBM associato, applicate all'utilizzo dell'offerta BYOL, vengono sospese e il Cliente non potrà più utilizzare tali titolarità per implementare il Programma IBM associato (soggetto ad eventuali eccezioni dichiarate).

Programma IBM Associato	Offerta BYOL	Rapporto n/m*
IBM Cloud Pak for Data Financial Crimes Insight	IBM Financial Crimes Insight BYOL	Rapporto: 1 Installazione / 1 Istanza
IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment	IBM Financial Crimes Insight Non-Production BYOL	Rapporto: 1 Installazione / 1 Istanza

Programma IBM Associato	Offerta BYOL	Rapporto n/m*
IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication	IBM Electronic Communication Surveillance Analytics on Cloud BYOL	Rapporti complessivi: Livello 1 (1-100 RVU): ● 1 RVU / 1 Partecipante eleggibile Livello 2 (101-235 RVU): ● 0,9 RVU / 1 Partecipante eleggibile Tier 3 (236-435 RVUs): ● 0,8 RVU / 1 Partecipante eleggibile Livello 4 (436-585 RVU): ● 0,6 RVU / 1 Partecipante eleggibile Livello 5 (586-835 RVU): ● 0,5 RVU / 1 Partecipante eleggibile Livello 6 (836-1.135 RVU): ● 0,4 RVU / 1 Partecipante eleggibile Livello 7 (1.136+ RVU): ● 0,3 RVU / 1 Partecipante eleggibile
IBM Financial Crimes Insight for Conduct Surveillance Software – Voice	IBM Voice Surveillance Analytics on Cloud BYOL	Rapporti complessivi: Livello 1 (1-100 RVU): ● 1 RVU / 1 Elemento Livello 2 (101-235 RVU): ● 0,9 RVU / 1 Elemento Tier 3 (236-435 RVUs): ● 0,8 RVU / 1 Elemento Livello 4 (436-585 RVU): ● 0,6 RVU / 1 Elemento Livello 5 (586-835 RVU): ● 0,5 RVU / 1 Elemento Livello 6 (836-1.135 RVU): ● 0,4 RVU / 1 Elemento Livello 7 (1.136+ RVU): ● 0,3 RVU / 1 Elemento
IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics	IBM Complaints Analytics on Cloud BYOL	Rapporti complessivi: Livello 1 (1-100 RVU): ● 5 RVU / 1 ID Entità Livello 2 (101-235 RVU): ● 4,5 RVU / 1 ID Entità Tier 3 (236-435 RVUs): ● 4 RVU / 1 ID Entità Livello 4 (436-585 RVU): ● 3 RVU / 1 ID Entità Livello 5 (586-835 RVU): ● 2,5 RVU / 1 ID Entità Livello 6 (836-1.135 RVU): ● 2 RVU / 1 ID Entità Livello 7 (1.136+ RVU): ● 1,5 RVU / 1 ID Entità

* "Rapporto n/m" indica che per ogni ('n') titolarità della metrica indicata per il programma IBM associato, il Cliente può applicare tali titolarità al numero specificato ('m') di titolarità della metrica indicata per l'offerta BYOL. Se la conversione da un Programma IBM Associato ad un'Offerta BYOL risulta in un numero non intero, arrotondare al numero intero più vicino.

Esempio 1:

710 RVU in Partecipanti Eleggibili (EPS)

(Applicabile a IBM Trade Surveillance Analytics e IBM Electronic Communication Surveillance Analytics)

Livello 1: se $710 > 100$, quindi $100/1 = 100$ EPS

Livello 2: se $710 > 235$, quindi $(235-100)/0,9 = +150$ EPS

Livello 3: se $710 > 435$, quindi $(435-235)/0,8 = +250$ EPS

Livello 4: se $710 > 585$, quindi $(585-435)/0,6 = +250$ EPS

Livello 5: se $710 > 835 \rightarrow$ no, quindi $(710-585)/0,5 = +250$ EPS

EPS totali: $100 + 150 + 250 + 250 + 250 = 1000$ EPS

Esempio 2:

250 RVU (pacchetto da 100.000) in ID Entità (pacchetto da 500.000)

(Applicabile a IBM Complaints Analytics)

Livello 1: se $250 > 100$, quindi $100/5 = 20$ ID Entità

Livello 2: se $250 > 235$, quindi $(235-100)/4,5 = +30$ ID Entità

Livello 3: se $250 > 435 \rightarrow$ no, quindi $(250-235)/4 = +3,75$ ID Entità

EPS Totali: $20 + 30 + 3,75 = 53,75$ ID Entità, arrotondati a 54 ID Entità

Verifica: $250 \text{ RVU} = 269 \text{ Risorse} * 100.000 \text{ Dimensione Pacchetto Prem} / 500.000 \text{ Dimensione pacchetto SaaS} = 53,75$, arrotondati a 54 ID Entità

5.3 Contenuto di Terze Parti

Il Cliente prende atto che i risultati della ricerca ottenuti e citati nei report generati come parte dei Servizi Cloud qui descritti ("Risultati della ricerca") possono includere dati o Contenuti di proprietà di terzi e che IBM non vende o per i quali non fornisce alcuna licenza o altri diritti. Il Cliente accetta di essere l'unico responsabile per l'ottenimento, prima dell'utilizzo di uno qualsiasi dei Servizi Cloud descritti nel presente documento, di tutte le licenze, i diritti e le autorizzazioni, necessari per utilizzare, conservare, elaborare o riprodurre o adattare i Risultati della ricerca, da parte dei terzi applicabili, in base a quanto richiesto al Cliente, o a IBM per conto del Cliente, dalle leggi applicabili a tali Risultati della ricerca. Il Cliente autorizza IBM e le sue affiliate e i suoi appaltatori ad accedere, riprodurre, adattare o altrimenti elaborare, per conto del Cliente, le origini dati di terze parti (inclusi dati o Contenuti presenti o ottenuti dai Risultati della ricerca) in connessione con i Servizi Cloud nel presente documento. Ai fini del presente Articolo 5.3, i Contenuti sono costituiti da opere, dati, immagini, software o informazioni protetti da copyright, che il Cliente o i relativi utenti autorizzati forniscono, autorizzano l'accesso o che inseriscono nel Servizio Cloud.

5.4 Scadenza del Servizio Cloud

Prima della scadenza o termine del Servizio Cloud, il Cliente può utilizzare una delle funzionalità di reportistica o esportazione del Servizio Cloud fornite per estrarre i dati. I servizi di estrazione dei dati personalizzati sono disponibili in base ad un accordo separato.

Dopo aver ricevuto una richiesta da parte del Cliente entro 30 giorni dalla data di scadenza o recesso dal Servizio Cloud, IBM restituirà al Cliente una copia elettronica del contenuto del Cliente nel formato nativo dell'applicazione.

Accettato da:

Firma e timbro del Cliente

Data:

Ai sensi e per gli effetti degli articoli 1341 e 1342 del Codice Civile Italiano, il Cliente approva specificamente i seguenti articoli del presente documento: "Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)", "Service Level Agreement ("SLA")", "Condizioni applicabili a IBM Financial Crimes Insight BYOL", "Contenuto di Terze Parti", "Scadenza del Servizio Cloud".

Firma e timbro del Cliente

Data: