IBM Financial Crimes Insight

Ce Descriptif de Services détaille le Service Cloud. Les bons de commande applicables contiennent les prix et des détails supplémentaires concernant la commande du Client.

1. Service Cloud

1.1 Offres

Le Client peut faire son choix parmi les offres disponibles ci-dessous.

1.1.1 IBM Financial Crimes Insight Basic

Ce Service Cloud fournit une infrastructure et un ensemble communs de services sur lesquels s'appuient les offres Financial Crimes Insights. IBM Financial Crimes Insight fournit l'intégration requise entre les offres permettant aux Clients de bénéficier d'un ensemble d'offres Financial Crimes intégré.

1.1.2 IBM Financial Crimes Insight Advanced

Ce Service Cloud fournit le même ensemble de fonctionnalités qu'IBM Financial Crimes Insight Basic et inclut également les fonctionnalités identifiées dans IBM Financial Crimes Insight – Data Science.

IBM Financial Crimes Insight Basic ou IBM Financial Crimes Insight Advanced est un composant obligatoire qui fournit l'Instance du Service Cloud.

1.1.3 IBM Financial Crimes Insight Basic Non-Production

Ce Service Cloud permet au Client d'accéder à la fonctionnalité IBM Financial Crimes Insight Basic Non-Production en tant qu'offre Cloud.

1.1.4 IBM Financial Crimes Insight Advanced Non-Production

Ce Service Cloud permet au Client d'accéder à la fonctionnalité IBM Financial Crimes Insight Advanced Non-Production en tant qu'offre Cloud.

1.1.5 IBM Financial Crimes Insight Advanced BYOL

Ce Service Cloud permet au Client d'accéder à la fonctionnalité IBM Financial Crimes Insight Advanced en tant qu'offre Cloud. Pour les offres BYOL (Bring Your Own Licenses), le Client doit avoir précédemment acquis les droits de licence appropriés pour le logiciel IBM associé identifié dans le logiciel IBM ci-dessous. Le Logiciel IBM requis par l'offre IBM Financial Crimes Insight Advanced BYOL est IBM Cloud Pak for Data Financial Crimes Insights.

1.1.6 IBM Financial Crimes Insight Advanced Non-Production BYOL

Ce Service Cloud permet au Client d'accéder à la fonctionnalité IBM Financial Crimes Insight Advanced Non-Production en tant qu'offre Cloud. Pour les offres BYOL (Bring Your Own Licenses), le Client doit avoir précédemment acquis les droits de licence appropriés pour le logiciel IBM associé identifié dans le logiciel IBM ci-dessous. Le Logiciel IBM requis par l'offre IBM Financial Crimes Insight Advanced Non-Production BYOL est IBM Cloud Pak for Data Financial Crimes Insights for Non-Production Environment.

1.1.7 IBM Financial Crimes Insight for Entity Research Negative News API

Ce Service Cloud utilise la technologie informatique cognitive et l'analytique évoluée pour rechercher, analyser et classer par ordre de priorité des nouvelles et médias non structurés afin de découvrir le risque potentiel lié aux délits financiers correspondant à une entité par l'élaboration d'une liste d'articles filtrés et classés. Cette offre est livrée sous la forme d'une API que les organisations peuvent appeler ou intégrer à leurs flux de travail ou leurs processus.

1.1.8 IBM Financial Crimes Insight for Entity Research Enrichment API

Ce Service Cloud utilise la technologie informatique cognitive pour regrouper des données de sources structurées afin d'aider les organisations à mieux comprendre une entité, à maintenir les enregistrements de l'entité ou du client à jour et d'exposer un éventuel risque lié aux délits financiers correspondant à une entité. Les entités peuvent comprendre des clients, des contreparties ou des fournisseurs. Cette offre est livrée sous la forme d'une API que les organisations peuvent appeler ou intégrer à leurs flux de travail ou leurs processus.

1.2 Services Optionnels

Outre l'abonnement à IBM Financial Crimes Insight ou IBM Financial Crimes Insight Non-Production, le Client doit également souscrire à l'un des Services Cloud suivants :

1.2.1 IBM Financial Crimes Insight Data Science

Ce Service Cloud fournit les fonctionnalités de préparation de données et de gestion, formation et gouvernance de modèles, ainsi qu'un catalogue de données permettant de gérer les données d'entreprise et la gouvernance, la qualité et la collaboration de modèles d'IA.

1.2.2 IBM Financial Crimes Insight for Anti-Money Laundering

IBM Financial Crimes Insight for Anti-Money Laundering (FCI for AML) applique ses couches d'analytique évoluée au suivi des activités financières afin d'aider le Client à identifier la propension des entités à se livrer au blanchiment d'argent. A l'aide de données démographiques et relatives aux comportements et aux relations, FCI for AML contribue au processus de révision par le Client de risques connus et peut éventuellement accroître le taux de couverture du risque en fournissant des analyses démontrables relatives aux risques masqués.

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

Ce Service Cloud utilise les données issues des cas historiques, l'agrégation des données probantes contextuelles et les fonctionnalités d'apprentissage automatique dans le but de simplifier le processus de triage d'alerte, de réduire les faux positifs, d'accélérer l'élimination de l'alerte et d'améliorer la prise de décision grâce à une meilleure compréhension du risque des entités. Le service est un composant additionnel qui se situe entre les systèmes de surveillance de transaction et de gestion de cas existants de l'établissement du Client.

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

Ce Service Cloud renforce le balayage des systèmes de sanctions existants en analysant les transactions ayant fait l'objet d'une alerte à l'aide d'un pipeline alimenté par une API configurable et extensible. Les données de transactions sont épurées, analysées et soumises à un processus de wrangling, puis traitées via différentes techniques informatiques heuristiques et cognitives. Les résultats obtenus permettent d'indexer les accès, d'identifier les faux positifs et de renvoyer des analyses informatives et personnalisables.

1.2.5 IBM Financial Crimes Insight for Entity Research

Ce Service Cloud utilise la technologie informatique cognitive pour filtrer, extraire et lier le contenu pertinent issu de sources de données structurées et non structurées dans le but d'améliorer la compréhension des entités et/ou du risque associé de travailler avec elles et de réduire le temps nécessaire pour réaliser les activités de connaissance de la clientèle. La solution aide à automatiser et normaliser la recherche et l'analyse des informations client par le biais de l'agrégation de diverses sources de données. L'objectif du service consiste à améliorer la qualité des dossiers de connaissance de la clientèle en plus d'améliorer l'expérience client grâce à la simplification de la recherche et des activités de diligence raisonnable.

Le Client peut faire son choix parmi les options d'autorisation d'utilisation ci-dessous :

- IBM Financial Crimes Insight for Entity Research – Enterprise : chaque Evénement permet de rechercher plus de 5 parties connexes.
- IBM Financial Crimes Insight for Entity Research – Advanced : chaque Evénement permet de rechercher jusqu'à 5 parties connexes.
- IBM Financial Crimes Insight for Entity Research – Basic : chaque Evénement permet de rechercher jusqu'à 2 parties connexes.

Le terme partie connexe désigne toute entité (organisation ou individu) devant faire l'objet d'une recherche dans le cadre de l'examen d'une Investigation Parent telle que définie à la Section 4.1. Il s'agit généralement de signataires autorisés, d'agents, de propriétaires effectifs en dernière analyse, d'organisations mères ou de filiales en fonction d'un organigramme. Dans le but de dissiper toute incertitude, lorsqu'une partie connexe est une entité dont tous les membres individuels ou associés doivent faire l'objet d'une recherche, chacun de ses membres individuels ou associés constitue une partie connexe à part entière.

1.2.6 IBM Financial Crimes Insight for Entity Research with Material Change

Ce Service Cloud utilise la technologie informatique cognitive pour filtrer, extraire et lier le contenu pertinent issu de sources de données structurées et non structurées dans le but d'améliorer la compréhension des entités et/ou du risque associé de travailler avec elles et de réduire le temps nécessaire pour réaliser les activités de connaissance de la clientèle. La solution aide à automatiser et normaliser la recherche et l'analyse des informations client par le biais de l'agrégation de diverses sources de données. L'objectif du service consiste à améliorer la qualité des dossiers de connaissance de la clientèle en plus d'améliorer l'expérience client grâce à la simplification de la recherche et des activités de diligence raisonnable. Cela comprend la fonctionnalité Changement Important, qui permet la surveillance des entités en fonction d'un planning et qui, lorsque des différences importantes sont détectées, envoie une alerte à l'analyste qui effectuera un examen plus approfondi.

Le Client peut faire son choix parmi les options d'autorisation d'utilisation ci-dessous :

- IBM Financial Crimes Insight for Entity Research – Enterprise : chaque Evénement permet de rechercher plus de 5 parties connexes.
- IBM Financial Crimes Insight for Entity Research – Advanced : chaque Evénement permet de rechercher jusqu'à 5 parties connexes.
- IBM Financial Crimes Insight for Entity Research – Basic : chaque Evénement permet de rechercher jusqu'à 2 parties connexes.

Le terme partie connexe désigne toute entité (organisation ou individu) devant faire l'objet d'une recherche dans le cadre de l'examen d'une Investigation Parent telle que définie à la Section 4.1. Il s'agit généralement de signataires autorisés, d'agents, de propriétaires effectifs en dernière analyse, d'organisations mères ou de filiales en fonction d'un organigramme. Dans le but de dissiper toute incertitude, lorsqu'une partie connexe est une entité dont tous les membres individuels ou associés doivent faire l'objet d'une recherche, chacun de ses membres individuels ou associés constitue une partie connexe à part entière.

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

Ce Service Cloud aide les organisations à analyser des données pour détecter le risque résultant de sinistres frauduleux soumis par leurs Clients, par les prestataires de soins médicaux ou autres entités, à gérer le cycle de vie complet d'une enquête et à communiquer les résultats.

1.2.8 IBM Financial Crimes Insight for Claims Fraud – Investigation

Ce Service Cloud aide les entreprises à gérer le cycle de vie complet des enquêtes sur les activités suspectes et les fraudes potentielles.

1.2.9 IBM Electronic Communication Surveillance Analytics on Cloud

Ce Service Cloud est un outil qui aide les établissements financiers à analyser et surveiller efficacement les données d'interaction des employés sur plusieurs canaux afin de détecter les différentes formes de communications suspectes. Cet outil aide à détecter les différents types de comportements agressifs liés aux abus et manipulations de marché. Il tire parti de la fonction de traitement automatique du langage naturel pour comprendre les informations textuelles et distinguer les termes ambigus en fonction du contexte. L'outil utilise également des fonctionnalités d'analyse des sentiments et des émotions pouvant être utilisées pour analyser les communications. Ces fonctionnalités ne sont pas destinées à et ne sont pas utilisées pour déduire les traits de personnalité des individus. Les résultats de cette analyse alimentent le moteur de raisonnement global qui contribue à l'établissement de liens entre diverses observations et à fournir une estimation des risques aux responsables de la vérification de la conformité.

1.2.10 IBM Voice Surveillance Analytics on Cloud

Ce Service Cloud est un outil conçu pour aider les organismes de services financiers à analyser et surveiller les communications vocales des employés sur plusieurs canaux afin de détecter les activités suspectes. L'outil utilise la technologie parole-texte pour convertir la voix humaine en texte écrit en tirant parti de l'apprentissage automatisé pour détecter la structure grammaticale et linguistique. Il lie la sortie parole-texte aux métadonnées enrichies générées par le système de téléphonie et applique la journalisation du conférencier au texte pour permettre une recherche rapide et simple, ainsi qu'une répétition des conversations vocales intéressantes. La sortie parole-texte, ainsi que les métadonnées, sont mises à la disposition du Client dans un format bien défini. L'outil utilise également le traitement du langage naturel pour extraire des métadonnées sémantiques du contenu et l'analyse linguistique pour

déterminer le sujet, le ton, les sentiments et les émotions. Ces fonctionnalités ne sont pas destinées à et ne sont pas utilisées pour déduire les traits de personnalité des individus. Toute conversion parole-texte est effectuée « en mémoire » pour réduire le stockage des fichiers et transcriptions en double, et aucune donnée vocale n'est stockée sur le Cloud après le traitement.

1.2.11 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics

Ce Service Cloud permet aux organisations d'identifier, de regrouper et de catégoriser les plaintes, allégations et autres activités. Il donne des informations sur les problèmes émergents afin de répondre aux attentes réglementaires toujours plus strictes. Cet outil exploite les analyses avancées pour identifier et analyser les plaintes que les systèmes traditionnels ignoreraient. Il peut traiter des données structurées et non structurées, telles que des données Client, des courriers électroniques, des notes de service, des plaintes sur les réseaux sociaux et des enregistrements vocaux. Il utilise ensuite des capacités cognitives pour regrouper et enrichir les données des plaintes afin d'identifier les risques systémiques. Il applique également une segmentation dynamique et un profilage des séries temporelles pour suivre et anticiper les changements et les tendances.

Afin de pouvoir utiliser IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics, le Client doit également s'abonner soit à IBM Electronic Communication Surveillance Analytics on Cloud, soit à IBM Voice Surveillance Analytics on Cloud.

1.2.12 IBM Electronic Communication Surveillance Analytics on Cloud BYOL

Ce Service Cloud permet au client d'accéder à la fonctionnalité IBM Electronic Communication Surveillance Analytics on Cloud en tant qu'offre Cloud. Pour les offres BYOL (Bring Your Own Licenses), le Client doit avoir précédemment acquis les droits de licence appropriés pour le logiciel IBM associé identifié dans le logiciel IBM ci-dessous. Le Logiciel IBM requis par l'offre IBM Electronic Communication Surveillance Analytics on Cloud BYOL est IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication.

1.2.13 IBM Voice Surveillance Analytics on Cloud BYOL

Ce Service Cloud permet au client d'accéder à la fonctionnalité IBM Voice Surveillance Analytics on Cloud en tant qu'offre Cloud. Pour les offres BYOL (Bring Your Own Licenses), le Client doit avoir précédemment acquis les droits de licence appropriés pour le logiciel IBM associé identifié dans le logiciel IBM ci-dessous. Le Logiciel IBM requis par l'offre IBM Voice Surveillance Analytics on Cloud BYOL est IBM Financial Crimes Insight for Conduct Surveillance Software – Voice.

1.2.14 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL

Ce Service Cloud permet au Client d'accéder à la fonctionnalité IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics en tant qu'offre Cloud. Pour les offres BYOL (Bring Your Own Licenses), le Client doit avoir précédemment acquis les droits de licence appropriés pour le logiciel IBM associé identifié dans le logiciel IBM ci-dessous. Le Logiciel IBM requis par l'offre IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL est IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics.

1.3 Services d'Accélération

1.3.1 IBM Financial Crimes Insight Set-up

Les services de configuration suivants sont requis en vue de la préparation du Client à l'utilisation du Service Cloud correspondant :

- 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. Fiches Techniques sur le Traitement et la Protection des Données

L'Addendum d'IBM relatif au Traitement de Données à caractère personnel, disponible sur http://ibm.com/dpa (DPA) et la ou les Fiches Techniques (désignées par fiche(s) technique(s) ou Annexe(s) DPA) dans les liens ci-dessous contiennent des informations additionnelles sur la protection des données pour les Services Cloud et leurs options concernant les types de Contenus pouvant être traités, les activités de traitement impliquées, les dispositifs de protection des données et les détails de conservation et de retour de Contenu. Le DPA s'applique aux Données à caractère personnel du Contenu dans la mesure où i) Le Règlement Général sur la Protection des Données (UE/2016/679) (RGPD) ; ou ii) d'autres lois relatives à la protection des données identifiées sur http://www.ibm.com/dpa/dpl s'appliquent.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=14BD7780D65B11E99EAFC519926DF897

3. Niveaux de Service et Support Technique

3.1 Accord Relatif aux Niveaux de Service

IBM fournit au Client l'Accord relatif aux Niveaux de Service (« SLA ») de disponibilité ci-dessous. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud, comme indiqué dans le tableau ci-dessous. Le pourcentage de disponibilité est calculé comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes d'indisponibilité du Service au cours du mois contractuel, divisé par le nombre total de minutes du mois contractuel. La définition de l'indisponibilité du Service, la procédure de réclamation et les moyens de contacter IBM concernant les problèmes de disponibilité de service figurent dans le guide de support de Services Cloud d'IBM à l'adresse https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilité	Avoir (% de redevance d'abonnement mensuelle*)
Inférieure à 99,9 %	2 %
Inférieure à 99,0 %	5 %
Inférieure à 95,0 %	10 %

* La redevance d'abonnement est le prix contractuel pour le mois objet de la réclamation.

3.2 Support Technique

Le support technique destiné au Service Cloud, y compris les coordonnées des personnes à contacter, les niveaux de gravité, les heures de disponibilité, les temps de réponse ainsi que d'autres informations et processus relatifs au support technique sont disponibles en sélectionnant le Service Cloud dans le guide de support IBM disponible à l'adresse https://www.ibm.com/support/home/pages/support-guide/.

4. Montant des Redevances

4.1 Unités de mesure des redevances

Les unités de mesure des redevances du Service Cloud sont indiquées dans le Document de Transaction.

Les unités de redevances suivantes s'appliquent à ce Service Cloud :

- Un Engagement est un service professionnel ou de formation relatif aux Services Cloud.
- Une Instance représente chaque accès à une configuration spécifique des Services Cloud.

- Un Evénement est une occurrence d'un événement caractéristique, qui est traitée par ou relative à l'utilisation des Services Cloud.
    - Pour IBM Financial Crimes Insight for Anti-Money Laundering, un Evénement est composé de 10 millions de transactions financières en un mois calendaire.
    - Pour IBM Financial Crimes Insight for Claims Fraud – Property and Casualty et IBM Financial Crimes Insight for Claims – Investigation, un Evénement est composé d'un Sinistre. Un Sinistre est un ensemble d'instructions relatives à une demande formelle adressée à une organisation pour la couverture ou l'indemnisation d'un préjudice ou événement couvert.
    - Pour IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring, un Evénement est une alerte individuelle/un événement versé dans le Service Cloud à partir du système d'origine en un mois calendaire. Généralement, un système source d'origine est un système de suivi des transactions ou un système de gestion des cas.
    - Pour IBM Financial Crimes Insight for Alert Triage – Transaction List Screening, un Evénement est composé de jusqu'à 1 000 alertes individuelles versées dans le Service Cloud à partir du système d'origine en un mois calendaire. Généralement, un système source d'origine est un système de suivi des transactions ou un système de gestion des cas.
    - Pour IBM Financial Crimes Insight for Entity Research and IBM Financial Crimes Insight for Entity Research with Material Change, un Evénement est composé de toute recherche parent traitée par le Service Cloud, y compris les recherches répétées identiques, pendant un mois calendaire. Une recherche parent correspond à un enregistrement n'étant lié à aucun dossier enfant lors de la recherche. Un dossier enfant est une partie connexe (telle que décrite à la Section 1.2.5) qui ne fait pas l'objet d'une recherche parent.
- Un Participant Admissible est un individu ou une entité habilitée à prendre part à un programme de prestation de service géré ou suivi par les Services Cloud.
- Un Elément est une occurrence d'un élément caractéristique, qui est gérée par, traitée par ou relative à l'utilisation du Service Cloud.
    - Pour IBM Voice Surveillance Analytics on Cloud, un Elément correspond à une heure de flux vocal traité par le Service Cloud pendant un jour calendaire. Un flux vocal désigne la capture d'une communication audio en temps réel ou par enregistrement.
- Un Appel d'API désigne l'invocation des Services Cloud par le biais d'une interface programmable.
- Un Identifiant Entité est un identificateur unique pour toute entité identifiée dans les Services Cloud.
- Un Message Numérique est une communication électronique gérée ou traitée par les Services Cloud.

5. Dispositions Additionnelles

Pour les Contrats de Services Cloud (ou des contrats Cloud de base équivalents) signés avant le 1er janvier 2019, les dispositions énoncées à l'adresse https://www.ibm.com/acs s'appliquent.

5.1 Logiciels de Support

IBM Financial Crimes Insight and IBM Financial Crimes Insight Non-Production comprend l'accès à certains logiciels (« Logiciels de Support ») qui sont déployés dans l'environnement Cloud. Le Client peut utiliser ces Logiciels de Support uniquement afin de faire opposition ou d'entreprendre une action visant à identifier et/ou neutraliser des activités frauduleuses, un délit financier ou des paiement irréguliers.

5.1.1 Limitations d'utilisation / S'appliquant spécifiquement à certains Logiciels de Support

Les Logiciels de Support ci-après sont disponibles sous réserve des limitations suivantes :

- IBM Watson Studio – Autorisation : 5 Utilisateurs simultanés
- IBM Watson Machine Learning – Autorisation : 50 Modèles
- IBM Openscale – Autorisation : 50 Modèles
- IBM SPSS Modeler Premium – Autorisation : 4 Utilisateurs Autorisés
- IBM SPSS Statistics Standard – Autorisation : 4 Utilisateurs Autorisés
- Watson Explorer Advanced Edition – Autorisation : par X Gigaoctets tel que défini ci-dessous.

Le Client est autorisé à analyser :

- tous les contenus stockés dans le référentiel du Service Cloud à utiliser dans le cadre de Collections Non-Analytiques ;
- jusqu'à 10 Gigaoctets de Contenu non stocké dans le référentiel du Service Cloud à utiliser dans le cadre de Collections Non-Analytiques ; et
- 100 Gigaoctets de Contenu stocké dans le référentiel du Service Cloud à utiliser dans le cadre de Collections Non-Analytiques.

  Les Collections Analytiques sont des collections créées dans la Console d'administration Watson Explorer annotation, créées dans la Console d'administration Watson Explorer Content Analytics ou via l'API en tant qu'« Analytique de Contenu » ou « Analytique ».

  Les Collections Non-Analytiques comprennent tout autre contenu analysé par le Service Cloud du Logiciel.

- IBM InfoSphere DataStage – Autorisation IBM InfoSphere DataStage and QualityStage Designer : 2 Utilisateurs Autorisés
- IBM Operational Decision Manager – Autorisation : 1 million de Décisions sur les Règles par Mois et 1 000 Artefacts de Règle Gérés par Mois

Définitions des Autorisations

a. Un Utilisateur Simultané est une personne accédant au Logiciel de Support à tout moment donné. Que la personne accède ou non simultanément au Logiciel de Support à plusieurs reprises, cette personne n'est considérée que comme un Utilisateur Simultané unique.

b. Un Modèle est un modèle mathématique ou un algorithme qui concerne les données sous-jacentes ou le processus de génération de données utilisé pour la simulation, l'explication et la formulation de prévisions dans le cadre du Logiciel de Support.

c. Un Utilisateur Autorisé est un utilisateur unique autorisé à accéder au Logiciel de Support de quelque manière que ce soit, directement ou indirectement (par exemple par le biais d'un logiciel, appareil ou serveur d'application multiplexe).

d. Un Gigaoctet (Go) représente 2 puissance 30 d'octets de données traités par, analysés, utilisés, stockés ou configurés dans le Logiciel de Support.

e. Une Décision sur les Règles est le résultat de l'appel d'un ensemble de règles à partir d'un serveur d'exécution de règle exécuté ou traité par le Logiciel de Support en un mois calendaire donné.

f. Un Artefact de Règle Géré par Mois est un objet géré par le Logiciel de Support en un mois calendaire donné.

5.2 Conditions applicables à IBM Financial Crimes Insight BYOL

Pour les offres BYOL (Bring Your Own Licenses), le Client doit avoir précédemment acquis les droits de licence appropriés pour le logiciel IBM associé identifié dans le tableau ci-dessous. Les droits d'accès du Client à l'offre BYOL SaaS ne peuvent pas dépasser les droits d'accès du Client au logiciel IBM associé, dans la limite des ratios indiqués ci-dessous.

L'offre BYOL n'inclut pas l'Abonnement et le Support (AS) pour le logiciel IBM associé. Le Client déclare qu'il a acquis (1) les autorisations de licence applicables et (2) l'AS du logiciel IBM associé. Pendant la période de souscription de l'offre BYOL, le Client doit maintenir l'AS actuel pour les droits du logiciel IBM utilisés conjointement avec les droits de l'offre BYOL. En cas de résiliation de la licence du Client pour l'utilisation du logiciel IBM associé ou l'AS du Client pour le logiciel IBM associé, le droit du Client d'utiliser l'offre BYOL sera résilié.

Le Client peut continuer d'utiliser les droits d'accès au logiciel IBM associé appliqués à l'utilisation de l'offre BYOL pour déployer le logiciel IBM associé en même temps que l'utilisation de l'offre BYOL par le Client pendant la période suivante (ci-après la « période d'Utilisation Simultanée ») : pour les Clients dont la durée de l'abonnement est inférieure à (3) ans, au maximum quatre-vingt-dix (90) jours suivant le début de l'abonnement initial du Client à l'offre BYOL ; pour les Clients dont la durée de l'abonnement est supérieure ou égale à trois (3) ans, au maximum un (1) an suivant le début de l'abonnement initial du Client à l'offre BYOL. A l'issue de la période d'Utilisation Simultanée, pendant la durée de l'utilisation de l'offre BYOL par le Client, les droits d'accès du Client au logiciel IBM associé appliqués à l'utilisation de l'offre BYOL sont suspendus et le Client ne pourra plus utiliser ces droits pour déployer le logiciel IBM associé (sous réserve des exceptions énoncées).

Le tableau ci-dessous présente le ratio des droits d'accès au logiciel IBM associé requis pour l'utilisation de l'offre BYOL dans le cadre du droit correspondant indiqué. Une fois que le Client aura obtenu l'offre BYOL et pendant la durée de l'utilisation de l'offre BYOL par le Client, les droits d'accès du Client au logiciel IBM associé appliqués à l'utilisation de l'offre BYOL sont suspendus et le Client ne pourra plus utiliser ces droits pour déployer le logiciel IBM associé (sous réserve des exceptions énoncées).

Logiciel IBM Associé	Offre BYOL	Ratio n/m*
IBM Cloud Pak for Data Financial Crimes Insight	IBM Financial Crimes Insight BYOL	Ratio : 1 Installation / 1 Instance
IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment	IBM Financial Crimes Insight Non-Production BYOL	Ratio : 1 Installation / 1 Instance
IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication	IBM Electronic Communication Surveillance Analytics on Cloud BYOL	Ratios cumulatifs : Niveau 1 (1 à 100 RVU) : ● 1 RVU / 1 Participant Admissible Niveau 2 (101 à 235 RVU) : ● 0,9 RVU / 1 Participant Admissible Niveau 3 (236 à 435 RVU) : ● 0,8 RVU / 1 Participant Admissible Niveau 4 (436 à 585 RVU) : ● 0,6 RVU / 1 Participant Admissible Niveau 5 (586 à 835 RVU) : ● 0,5 RVU / 1 Participant Admissible Niveau 6 (836 à 1135 RVU) : ● 0,4 RVU / 1 Participant Admissible Niveau 7 (1136 RVU et plus) : ● 0,3 RVU / 1 Participant Admissible
IBM Financial Crimes Insight for Conduct Surveillance Software – Voice	IBM Voice Surveillance Analytics on Cloud BYOL	Ratios cumulatifs : Niveau 1 (1 à 100 RVU) : ● 1 RVU / 1 Elément Niveau 2 (101 à 235 RVU) : ● 0,9 RVU / 1 Elément Niveau 3 (236 à 435 RVU) : ● 0,8 RVU / 1 Elément Niveau 4 (436 à 585 RVU) : ● 0,6 RVU / 1 Elément Niveau 5 (586 à 835 RVU) : ● 0,5 RVU / 1 Elément Niveau 6 (836 à 1135 RVU) : ● 0,4 RVU / 1 Elément Niveau 7 (1136 RVU et plus) : ● 0,3 RVU / 1 Elément
IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics	IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL	Ratios cumulatifs : Niveau 1 (1 à 100 RVU) : ● 5 000 RVU / 1 Message Numérique Niveau 2 (101 à 235 RVU) : ● 4 500 RVU / 1 Message Numérique Niveau 3 (236 à 435 RVU) : ● 4 000 RVU / 1 Message Numérique Niveau 4 (436 à 585 RVU) : ● 3 000 RVU / 1 Message Numérique Niveau 5 (586 à 835 RVU) : ● 2 500 RVU / 1 Message Numérique Niveau 6 (836 à 1135 RVU) : ● 2 000 RVU / 1 Message Numérique Niveau 7 (1136 RVU et plus) : ● 1 500 RVU / 1 Message Numérique

* « Ratio n/m » signifie que, pour tous les ('n') droits de l'unité de mesure indiquée pour le logiciel IBM associé, le Client peut appliquer ces droits au nombre indiqué de ('m') droits de l'unité de mesure indiquée pour l'offre BYOL. Si la conversion d'un Logiciel IBM associé en offre BYOL donne lieu à un nombre non entier, le résultat doit être arrondi au nombre entier le plus proche.

Exemple 1 :

710 RVU en Participant Admissible (EPS)

(Applicable à IBM Trade Surveillance Analytics et IBM Electronic Communication Surveillance Analytics)

Niveau 1 : si 710>100, alors 100/1 = 100 EPS

Niveau 2 : si 710>235, alors (235-100)/0,9 = +150 EPS

Niveau 3 : si 710>435, alors (435-235)/0,8 = +250 EPS

Niveau 4 : si 710>585, alors (585-435)/0,6 = +250 EPS

Niveau 5 : si 710>835, alors (710-585)/0,5 = +250 EPS

Total EPS : 100 + 150 + 250 + 250 + 250 = 1000 EPS

Exemple 2 :

500 000 RVU en Messages Numériques (lot de 5 000)

(Applicable à IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics)

Niveau 1 : si 500 000>100, alors 100/5 000 = 0,02 Message Numérique

Niveau 2 : si 500 000>235, alors (235-100)/4 500 = + 0,03 Message Numérique

Niveau 3 : si 500 000>435 →, alors (435-235)/4 000 = + 0,05 Message Numérique

Niveau 4 : si 500 000>585 →, alors (585-435)/3 000 = + 0,05 Message Numérique

Niveau 5 : si 500 000>835 →, alors (835-585)/2 500 = + 0,1 Message Numérique

Niveau 6 : si 500 000>1 135 →, alors (1 135-835)/2 000 = + 0,15 Message Numérique

Niveau 7 : si 500 000>1 135 →, alors (500 000-1135)/1 500 = + 99,6 Message Numérique

Nombre total de Messages Numériques : 0,02 + 0,03 + 0,05 + 0,1 + 0,15 + 99,6 = 100 Messages Numériques

5.3 Résultats de la Recherche

Le Client reconnaît que les résultats de la recherche obtenus et mentionnés dans les rapports générés dans le cadre du Service Cloud décrits dans le présent document (« Résultats de la Recherche ») sont susceptibles de contenir des données ou du Contenu dont un tiers est propriétaire et qui ne sont pas vendus par IBM ou pour lesquels IBM ne fournit pas de licence ou de droits applicables auxdits Résultats de la Recherche ou Contenu. Les Résultats de la Recherche sont considérés comme étant du Contenu pour ces Services Cloud.

5.4 Expiration du Service Cloud

Avant l'expiration ou la résiliation du Service Cloud, le Client peut utiliser l'une quelconque des fonctions de génération de rapports ou d'exportation fournies du Service Cloud pour extraire des données. Des services d'extraction de données personnalisées sont disponibles dans le cadre d'un contrat distinct.

A réception d'une demande d'assistance du Client dans les 30 jours suivant la date d'expiration ou de résiliation du Service Cloud, IBM retournera au Client une copie électronique du contenu du Client au format d'application natif.