The Financial and
Risk business of
Thomson Reuters
is now Refinitiv.

REFINITIV™

KYC as a Service (KYCaaS)

Service Description

Version 1.6

Document Version 1.6
Date of issue: November 17, 2018

Contents

About this Document

INTENDED READERSHIP

This document is available for prospective and current customers of Refinitiv's KYC as a Service (KYCaaS).

IN THIS DOCUMENT

This document describes the service that customers of KYCaaS can expect, alongside the experiences and choices that Refinitiv has designed for you to have. It covers all the stages of your interactions with the company, from initial interest through to end of usage. It is not a legally binding document but intended to give a reasonable expectation of the service you will receive as part of KYCaaS.

Please refer to this document for any information about the service included with KYCaaS, whether as a prospective or ongoing client. If you have any further questions, do not hesitate to contact us in any of the channels listed below. More information about the general service offered by Refinitiv is available upon request in the form of the Statement of Service.

KYC as a Service

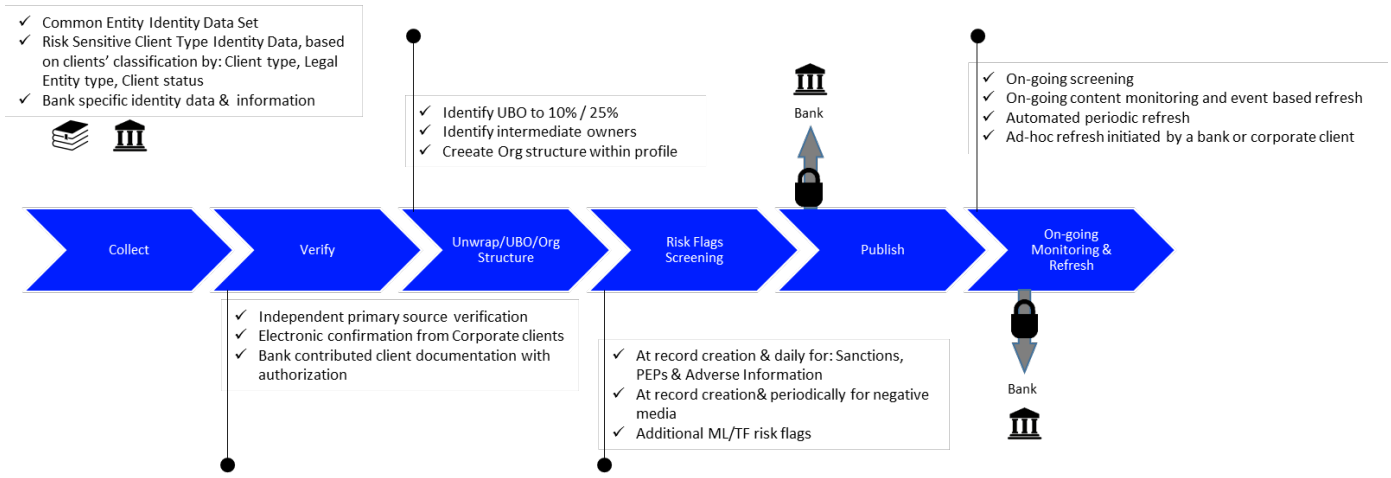
ABOUT

KYCaaS is a secure end-to-end client identity and verification, screening and monitoring service which integrates regulatory technology, market leading entity data and flexible and scalable operational capabilities. It has been designed to provide financial institutions and their end clients with a complete legal entity due diligence and document exchange solution which enables compliance with changing KYC regulatory requirements.

The service brings together a number of Refinitiv's risk-based solutions and offers a synthesis of client on-boarding platform, screening, monitoring and regulatory intelligence.

KYCaaS is a componentized service and is able to provide customers with the flexibility to address specific requirements within their existing processes. The core functions are summarized below:

- Due diligence based on a global KYC/AML policy and supported by continuous monitoring of legislation
- Classification of clients into one of three due diligence levels (Simplified, Standard or Heightened)
- Sourcing legal entity due diligence documents in over 200 markets and 60 languages
- Client outreach via a dedicated Client Liaison team
- Screening and identification of risk flags
- Ultimate beneficial owner unwrapping to 10%
- Ongoing monitoring and screening of completed KYC profile records
- Refresh and update of KYC profile records on a continuous basis



Services Provided

KYCaaS currently offers three different forms of service capability – managed, remediation, and document exchange.

Managed Service

KYCaaS provides financial institutions with a value-based approach to client due diligence by streamlining workflows to accelerate on-boarding on behalf of their end clients and providing high levels of operational integration and scalability.

Remediation Projects

KYCaaS remediation projects are one-off exercises to refresh end client records with up to date KYC information to an agreed level of due diligence and set timescale. The financial institution will provide KYCaaS with end client records which are built out as

required using existing data. These are then returned to the financial institution for management. No ongoing monitoring or screening of end client entities takes place as part of the remediation process.

Document Exchange

KYCaaS provides a free of charge online document exchange facility to provide end clients with a secure and efficient platform for proactively managing and sharing their identification data and documentation with multiple financial institutions. End clients are able to upload their relevant information via a secure web portal and use a permission based workflow to control distribution and access. The financial institution will receive a profile report and documentary proofs for the end client and relevant counterparties.

KYCaaS Policy

KYCaaS is underpinned by a risk based Global Regulatory Policy (Policy) which defines the parameters used for conducting due diligence on end clients and provides the basis for translating them into operational processes. The Policy has been stress tested by over 100 financial institutions and industry regulators and is regularly reviewed and updated in line with regulatory changes and industry standards.

Customized policies, called 'visas' are available for financial institutions whose identification and verification requirements fall outside the scope of the KYCaaS Policy.

KYCaaS Value Proposition and Benefits

KYCaas has been designed to address the operational challenges facing financial institutions as part of the client on-boarding process and enabling the delivery of a first class service to their end clients whilst ensuring regulatory compliance in a rapidly changing market. The service offers customers a genuinely differentiated solution in a competitive market and provides them with a number of clear and tangible benefits:

Benefits

- Operational efficiencies and cost savings by eliminating manual processes and enabling the automation of back office functions
- Improved customer retention through faster client on-boarding
- An enhanced client experience through a secure and permission controlled document exchange facility and user-friendly interfaces
- A scalable workflow to meet increased growth and fluctuations in volume
- Reduced regulatory burden through alignment with existing and future KYC regulations
- Revenue growth through reallocating resources to focus on value added activities and enabling cross selling
- Improved time to revenue by reducing the time taken for customer acceptance decisions during the on-boarding process
- Strict data protection and information security controls to access and protect sensitive customer data
- A risk based governance framework providing comprehensive levels of assurance supported by audit trails of changes to data and information

Differentiators

- Experience: KYCaaS was launched in 2014 as the industry's first KYC managed service and are the only provider to have successfully designed and operated a large regional KYC utility. The transferable knowledge and lessons learned from this project have enabled considerable value-add to customers.
- Depth and Quality of Data: KYCaaS has published nearly 400,000 KYC records across 140 countries and have the largest volume of completed profiles and maintained legal entity profiles (1.25million) in the market
- Regulatory Policy: The KYCaaS Policy has been informed by and stress tested with regulators and over 100 financial institutions, and covers over 40 jurisdictions
- Governance and Quality: KYCaaS are the only vendor in the market to be accredited with Type II ISAE3000 (PWC) for its operational processes and controls. This emphasis on quality assurance is reflected in the accuracy of the information in published end client records which is consistently over 98%
- Customer base: KYCaaS has built a customer base of over 55 financial institutions globally, which include a number of the world's top banks and asset managers. Over 3500 end client entities have distributed their private information through the document exchange platform

KYCaaS Components

An overview of the core components of KYCaaS have been summarized below:

Data Sources
The ability to access high quality 'golden' data sources in order to collect and verify the identity of an end client is a central design principle of KYCaaS. These have been defined using an industry standard developed and approved through consultation with financial institutions and are articulated in a set of individual Market Manuals covering over 220 jurisdictions. Both primary and secondary data sources are utilized, although KYCaaS will endeavor to use primary sources wherever possible, and include a number of Refinitiv's proprietary data sets such as World Check, Organization Authority, Lipper and Zawya.

Data Collection
The form and level of identity data collected on an end client is determined by their risk categorization based on a core set of attributes which includes; full name, address(es) and contact details, registration no. or unique identifier, country of formation, name, legal form and status.

Verification
KYCaaS uses risk sensitive standards to ensure that the sources used for verifying the identity of end clients are authentic and meet the requirements of the Policy. Further confirmation as to the accuracy of the information is provided by authorization from financial institution and electronic confirmation from the end client themselves.

Ultimate Beneficial Ownership
The identification of an end clients' ultimate beneficial owner, intermediaries and supporting ownership structure is an integral part of KYCaaS. The service is able to 'unwrap' this information to a 10% stakeholder threshold.

Screening
Refinitiv's WorldCheck is used by KYCaaS to screen entities, beneficial owners and related parties against sanctions and watchlists, PEP's, adverse information and negative media. This process is run on a daily basis and positive and possible identity matches will generate risk flags which are shared with the financial institution.

End Client Outreach
KYCaaS provides a dedicated outreach function which interfaces directly with end clients to support and guide them through the process of providing additional or missing information not available in the public domain. The team is trained in customer handling skills and are able to communicate in more than 60 languages. Customers using the service can achieve significant benefits through reduced overhead and enabling a greater utilization of efficiencies.

Ongoing Monitoring
Ongoing monitoring is used to ensure that information held on the end client is accurate and remains compliant with regulatory requirements. KYCaaS uses four separate processes to identify and share any changes to end client data:

- Daily screening for sanctions, PEP's and adverse information (periodically for negative media)
- Fixed periodic reviews of end client information at set times following completion of on-boarding
- Monitoring and event based refresh for activities that impact an end client record profile
- Dynamic monitoring to highlight red flags and potential problems before they develop

KYCaaS are the only KYC managed service provider to offer an ongoing screening and monitoring service.

Publishing End Client Records
Completed end client records are made available to financial institutions to view or download via the online portal (or API).

SCOPE AND SCALE

KYCaaS is relevant for both existing and prospective new customers of Refinitiv globally. These fall into two broad categories:

Financial Institutions (Subscribers)
Financial institutions are customers which have regulatory obligations to conduct due diligence on their end clients and will contract with and pay Refinitiv for the delivery of records. KYCaaS's current strategic focus is on two key growth segments of this market:

- Bilateral contracts with large financial institutions in EMEA, APAC and North America
- The growing market for regional and industry-based KYC utilities

End Clients (Contributors)

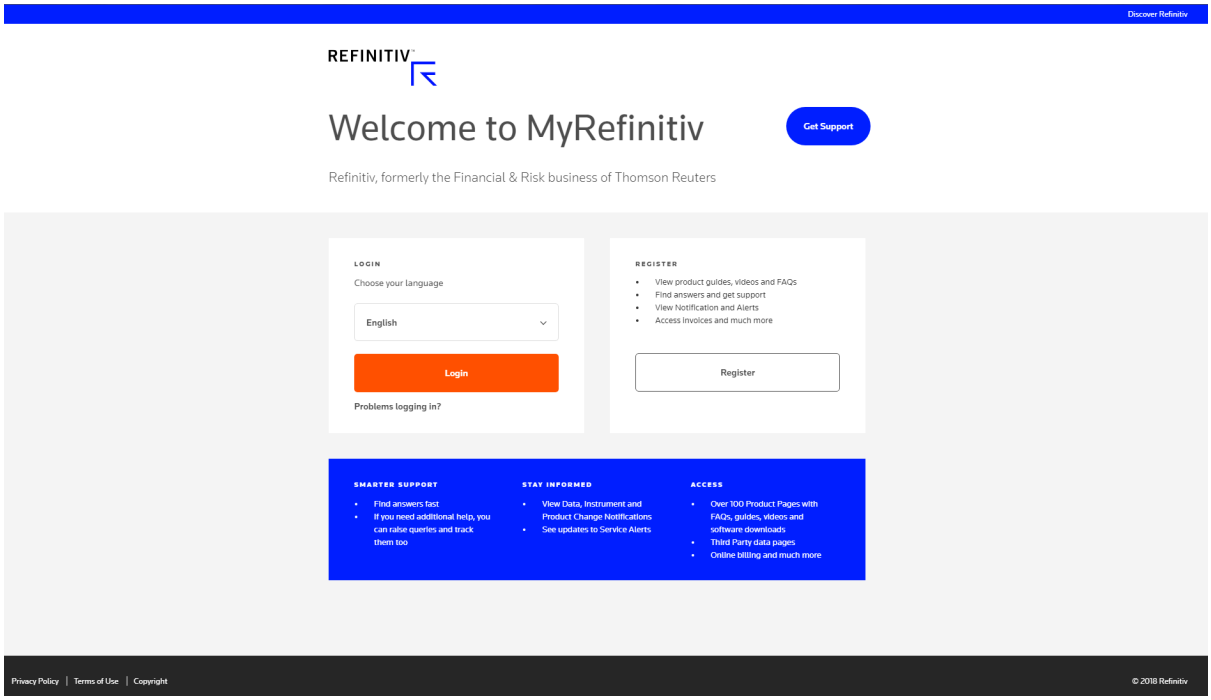
End clients are end users or counterparties on whom financial institutions are required to conduct due diligence. They provide the data required by KYCaaS to build their record and do not pay for use of the service. End clients also provide and permission access to their KYC documentation through the KYCaaS Document Exchange secure repository and sharing platform.

1. Discover

Prospective customers wishing to know more about KYCaaS are able to contact a specialist business development team who will provide advice and discuss their specific requirements in detail.

Existing customers can contact KYCaaS through their dedicated Account Manager, the My Account portal or by contacting the KYCaaS Business Support Team using telephone, email or the online portal as well as face to face.

MyRefinitiv is a portal that provides a single access point for timesaving support services, along with billing, user management, and product information and documentation.



2. Evaluate

A. DEMONSTRATION

KYCaaS is able to provide demonstrations to customers that will showcase the end to end process using a subset of end client records. The availability and scope of the demonstration is generally flexible and is built around customer requirements. It can be requested through the My Account portal or by contacting the Account Manager for existing customers or the KYCAAS business development team.

B. TRIAL

A Proof of Concept (PoC) is usually offered to customers for evaluation purposes. The scale, scope and timings are at the discretion of the customer and will typically involve providing KYCaaS with a list of end client entity names which are built out or populated to an agreed standard of due diligence from existing information in the KYCaaS database. If required, a comprehensive gap analysis process is used to highlight any variations between the customers' and the KYCaaS Policy which may require further attention. Copies of the completed records are then provided to the customer in order to enable an overall evaluation of the quality of service.

Content Requirement

The financial institution will provide KYCaaS with the end client entities to be used as part of the proof of concept.

Support

Support and training is provided as required during the proof of concept stage and will usually be arranged through the KYCaaS business development team and delivered by a subject matter expert.

3. Purchase & Renew

A. ORDERING

Managed service contracts with KYCaaS will typically run between three and six years. The contractual agreements with customers are translated into operational deliverables through a Statement of Work, which is used to set out details of the scope, operational requirements, processes and agreed pricing and commercial models.

Customers are able to raise orders on KYCaaS for end client records by using either a bulk request upload via secure file transfer on the FTP site or through an individual request via the portal.

B. BILLING

Billing for the KYCaaS managed service is based on the projected volume of end client records. It will usually consist of a fixed recurring quarterly service charge, invoiced in advance at the beginning of each quarter, and one off implementation and professional service charges for training, set-up and project management. Where there is a material deviation from the assumed volumes the quarterly charge is adjusted through a 're-baselining' process.

Additional factors, which may influence the pricing charged to customers, include:

- The scope of the service provided (for example: screening, ongoing monitoring and client outreach)
- The risk category of the client
- The minimum committed volume of profiles

There is usually no limit to the number of end client records that a customer can order from KYCaaS, although unit pricing may be tiered to reflect different pricing bands above certain volume thresholds.

Invoices are issued electronically and include:

- Date of the invoice
- Unique invoice number
- Period(s) to which the relevant Service Charge(s) relate
- Methodology applied to calculate the Service Charges plus supporting documentation if required
- Banking details for payment to KYCaaS via electronic transfer of funds

C. ENTITLEMENTS

Refinitiv's identity and access controls are used as the basis of KYCaaS' entitlements policy. Individual security levels and access to data are determined by a role-based permissions matrix. This process is covered in more detail in the section under security.

D. PACKAGING AND CONTRACT

Financial institutions subscribing to KYCaaS have the option of contracting with Refinitiv under one of two models, depending on whether they wish to leverage an existing Refinitiv Master Service Agreement (TRMA). Different contractual models apply to customers requiring remediation and end clients. The various details and options are highlighted below:

Financial Institutions

Managed service:

- TRMA:
  - TRMA Master terms
  - Screening schedule
  - KYCaaS schedule plus KYCaaS Commercial Appendices

- 'Standalone' KYCaaS contract
  - KYCaaS specific contract (The Agreement for the Provision of Refinitiv KYCaaS Services)
  - KYCaaS commercial appendices.

Remediation:

- GRC / Risk Client Terms of Business,
- Screening Schedule
- Professional Services Schedule
- A tailored Statement of Work (detailing the scope, pricing etc for the project).

End Clients

End clients will initially engage with KYCaaS through the online portal. Upon first login, users will accept the Terms of Use and confirm agreement with a Privacy Statement that contains details of how their data will be used. Where there are changes to the policies, users will be prompted to re-accept upon the next login.

4. Setup

A. IMPLEMENTATION

Following contract signature, a Client Consultant will be assigned to the customer to ensure a seamless transition and implementation. This process is based on a jointly agreed migration plan with milestones that has been developed following a review of the customer's specific processes and the changes necessary to integrate KYCaaS into their operations. The plan will use Refinitiv Global Policy Standards as a template and use RAID methodology to identify, mitigate and document potential risks. Functions and processes typically covered include policy alignment, operational workflows, governance, data migration, client data loading, user acceptance testing and set-up, training and stakeholder communication.

Typical key KYCaaS roles and responsibilities during the implementation phase are summarized below:

KYCaaS Role	Key Responsibilities
Director	- **Point of Escalation for major issues**
Head of Delivery	- **Resolve majority of escalated issues** - **Ensure that the implementation is managed in a professional manner**
Client Consultant	- **Act as single point of contact for the customer** - **Day to day management of the implementation process** - **Ensure risks are mitigated and delivery takes place on schedule**
Support Functions	- **Deliver support as required**

A post implementation review will be held approximately one month following go-live. This provides the opportunity to confirm that all elements of the migration plan have been delivered satisfactorily and ensure a seamless handover to a Refinitiv Account Manager who will be responsible for managing ongoing relationships and operations.

B. CONNECTIVITY

KYCaaS is compatible with most customer systems and third-party data platforms. User interface is via an HTML5 browser application which supports Internet Explorer 9 and above, Chrome, and Firefox (as the service is accessed via the internet no Microsoft Office plug- ins or Windows integration are required).

The integration and ingestion of end client data into a financial institutions' on-boarding workflow is through a web based dynamic API using a JSON data integration format with SSL encryption and secure FTP for bulk data imports. The API is language and platform independent and is compatible with the KYCaaS web portal, enabling them to be used interchangeably if required.

Integration is facilitated through the provision of a test environment that enables customers to evaluate the process using a dummy API user account, profiles and access to end clients.

C. HARDWARE

KYCaaS is accessed over the public internet via a web browser and does not require any dedicated hardware or IT infrastructure.

D. SOFTWARE

Customer integration via the KYCaaS Web API requires the following software:

- Web Browser
- SFTP client to upload files
- SSH application to access Refinitiv servers
- API Integration Client: To send https REST based requests over the internet to the KYCaaS Web API end points and receive data in response.
- API Request Management: To manage the linkages between customer requests for data and the corresponding KYCaaS request identifiers and end client identifiers.
- API data mapping: To map the KYCaaS data model onto the customers' own internal data model
- Document management: To provide an interface to the customers' document repository or document management system to provide storage for proof images from KYCaaS.

E. INSTALLATION ASSISTANCE

Installation of KYCaaS is via the web portal. Following receipt of a list of users of the service from the financial institution, a welcome email is sent to the relevant individuals. This includes a link, login credentials and a unique registration key which is used to prompt set-up and provide access to the portal.

The Client Consultant is responsible for working with the customer to ensure that the planning, implementation and delivery of KYCaaS is as seamless as possible. Specific assistance with installation is not usually required, however, if necessary, the customer will be able to contact either the Client Consultant or the Business Support Helpdesk.

F. TESTING

A comprehensive testing and quality assurance program that includes multi-tier system testing, development tests and predefined user acceptance testing scenarios, are run as part of each software release for KYCaaS. These are carried out in a separate pre-production test environment and any incidents are escalated through the incident management process for resolution.

User acceptance testing is usually provided as part of the implementation process (although it may not be required if the customer has already undertaken a PoC). Its purpose is to determine whether KYCaaS has been successfully implemented and installed and enable any system configurations to be made.

G. PROFESSIONAL SERVICES

Professional Services support for KYCaaS is provided by the Client Consultant. It typically covers the following activities:

- Change management activities associated with customer initiated policy changes
- Support during the implementation phase

- Support during API integration

5. Product & Usage

A. ENVISAGED USAGE

The purpose of KYCaaS is to provide financial institutions with a secure, flexible, efficient, and customer friendly due diligence service which delivers compliance with changing legal and regulatory requirements.

B. CAPACITY MANAGEMENT

KYCaaS utilizes a combination of long range, medium term and short-term planning to ensure that the delivery of end client records is able to meet customer demand. The capacity planning process is based on an 18 month forecast which is reviewed and, if necessary, updated on a monthly basis following input from customers and KYCaaS Operations and business development functions. Weekly meetings are also used to further refine the forecast by factoring short-term fluctuations into the process.

The KYCaaS capacity planning process is underpinned by highly scalable technology that provides the flexibility necessary to make any adjustment required to meet customer growth requirements.

C. SERVICE AVAILABILITY

The KYCaaS web portal and API is designed to be available to customers on a 24x7 basis. The specific performance indicators relating to service and application availability for customers are usually subject to negotiation as part of the commercial agreement.

D. MONITORING

Performance monitoring is a key function of the customer engagement process and will typically include formal reviews on a monthly or quarterly basis with the Account Manager as well as ad hoc communication with the relevant KYCaaS personnel. In cases requiring rapid resolution or escalation, customers are able to contact their Account Manager, Client Consultant or the Business Support helpdesk as required.

E. CONTENT COVERAGE

Details of approved KYCaaS data sources, documentary requirements, and jurisdiction-specific regulatory and legal information across areas such as corporate governance and ownership are articulated in 220 market manuals. These are reviewed and updated on a regular basis.

This model provides an established and effective blueprint for rapid coverage of jurisdictions not currently included in the KYCaaS Policy.

F. DATA TIMELINESS AND FREQUENCY

The frequency with which the data and information held in an end client record is updated or refreshed is driven by three factors:

- Periodic – End client records categorized as requiring Heightened due diligence are updated annually and those categorized as Standard and Simplified are updated every three years. The end client is notified in advance of any changes to their information.
- Events: KYCaaS monitors data sources to identify trigger events which may impact the end client such as a change of address, name or ownership. This component of the service requires the customer to have acquired ongoing monitoring and refresh functionality.
- New Requests: A financial institution wishes to on-board an entity which has an existing end client record held within the KYCaaS system

G. CUSTOMER RESPONSIBILITIES

Client Data

KYCaaS has been designed on the basis that the following controls and responsibilities relating to the use of client data and personal information are in place with prospective customers:

- Financial institutions will only use the personal information provided by KYCaaS for internal due diligence and screening in connection with anti-money laundering, anti-bribery and corruption, and other legal, compliance or risk management processes designed to prevent, detect or investigate financial crime.
- End client data is adequately protected in order to comply with Data Privacy obligations.
- Consent and permission for KYCaaS to use end client data is obtained in a timely manner

Additional responsibilities include ensuring that documentation and information provided to KYCaaS is accurate, complete and correctly formatted.

Implementation

As part of the implementation process, financial institutions are responsible for integrating the following:

- Client on-boarding platform / system
- Sales and customer relationship management workflow
- Document management services and/or file repositories
- Enterprise data management platforms
- Customer-specific data mapping
- Customer-specific systems integration
- Verify the security protocols on the Online Portal

Resources

Customers of KYCaaS are expected to provide an effective allocation of resources where necessary. These are used to ensure the availability of the appropriate authority to make decisions and sign off deliverables such as transition and transformation processes and to review end client records, documentation and key processes such as policy and process map gap analysis

H. SECURITY

The principles guiding KYCaaS' approach to security befit one of the world's leading providers of sensitive data and information. They are based on Refinitiv's Information Security Policy which mandates the policies which apply to its people, processes and technology and is endorsed by the Executive Committee.

The security practices used by KYCaaS are based on recognition of the criticality of data protection to financial institutions and end clients and are designed to ensure that they benefit from best practice. The policies and supporting standards are reviewed and updated as necessary to consider evolving technical risks, regulatory changes, and the information security requirements of customers.

Privacy

Your privacy and trust are important to Refinitiv. Please consult our Refinitiv Privacy Statement for more information.

Compliance

All KYCaaS policies, processes and structures are covered by an integrated risk assessment and governance model utilizing a best-approach methodology to identify and assess potential problems and ensure a proportionate response. This is verified through a comprehensive assessment program against the ISAE3000 assurance standard and supported by detailed audit trails of all user activity, actions on information and security events. KYCaaS are the only KYC managed service provider to have achieved this level of accreditation to date.

All KYCaaS risk and compliance policies are implemented through a three lines of defense model. This ensures alignment of the ownership and accountability of risk controls with internal and external governance processes.

Data Protection and Access Control

KYCaaS uses Refinitiv's managed data centres for the secure storage of data which are certified to ISO27001 and ISO9001 standards. All end client data is encrypted in motion and at rest using SSL/TLS and all backups are performed each weekend with incremental backups each weeknight.

Access to data for both KYCaaS and customers is through a strict role-based permissions model which is centrally managed by Refinitiv Business Support. This ensures that only those individuals with the appropriate roles and levels of authority are able to

access end client information. Any changes to user access require verification with an electronic signature and are tracked for audit purposes. End clients grant permission for financial institutions to access their data through acceptance of the Terms of Use.

Network & System Security

Access to the KYCaaS production environment is governed by controls which include multi-factor authentication and firewall protection which has been configured to only permit authorized traffic. Additional network protection is provided through the deployment of anti-virus software along with regular vulnerability assessments and third-party penetration testing.

Federated authentication for financial institutions can be provided through Refinitiv ONEPASS which enables each customer to implement their own security protocols.

Device and Cybersecurity

A number of preventative measures are used to ensure secure access to data through individual devices. These include dedicated terminals which are secured to allow only essential access to network resources and the internet, no local administrator rights or access to removable media and printers and bans on remote working, photography and printing in the KYCaaS record-processing centres

Physical Access and Environmental Security

Refinitiv data centres are secured by computer managed access control systems and security guard-monitored entrances with multi-level security access required for restricted areas. All access traffic is recorded, monitored and documented and all visitors are required to be signed in and escorted throughout the premises. Additional security features include fire suppression, air conditioning and an uninterruptible power supply with generator backup. .

Business Continuity and Disaster Recovery

KYCaaS has record-processing centres at Gdynia (Poland), Penang (Malaysia), Cape Town (South Africa) and Wrexham (UK). The business continuity plan is based on ensuring the effective and efficient transfer of record production and employees if one of these hubs is out of action and unavailable to staff (for example, due to fire, power or communications failures). The plan is tested at least annually and covers business impact assessments and recovery plans for critical business functions, an assessment of potential threats, vulnerabilities and scenarios and the ability to contact staff

The KYCaaS disaster recovery plan is aimed at minimizing disruption to operations by identifying potential single points of failure and ensuring that production functionality and data can be recovered as per the Recovery Time (4 hours) and Recovery Point (30 **minutes) objectives. The plan is tested and fully documented on a periodic basis in line with Refinitiv's Disaster Recovery** Policy.

J. COMMUNICATION

The governance framework employed by KYCaaS serves to ensure effective engagement and communication with customers throughout the entire process from implementation to the end of contract. The model includes the organizational and operational structures necessary to provide leadership, accountability, decision making and escalation as well facilitating the day to day running of the service, incident management and monitoring and reporting on performance.

An overview of the typical communication channels and interfaces with customers is provided below:

Meeting Type	Purpose/Agenda	Typical Attendees	Frequency & Format
Implementation Performance	Reviewing operational issues relating to implementation Performance against plan Data migration Quality control Other items as required	Customer – Project Manager KYCaaS – Client Consultant	Weekly during implementation Face to face or conference call
Service Performance	Review of operational issues relating to service performance Performance against service levels Other items as required	Customer – Regional Head of KYC Operations KYCaaS – Account Manager	Monthly following service commencement date Face to face or conference call

Business Review	Review of the relationship and any strategic issues relating to the service Service review On-going relationship and future engagement	Customer – Head of KYC Operations, Regional Head of Compliance KYCaaS – Account Manager, Global Head of Service Delivery	Typically within six months of commencing service and then quarterly thereafter Face to face
Annual Review	Review of the relationship and strategic issues relating to the service Service performance over the year Review of on-going relationship and future engagement Review of changes in the industry and the potential impact on the service and business relationship	Customer – Global and Regional Heads of KYC Operations, Global and Regional Heads of Compliance KYCaaS – Executive, Head of Service Delivery, Account Manager	Annually at the end of the contract year Face to face
Issue Resolution	Review and resolve contract and service related issues	Customer – As required depending on the issues KYCaaS – Account Manager and other depending on the issues	As required Conference call

Escalation

An escalation process is used to highlight and rapidly resolve issues which fall outside the remit of the responsible individual. The exact process will be dependent on the nature and prioritization of the issue, but will typically involve the KYCaaS Head of Service Delivery and Senior Management, if necessary. In order to ensure the effective resolution of escalated issues customers are expected to put in place a similar escalation process.

Documentation

Documentation provided to customers by KYCaaS will vary according to the nature of the service and the agreed contractual terms. However, it will typically include the following:

- A copy of the KYCaaS Policy & Standards
- Notification of any changes to the Policy which may affect the customer
- An API Developers Guide which will also enable data model gap analysis
- Access to the relevant governance and audit reports impacting KYCaaS such as ISAE3000
- Notification of system and technology updates

Reporting

The following standard reports are produced for KYCaaS customers:

Phase	Report Type	Content	Typical Recipients	Frequency
Implementation	Implementation Performance Report	Performance against implementation plan Data Migration Quality Assurance Other items as required	Customer Head of KYC Operations Customer Implementation Project Manager	Weekly - during implementation
Business as Usual	Service Performance Report	Service Levels and status of other Key Performance Indicators Root cause analysis (if required) Quality Assurance issues Other items as required	Customer Head of KYC Operations	Monthly –following the commencement of service
Specific	Incident	Details of material incidents/issues raised in the preceding month and actions to remedy/redress	Customer Head of KYC Operations	Monthly

K. THIRD PARTY APPLICATIONS AND SERVICES

Third party applications are not generally used by KYCaaS in the delivery of its core service. However, they may be utilized in instances where the scope and scale of the customer requirement demands additional technology or expertise. In these instances, the cost of these additional services will be included in the overall pricing to the customer.

6. Support

A. TRAINING

KYCaaS training programs are usually tailored to a customers' specific requirements and will typically include role-based training for relevant technical and process skills as well as 'train the trainer' and 'super user' modules.

Training is carried out by subject matter experts and aims to use real world examples to ensure maximum impact. The methodology used is flexible but will generally include one-to-one, workshops, seminars and virtual training delivered via Webex. The program is supported by communicating updates on changes or amendments to the KYCaaS policy.

B. SCOPE OF SUPPORT

The KYCaaS support model consists of four core components with an escalation process to subject matter experts and/or management where required:

- Business Support Helpdesk: This provides 1st and 2nd level support and is the initial point of contact for most customers. Its primary function is to provide product support and resolution updates on technical issues
- Client Consultant: The Client Consultant is responsible for the implementation of KYCaaS and ensuring the customer experiences a smooth transition to business as usual. They are available to provide any support required during this phase of the service delivery
- Account Manager: The Refinitiv Account Manager provides the initial point of contact and escalation for issues relating to ongoing running and performance of KYCaaS
- Portal: End users are able to utilize the portal to raise issues with the KYCaaS Quality Control function

A Client Liaison Manager is also available to customers who use the KYCaaS client outreach service. Their role is to co-ordinate an effective response from the relevant individuals within KYCaaS in the case of any issues.

C. SUPPORT CHANNELS

The communication and interface channels with the KYCaaS support functions are:

- Email: support.kycaas@thomsonreuters.com
- Online portal

Response times are dependent on the criticality of the issue but will typically be within 12 hours.

D. LANGUAGES AND AVAILABILITY

The Business Support team can provide support in English

Helpdesk support is available Monday to Friday 01:00 – 24:00 GMT.

E. INCIDENT MANAGEMENT

KYCaaS utilizes a structured and documented incident management and escalation model based on ITIL to ensure that incident resolution and root-cause analysis takes place as soon as possible. All incidents are prioritized according to severity and the details captured in a JIRA ticketing system and reported to the customer on a monthly basis via the Account Manager.

7. Evolution

A. FUTURE ENHANCEMENTS

Since its launch in 2014 KYCaaS has evolved in line with and encompassed market, regulatory and technology trends whilst particular importance is also given to customer feedback. This process is expected to continue with future short, medium and long-term developments and enhancements clearly articulated on a detailed roadmap. These are primarily aimed at providing a best in class service and customer experience through further enhancements in efficiency and in areas such as automated data collection.

As part of this extensive program, KYCaaS are currently engaged in leading a number of market wide initiatives with leading financial institutions, major customers and partners to fully understand the scope and scale of cross industry benefits available

through optimizing the client due diligence process. An example of this is in improving the availability of end client information through a wider facilitation of the document exchange process.

Refinitiv's role at the forefront of the marriage between financial and regulatory technologies has also enabled KYCaaS to take a highly informed and pragmatic leadership position on the potential value to existing and future customers of emerging themes in areas such as intelligent automation, open source API's, DLT and Big Data in client due diligence.

B. CHANGE MANAGEMENT

The KYCaaS change management process follows best practice and in the unlikely event of a problematic change or deployment, pre-tested and documented rollback procedures are in place to ensure minimum disruption.

Updates and upgrades to KYCaaS utilize regular maintenance windows and follow a structured change management and release process. Customers are usually notified a minimum of two days in advance of any planned service interruption.

The web portal is updated every month and the web API (REST/JSON) updates are configured to enable regular minor version updates to occur once a month in order to align with the web portal. They are also backwards compatible. Major version changes which require customers to make changes on their API client-side integration are made typically once every 6-12 months and at least two major versions are supported at any one time. This allows customers time to make any necessary adjustments in order to accept the major version changes. System patches are also centrally managed and are applied regularly to servers.

C. CANCELLATION

Customers wishing to cancel KYCaaS would typically discuss the details with their Account Manager in order to understand the circumstances or review possible alternatives if required. If an exit from the service is required a mutually agreed plan will be drawn up to cover the transition of the service in-house or to an alternative supplier.

Contractually, customers are able to cancel or terminate a contract with KYCaaS if there is a material change to the service provided which impacts their ability to provide a service to their customers. Mutual termination requires the use of break clauses in the contract and includes unremedied material breach and insolvency. KYCaaS does not offer contract cancellation for convenience as part of its standard terms and conditions.