MOODY'S

Service Level Document

What the service is

Grid is a risk database of adverse media, sanctions, watchlists and PEPs. It's the most comprehensive database of its kind. Risk information is curated into detailed profiles, by individual or organization, so you can see all associated risk-relevant data in structured detailed reports.

Grid helps you screen more effectively. Its combination of comprehensive data and categorization means you can filter content by risk type, risk stage and risk age, based on relevance and your own risk profiles, resulting in more precision, fewer false positive results and more efficiency.

Grid has over 28 million risk profiles. A risk profile can be about a person, or an organisation, and it's a collation of risk-relevant information relating to that entity.

Grid takes information from over 120,000 media sources, 1,800 watchlists and more. it covers 240 countries and territories and over 3 billion articles from the last 10 years.

It includes adverse media, sanctions and watchlists, PEPs and other focused datasets around risk themes including extended sanction coverage, Iran linked firms and the Panama Papers.

Get the 'gold standard' in adverse media screening

Global news coverage – the largest collection of negative news in the industry

Benefit from global media coverage ranging from large publications to those with low or regional circulation – more than 120,000 trusted media sources in all. We cover 240 countries and territories and over 70 languages. Grid has over 20 years of content and 10,000 risk profiles are added or updated every day.

Global watch list coverage - Grid integrates more than 1,800 government (regulatory) lists and watch lists, local, state and federal sources across the globe. also includes specialized databases covering sanctions, Iran, the Panama Papers and marijuana-related business.

Precise filters: precise alerts - Our highly categorized articles include more than 50 risk codes and 30 risk stages for precise filtering and precise alerting. Detailed categories include terrorism, human trafficking, organized crime, cybercrime and environmental crime. These categories align to the AML6 Predicate Offences and the designated categories of offences in the FATF Recommendations.

Simple integration - Integrate with your own systems and processes in a few simple steps.

PEPs – politically exposed persons

Grid provides detailed PEP coverage built on years of research covering individuals in 240 countries and territories. We've created a risk categorization system that considers the country, position, level, and event risks associated with the PEP. Our data meets or exceeds country and region-specific regulatory requirements and guiding principles including the US Patriot Act Section 312, the fourth and fifth EU anti-money laundering directive, the Financial Action Task Force (FATF) Recommendations and Wolfsberg Principles.

For countries that could be considered higher risk, you may want to consider a wider range of individuals in your risk assessments. For these we include data on opposition party members, shadow government officials, influencers, and other risk-relevant individuals.

A more holistic view of PEPs - Our PEP profiles deliver aggregated risk information from several sources. If a PEP is sanctioned, or appears in watchlists or adverse media, this information will be clearly indicated on their risk profile.

PEPs by category - Some PEPs can be considered higher risk than others. Our PEP information is structured and includes information on position type, country and classification. We use this information to create risk categories for PEPs. You can filter or prioritize screening results according to these risk groups, and other factors.

Sanctions and watchlists

Grid contains the most up-to-date and accurate sanctions and watchlist data sourced directly from government authorities. This is combined with a record of individuals and organizations connected to sanctioned entities, adhering to guidance published by the US Department of Treasury and the EU. Comprehensive coverage of watchlists We provide global coverage of domestic and international sanctions and watchlists which are checked daily for updates, including:

→ Office of Foreign Assets Control (OFAC) sanctions

→ United Nations Security Council (UNSC) sanctions

→ EU Consolidated List of Sanctioned Persons, Groups and Entities

→ UK HM Treasury sanctions

→ Australia Department of Foreign Affairs and Trade (DFAT) sanctions

→ Canada Special Economic Measures Act sanctions

→ Fugitive lists

→ Debarment lists

→ Fraud warning lists

Identify associated risk with Sanctions Connect - Sanctions Connect is a comprehensive dataset identifying individuals and organizations associated with sanctioned entities. This information helps meet regulatory requirements and protects against reputational risk by highlighting entities that may

pose a higher risk than would otherwise be known. The nature of the relationship to the sanctioned entity is clearly highlighted in profiles and can include:

Organization relationships

→ Subsidiaries (ownership > 50%).

→ Affiliates (ownership > 50%)

→ Board members and senior officials

→ Affiliated entities of board members and senior officials

→ Family members and close associates of board members and senior officials.

Individual relationships

→ Affiliated entities – all entities in which a sanctioned individual currently holds a position

→ Family members and close associates of sanctioned individuals.

Adverse media

You can identify a broad set of risks with global adverse media information gathered from more than 120,000 trusted sources. Profiles in Grid uncover relevant negative news information covering more than 50 categories of risk. These categories include all 22 predicate offences defined in the EU's sixth anti-money laundering directive and all designated categories of offences outlined in the FATF Recommendations.

Grid contains billions of relevant adverse media records sourced from news publications, magazine articles, television and radio transcripts. Global media sources cover every region in the world, ranging from large international publications to smaller, more local reporting.

Foreign language news is monitored from more than 75 countries and translated by linguists into English. Thousands of quality-checked media articles are added to Grid every day, helping to make sure you're alerted to the latest risks uncovered.

Automate your adverse media search - Once you match an individual or organization to a profile in Grid, relevant adverse media information is summarized highlighting the offence category, stage, date and source. All content is de-duplicated, so you do not need to trawl through long lists of articles or waste time reviewing irrelevant information.

Benefit from reliability - All media sources used in Grid must pass rigorous assessment for accuracy and quality. We strive to use source material from established media organizations with the highest journalistic standards wherever possible.

Specialist datasets

Iran Connect - Iran Connect is an expanding dataset identifying individuals and organizations with connections to Iran's energy, transport and military sectors. This information was originally compiled following the enactment of the US Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, and a coordinated tightening of sanctions against Iran imposed by the US, Canada, the EU and the UK. Coverage is continually updated as new information emerges.

Panama Papers - The Panama Papers comprises 11.5m files from the database of Panamanian law firm Mossack Fonseca. The files are related to how tax havens are used to hide wealth. More than 360,000 entities have been added to Grid following extensive data cleansing, including name and address parsing. The profiles of entities identified in the Panama Papers are combined with the full power of Grid to reveal any associations with adverse media, PEPs and sanctions, providing a complete view of risk.

Detailed risk profiles

Risk information is curated into detailed profiles, by individual or organization, so you can see all associated risk-relevant data in structured detailed reports. A short summary of the most relevant risk information is provided and then broken down by each risk event. The category, offence stage, date and source are clearly highlighted for each item, making it easier to analyze relevant information.

The levels of data backup and restore, and disaster recovery you'll provide, such as business continuity and disaster recovery plans

GRID maintains an appropriate BCP in compliance with applicable laws and consistent with industry standards.

→ BCPs are maintained and tested regularly: We review our BCP and risk assessment regularly. The BCP is tested and updated regularly to ensure that it is up to date and effective. We can provide a Business Continuity Disclosure statement upon request.

→ DR plans are maintained and tested annually: We maintain appropriate DR plans for each of our SaaS-hosted products. The plans include details on application description, key personnel, data backups and recovery, offsite storage, and failover and failback procedures. We perform annual disaster recovery tests for our SaaS-hosted products to validate the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) timeframes of less than or equal to 24 hours

The objective of the DRP covered in this document (document can be retrieved via: https://support.rdc.com/hc/en-us/articles/203900161-Disaster-Recovery-DR-Procedures-) is to return GRID system to normal operations as soon as possible with minimum data loss in the event of a disaster. Specifically, this DRP deals with unplanned events that result in the interruption of the GRID IT infrastructure components used to support GRID business processes, such as:

→ Computer systems

→ Data

→ Networks

→ Computer sites

→ Alerting Center

DRP is only one part of a Business Continuity Plan (BCP). DRP refers to an IT-focused plan designed to restore operation of the GRID system. The objectives of a BCP are to enable a company to survive a disaster and to reestablish normal business operations. This includes the restoration of IT infrastructure components as well as other day-to-day operations with focuses on sustaining an organization's business functions during and after a disruption. This DRP covers the following:

→ Overview of the current GRID processes

→ Identify risks and threats of each GRID component

→ Outline the procedure to reduce the risks and actions to be taken in the event of a failure of the component

→ Testing of the DRP

→ Activation of DRP

→ Maintenance of the DRP

Onboarding and offboarding support

Onboarding Support

Alignment & Connections - After a solution has been proposed, agreed and a contract has been signed we will begin to gather more detailed requirements for the configurations and settings. During this phase we will collaboratively revisit the requirements with the customer to ensure that they are complete and capture any changes since scope was agreed.

During the requirements gathering phase the customer will need to ensure they have enough resources internally to provide details to the Project Team of Bureau van Dijk for implementation. The capturing of the requirements could be in the form of workshops, meetings or online calls. During this phase we can further build out the initial timeline for implementation depending on the requirements and customization needs.

Configuration - With the requirements aligned with the customer, we have a solid base of requisites and set of expectations allowing us to move into the configuration design. The solution designed is based on our experience, capabilities and the proposed solution from the Use Case.

The solution design will cater for the scope of the project and is aligned with the initial expectations.

As part of this stage, we will create a Configurations by Risk Level documentation summarizing all settings required to implement the solution, as well as parameters required to configure it to the customer's needs. Once the document is ready, we will work collaboratively with the customer to review and approve the solution before moving to the Implement stage.

Design & Test Workflow - Once all detailed requirements have been gathered and agreed, the Moody's Project Team will then begin the implementation phase where the main substance of the project is delivered. Dependent on what product and delivery of data is permitted, we will see this taking varying times. If more than one product or delivery method is involved, more than one internal team at Moody's may get involved in the implementation.

We will communicate throughout this phase and update project documentation appropriately. A full team of delivery experts will be put on a project to ensure full coverage of duties and allow for thorough communication channels.

Initial implementation will be achieved through translation of the system requirements.

Training & Go-Live - Once implementation is completed, it's basically go-live. Training will be provided to the users who will be involved using the screening solution actively and besides your dedicated Relationship Manager, the account will be supported by the Customer Success Team within Moodys.

Offboarding Support

At offboarding, all client data is overwritten. Any data can be extracted using the usual reports.

Service constraints like maintenance windows or the level of customisation allowed

As a cloud-based SaaS based service there is no downtime associated to maintenance windows. In the rare event that maintenance requires the service be taken offline (e.g., for a large infrastructure update), adequate notice will be provided to all customers.

Service levels like performance, availability and support hours

Support help desk can be reached at ma_kyc_support@moodys.com, email support is available 24/7, phone support is available during office-hours (08:30 AM – 6 PM UK hours).

For phone support, please contact one of our client services teams at:

EMEA +44-20-7772-5454

AMERICAS +1-212-553-1653

ASIA PACIFIC +852-3551-3077

JAPAN +81-3-5408-4100

In case of an outage, please email clientservices@moodys.com with the subject line: Severity 1 Outage.

MOODY'S

After sales support

During post-delivery, each customer will have a dedicated team that will cover: front-line support (helpdesk), training, commercial account management, customer success, and solutions delivery. Each one of these roles provides a key element and together will ensure the customer has the best support possible.

We will outline this in a "Business as Usual" (BAU) document, making sure each support item has a defined point of contact. It is at this stage that a training plan, regular catch-up meetings, and future enhancements communications will be scheduled and agreed upon.

Hosting options and locations

US - AWS US East 1 (Virginia) is primary, Secondary is AWS US West 1 (Oregon), EU -

AWS EU West 1 (Ireland), Secondary is EU-Central 1 (Germany).

Access to data (upon exit)

Client data is overwritten shortly after the client exit. Therefore, any data extract must be done before then. The data can be extracted via reports, API or SFTP.

Security

Security and compliance of the cloud environment is a shared responsibility between the cloud service provider (CSP) (AWS or Microsoft Azure) and Moody's.

The CSP is responsible for protecting the infrastructure that runs all of the services that the CSP offers. This infrastructure is composed of the hardware, software, networking, and facilities that run the CSP's services. Moody's is responsible for designing, implementing, operating, and monitoring security controls implemented within the cloud. We have adopted the NIST Cyber Security Framework (CSF) for designing security controls on our applications/products and underlying services hosted on a public cloud environment. We have certified cloud security engineering team members who ensure that cloud environments are designed and architected with robust security controls. The cloud security engineering team follows the CSP's security best practices and guidelines in implementing security controls. The following cloud security controls are in addition to our standard information security controls and practices. Our cloud security controls include the following:

→ An identity and access management automated workflow system is used for provisioning and de-provisioning access to cloud services.

→ Before accessing the cloud environment, access to a Moody's Analytics corporate network is required. Access to the corporate network is managed through strong Active Directory credentials.

→ Once users log onto the corporate network, they can gain access to the cloud environment through Single Sign On (SSO). AWS user access permissions are controlled through AWS Identity Access Management (IAM) privileges and restricted based on job role. Microsoft Azure user access permissions are controlled by Azure Active Directory privileges and restricted based on job role.

→ Administrator access to the cloud console requires MFA and is restricted to the cloud engineering and security teams.

→ User access rights and privileges to the cloud environment are reviewed periodically.

→ In addition to our standard network security perimeter controls, we have implemented additional ingress and egress controls for cloud environments. These controls include implementing network segmentation using firewalls, Virtual Private Clouds (VPCs), and security groups.

→ We use container scanning and inspection services to provide security controls for container images and orchestration activity.

→ We have a cloud tagging policy that outlines tagging standards to follow while creating CSP resources.

→ We gain visibility into cloud workloads at all layers through various log collection and monitoring features. Logs from AWS CloudTrail, CloudWatch, and VPC flow are forwarded to our SIEM solution for analysis. Similarly, logs from Azure Log Analytics, Azure App Insights, and Azure Monitor and Virtual Network are forwarded to our SIEM solution for analysis.

→ We use cloud security and compliance monitoring tools to provide continuous monitoring of the cloud environment for security policy violations.

→ We architect cloud environments to be resilient using AWS and Microsoft Azure architecture design patterns:

→ For AWS, we use multi-Availability Zones/Regions, backups on S3 buckets, and AWS managed Relational Database Service.

→ For Microsoft Azure, we use Azure Availability Zones/Regional Pairs, geo-redundant backups on Azure Blob Storage, and the Azure SQL/PostgreSQL database.

MOODY'S

For more information visit moodys.com/publicsector

MOODY'S

from sources MOODY'S considers to be reliable including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the credit rating process or in preparing its Materials.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY CREDIT RATING, ASSESSMENT, OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby discloses that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any credit rating, agreed to pay to Moody's Investors Service, Inc. for credit ratings opinions and services rendered by it. MCO and Moody's Investors Service also maintain policies and procedures to address the independence of Moody's Investors Service credit ratings and credit rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold credit ratings from Moody's Investors Service, Inc. and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at www.moodys.com under the heading "Investor Relations — Corporate Governance — Charter Documents - Director and Shareholder Affiliation Policy."

Moody's SF Japan K.K., Moody's Local AR Agente de Calificación de Riesgo S.A., Moody's Local BR Agência de Classificação de Risco LTDA, Moody's Local MX S.A. de C.V, I.C.V., Moody's Local PE Clasificadora de Riesgo S.A., and Moody's Local PA Calificadora de Riesgo S.A. (collectively, the "Moody's Non-NRSRO CRAs") are all indirectly wholly-owned credit rating agency subsidiaries of MCO. None of the Moody's Non-NRSRO CRAs is a Nationally Recognized Statistical Rating Organization.

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited ABN 61 003 399 657AFSL 336969 and/or Moody's Analytics Australia Pty Ltd ABN 94 105 136 972 AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761G of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761G of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not on the equity securities of the issuer or any form of security that is available to retail investors.

Additional terms for India only: Moody's credit ratings, Assessments, other opinions and Materials are not intended to be and shall not be relied upon or used by any users located in India in relation to securities listed or proposed to be listed on Indian stock exchanges.

Additional terms with respect to Second Party Opinions (as defined in Moody's Investors Service Rating Symbols and Definitions): Please note that a Second Party Opinion ("SPO") is not a "credit rating". The issuance of SPOs is not a regulated activity in many jurisdictions, including Singapore. JAPAN: In Japan, development and provision of SPOs fall under the category of "Ancillary Businesses", not "Credit Rating Business", and are not subject to the regulations applicable to "Credit Rating Business" under the Financial Instruments and Exchange Act of Japan and its relevant regulation. PRC: Any SPO: (1) does not constitute a PRC Green Bond Assessment as defined under any relevant PRC laws or regulations; (2) cannot be included in any registration statement, offering circular, prospectus or any other documents submitted to the PRC regulatory authorities or otherwise used to satisfy any PRC regulatory disclosure requirement; and (3) cannot be used within the PRC for any regulatory purpose or for any other purpose which is not permitted under relevant PRC laws or regulations. For the purposes of this disclaimer, "PRC" refers to the mainland of the People's Republic of China, excluding Hong Kong, Macau and Taiwan.