



BUREAU VAN DIJK

A Moody's Analytics Company

Your **A-Z** guide

to corporate ownership and
compliance terms

Click on a letter to look
up a compliance term

J L
N
Q
V X
Y

- > **Anti-money laundering (AML)**
- > **AML 4**
- > **AML 5**
- > **AML 6**
- > **Anti-bribery and corruption (ABC)**
- > **Artificial intelligence**
- > **Association of Certified Anti-Money Laundering Specialists (ACAMS)**
- > **Audit trail**

Anti-money laundering (AML)

AML encompasses all efforts to combat money laundering and terrorist financing. Across much of the globe, governments have passed legislation that compels banks and other institutions to comply. AML programs should include written policies, procedures and controls, a designated AML compliance officer, employee training, and independent review and testing.

See also > [Money laundering](#)

AML 4

The European Union's Fourth Anti-Money Laundering Directive – AML 4 – took effect in the national legislatures of all (then 28) Member States on 26th June 2017.

- It aimed to harmonize anti-money laundering laws in the EU with those in the US.
- Businesses became legally required to hold beneficial ownership records.

People with significant control (PSC) are sometimes included in the definition of beneficial owners. A common lower limit for beneficial ownership is 25% at any hierarchical level in a corporate ownership structure.

See also > [AML 5](#); [AML 6](#)

AML 5

A series of amendments to AML 4, agreed in December 2017, specify that EU citizens will have access to ownership records on companies operating in the EU, even without having to demonstrate 'legitimate interest'.

- > **Anti-money laundering (AML)**
- > **AML 4**
- > **AML 5**
- > **AML 6**
- > **Anti-bribery and corruption (ABC)**
- > **Artificial intelligence**
- > **Association of Certified Anti-Money Laundering Specialists (ACAMS)**
- > **Audit trail**

AML 6

AML 6 is being transposed into national law by EU Member States by December 2020; those laws must be implemented by June 2021. It focuses on criminal offences and penalties, listing 22 predicate offences concerning money laundering. It will also increase the accountability of companies, including aiding, abetting, attempting and inciting money laundering offences.

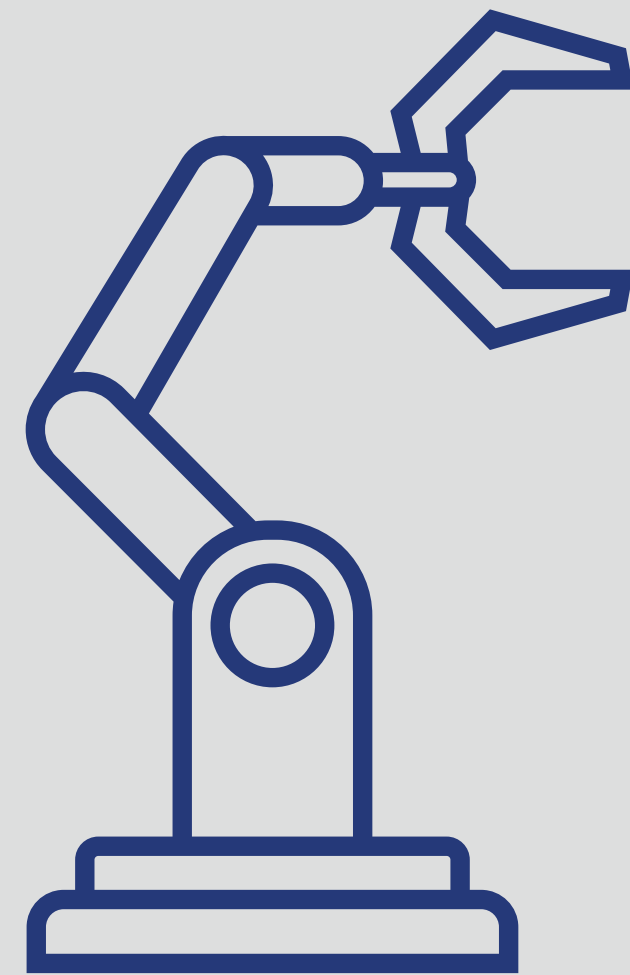
The 22 offences mean that companies will be keen to screen for connections with money laundering including cybercrime, environmental crime, human trafficking and migrant smuggling, arms dealing and counterfeiting.

Anti-bribery and corruption (ABC)

Anti-bribery and corruption (ABC) relates to banks' and other companies' processes (some of them legal requirements) for cracking down on corruption generally and on bribes specifically. Bribes refer to inducements given or offered to individuals or entities to benefit the briber.

See also > **Politically exposed person**

- > **Anti-money laundering (AML)**
- > **AML 4**
- > **AML 5**
- > **AML 6**
- > **Anti-bribery and corruption (ABC)**
- > **Artificial intelligence**
- > **Association of Certified Anti-Money Laundering Specialists (ACAMS)**
- > **Audit trail**



Artificial intelligence

Artificial intelligence (AI) uses machine learning to carry out compliance tasks such as screening. AI review is a screening solution that is capable of accurately imitating the decisions of analysts when reviewing alerts. It can quickly process alerts, significantly reducing false positives while improving consistency.

Association of Certified Anti-Money Laundering Specialists (ACAMS)

ACAMS is an influential international membership organization dedicated to enhancing the knowledge and expertise of anti-money laundering (AML), countering the financing of terrorism (CFT) and financial crime detection.

Audit trail

An audit trail is a manual or electronic record that chronologically logs events, procedures or operations. It can provide proof of compliance and operational integrity, as well as identifying any areas of non-compliance.

See also > **Compliance; Due diligence; Enhanced due diligence**

- > **Beneficial owner**
- > **BIS**
- > **Bribery**
- > **Bribery Act 2010**
- > **Bureau van Dijk**

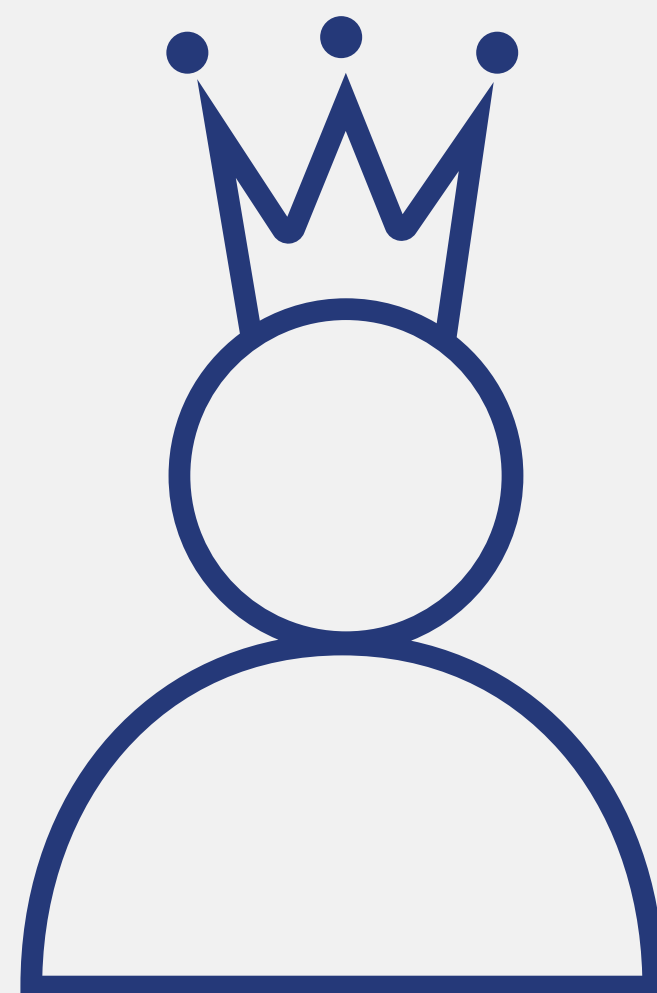
Beneficial owner

A beneficial owner is a 'natural person(s) [individual(s)] who ultimately owns or controls a company and/or the natural person on whose behalf a transaction is being conducted', according to the intergovernmental body Financial Action Task Force (FATF). It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

See also > **Financial Action Task Force (FATF); Countering the financing of terrorism (CFT)**



[Read more on beneficial ownership](#)



BIS

The US Bureau of Industry and Security (BIS) regulates national security and technology, such as the export of arms and sensitive goods, including software.

See also > **Export Administration Regulation (EAR)**

Bribery

See also > **Anti-bribery and corruption (ABC)**

Bribery Act 2010

An influential UK law, perhaps the most comprehensive on the subject and similar to the Foreign Corrupt Practices Act in the US.

- > Beneficial owner
- > BIS
- > Bribery
- > Bribery Act 2010
- > Bureau van Dijk

Bureau van Dijk

Welcome to the business of certainty.

We capture and treat entity information for better decision making and increased efficiency.

With information on some 400 million companies across all countries worldwide, we are the leading resource for entity data.

We do all we can to add certainty to your compliance decision making by delivering information derived from rigorous processes, a huge variety of sources, and treating it to make it as easy as possible to compare companies internationally and evaluate risk.

Data defines who we are and what we do. We are committed to providing the best breadth and depth of information on the market, including adverse media, news and risk events.

Our entity data resource Orbis powers state-of-the-art compliance with our decision making risk platform Compliance Catalyst.

See also > [Compliance Catalyst](#); [Grid](#); [Orbis](#)



- > **California Consumer Privacy Act 2018**
- > **Client on-boarding**
- > **Company**
- > **Compliance**
- > **Compliance Catalyst**
- > **Controlling ownership**
- > **Countering the financing of terrorism (CFT)**
- > **Criminal Finances Act 2017**
- > **Cryptoassets**
- > **Currency (cash) transaction report**
- > **Customer Due Diligence (CDD) Final Rule**
- > **Cybercrime**

California Consumer Privacy Act 2018

This privacy rights protection legislation nevertheless allows for the collection of California residents' personal information for compliance with legal obligations, including combatting fincrime.

See also > **Financial Crimes Enforcement Network (FinCEN)**

Client on-boarding

See > **Know your customer**

Company

See > **Entity**

Compliance

Compliance is the discipline of ensuring that companies conform to the national and international rules of conduct, both in their internal operations and in their connections with third parties. In relation to corporate ownership research, third-party dealings are key. Researchers must perform due diligence – often a specific area of customer due diligence (CDD) – not only on their third parties but on some of their owners. Identifying the types of owner and their percentage shareholdings is crucial.

Whether for regulatory reasons or for reputation protection, compliance relates to the overlapping areas of anti-money laundering (AML), know your customer (KYC), anti-terrorist financing, anti-bribery and corruption (ABC), and sanctions enforcement. These are all linked to ownership.

- > **California Consumer Privacy Act 2018**
- > **Client on-boarding**
- > **Company**
- > **Compliance**
- > **Compliance Catalyst**
- > **Controlling ownership**
- > **Countering the financing of terrorism (CFT)**
- > **Criminal Finances Act 2017**
- > **Cryptoassets**
- > **Currency (cash) transaction report**
- > **Customer Due Diligence (CDD) Final Rule**
- > **Cybercrime**

Compliance Catalyst

The data-driven decision engine and risk management platform, Compliance Catalyst combines data and technology in a single platform. It blends your data with the best entity data powered by Orbis, risk events and adverse media (from Grid) and flexible, automated risk analysis and screening. It streamlines know-your-customer (KYC), AML and ABC research to make your client onboarding and customer due diligence more efficient.

See also > **Grid; Orbis;**



Controlling ownership

The concept of control has many meanings, ranging from voting rights to decision making and general influence. In compliance, it is strongly associated with sanctions, one of the key influential bodies overseeing sanctions being OFAC in the US. You cannot do business with individuals or entities that are sanctioned. Crucially an entity can be sanctioned by extension through its ownership relationships.

Controlling ownership of an entity by an individual or other entity is determined purely by that individual's or other entity's total direct ownership percentage share of the entity; 50% is the usual lower limit. Note that for compliance research, in some jurisdictions the cut-off is 50% plus one share, while in others it is exactly 50% (despite the potential voting stalemate).

Determining whether an individual or entity exceeds the limit can be difficult for complex structures. Note that total integrated ownership isn't usually relevant for determining control. What matters is control at each level in a corporate structure.

See also > **People with significant control; Sanctioned by extension**

- > **California Consumer Privacy Act 2018**
- > **Client on-boarding**
- > **Company**
- > **Compliance**
- > **Compliance Catalyst**
- > **Controlling ownership**
- > **Countering the financing of terrorism (CFT)**
- > **Criminal Finances Act 2017**
- > **Cryptoassets**
- > **Currency (cash) transaction report**
- > **Customer Due Diligence (CDD) Final Rule**
- > **Cybercrime**

Countering the financing of terrorism (CFT)

Countering the financing of terrorism (CFT) forms part of AML compliance under the Financial Action Task Force's global compliance standards.

See also > **Beneficial owner; FATF (Financial Action Task Force); Financial Crimes Enforcement Network (FinCEN)**

Criminal Finances Act 2017

This UK Criminal Finances Act is designed to give law enforcement agencies and partners capabilities and powers to recover the proceeds of crime, tackle money laundering, tax evasion and corruption, and combat the financing of terrorism.

Cryptoassets

Emerging currencies such as Bitcoin, and other anonymous asset classes and 'wallet service providers' (WSPs) are potential vehicles for money laundering. They are regulated in the EU under AML 5 and in the US by the Bank Secrecy Act (BSA) 1970.

Currency (cash) transaction report

US companies must file a currency transaction report (CTR) with FinCEN for any cash currency transaction in excess of \$10,000.

See also > **Financial Crimes Enforcement Network (FinCEN)**

- > **California Consumer Privacy Act 2018**
- > **Client on-boarding**
- > **Company**
- > **Compliance**
- > **Compliance Catalyst**
- > **Controlling ownership**
- > **Countering the financing of terrorism (CFT)**
- > **Criminal Finances Act 2017**
- > **Cryptoassets**
- > **Currency (cash) transaction report**
- > **Customer Due Diligence (CDD) Final Rule**
- > **Cybercrime**

Customer Due Diligence (CDD) Final Rule

The CDD Rule aims to improve financial transparency and prevent criminals using companies to hide illicit activities and money-laundering in the US. The Rule clarifies customer due diligence requirements for US banks, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities. These financial institutions must verify the identity of the beneficial owners of legal entity customers who own, control and profit from companies when they open accounts.

See also > **Compliance; Due diligence/customer due diligence (CDD); Enhanced due diligence (EDD)**

Cybercrime

Computers, networks and the internet have been a boon to fincrime as well as instrumental in combatting it. Digitization and automation not only allow more transactions but bring with them the increasing integration of financial systems, integration which in turn amplifies the risk of fincrime, including money laundering, bribery, tax evasion and fraud.

- > **Department of Justice**
- > **De-risking**
- > **Due diligence/customer due diligence (CDD)**
- > **Duty of Vigilance Law**

Department of Justice

Many relevant laws emanate from the US Department of Justice (DoJ), some with naturally resulting supranational applications, given globalization. The UK equivalent is the Ministry of Justice (MoJ), and many countries regulate activities through similar departments.

De-risking

Refers to banks and other financial institutions closing the accounts of clients that are perceived to be high-risk in relation to money laundering or terrorist financing. Remittance companies and local banks worldwide are often the target of de-risking.

Due diligence/customer due diligence (CDD)

Due diligence is the general process of investigating an individual or entity before signing a contract or entering a significant business relationship with them. While some types of due diligence are carried out to assess the commercial viability of a such a relationship, other types are legal obligations. Due diligence generally and customer due diligence (CDD) specifically are strictly controlled in banks and are related to know-your-customer programs.

See also > **Enhanced due diligence (EDD)**

Duty of Vigilance Law

In France, under the Duty of Vigilance Law 2017, corporations are legally obliged to identify and prevent negative effects on human rights and the environment resulting from their own activity and activity within their supply chain.

- > **Enhanced due diligence (EDD)**
- > **Entity**
- > **Entity resolution**
- > **Environmental, social, governance (ESG)**
- > **European Union (EU)**
- > **Europol**
- > **Export administration regulation (EAR)**

Enhanced due diligence (EDD)

This consists of tougher measures designed for customers deemed 'higher-risk' in relation to money laundering or terrorist financing. A bank may demand information on the purpose of the account, the source of funds, details on individuals with control over the account, financial statements, domicile information and explanation of any changes in account activity, or other details.

See also > **Due diligence/customer due diligence (CDD)**

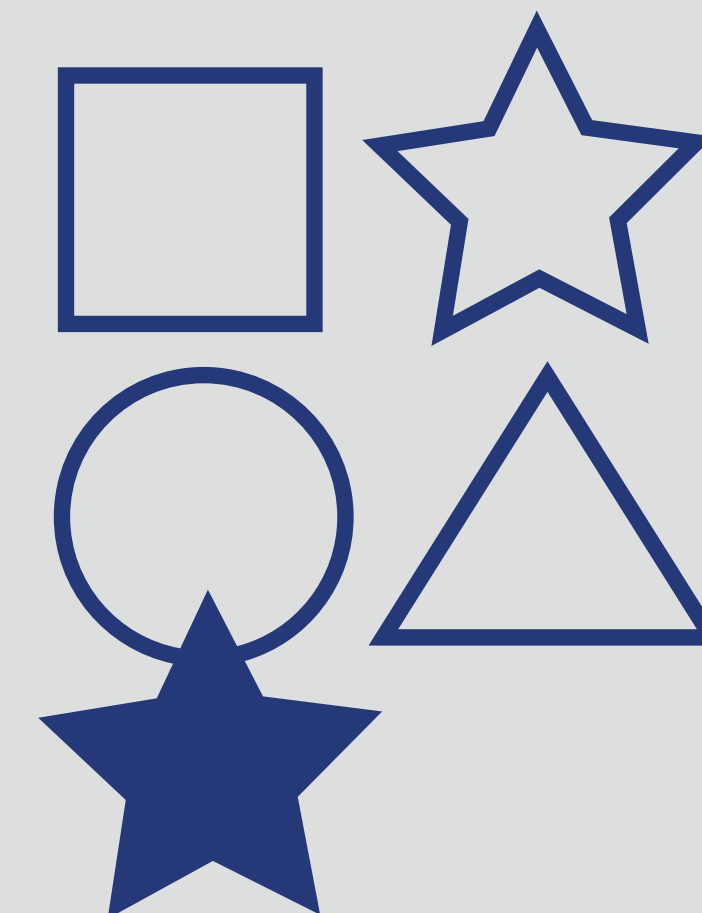
Entity

In corporate ownership research, entity refers to a company or person. It includes organizations such as charities and non-profit organizations, trusts, partnerships, and public authorities. On the Orbis database, all entities are given Bureau van Dijk identities to aid their positive identification and verification, particularly those with names similar or identical to those of others. Entities in the financial services sector carry internationally recognized legal entity identifiers (LEIs), regulated by the Global LEI Foundation (GLEIF).

Entity resolution

This is the process of disambiguating records of entities within different datasets by matching, linking and grouping. This process makes use of LEIs and other unique identifiers. Orbis can be used to match information from different datasets to build a better picture of an entity, such as identifying associated companies, companies within a wider corporate group, their directors or beneficial owners.

See > **Entity**



- > Enhanced due diligence (EDD)
- > Entity
- > Entity resolution
- > Environmental, social, governance (ESG)
- > European Union (EU)
- > Europol
- > Export administration regulation (EAR)

Environmental, social, governance (ESG)

Environmental, social and governance (ESG) reporting is often used as an indicator of potential (reputational) risk as well as for ethical reasons. Investors increasingly seek ESG data and many jurisdictions have already made some reporting mandatory, such as under the EU Directive on Disclosure of Non-financial and Diversity Information; future standardization is likely.

European Union (EU)

A supranational economic and political union. Through regulations and directives, such as on anti-money laundering, the EU drives much of Europe's compliance rules; non-EU members doing business with EU Member States are often required to comply with EU regulation.

Europol

Serving EU Member States, Europol combats terrorism, drug trafficking, money laundering, organized fraud, the counterfeiting of euros and human trafficking.

Export administration regulation (EAR)

The US Bureau of Industry and Security administers Export Admission Regulations (EAR), which relate to exports, re-exports and the transferral of goods and technology from one person to another in a foreign country.

- > **Fail fast**
- > **Financial Action Task Force (FATF)**
- > **Financial Conduct Authority (FCA)**
- > **Financial crime ('fincrime')**
- > **Financial Crimes Enforcement Network (FinCEN)**
- > **Financial intelligence unit (FIU)**
- > **Foreign Account Tax Compliance Act (FATCA)**
- > **Foreign and Commonwealth Office (FCO)**
- > **Foreign and Corrupt Practices Act (FCPA)**
- > **Fraud**

Fail fast

A fail fast approach speeds up your compliance screening by quickly identifying cases that will not pass your risk assessment and flagging them immediately, rather than allowing the assessment process to continue.

See also > **Due diligence/customer due diligence (CDD); Enhanced due diligence (EDD)**

Financial Conduct Authority (FCA)

The FCA is the conduct regulator for financial services firms and financial markets in the UK and the prudential regulator for about a third of those firms.

Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) on Money Laundering is a highly influential intergovernmental body that was set up by G7 countries (Canada, France, Germany, Italy, Japan, UK and US) to counter money laundering.

See also > **Beneficial owner; Countering the financing of terrorism (CFT)**

Financial crime ('fincrime')

Financial crime (known as 'fincrime') includes any kind of criminal conduct relating to money, financial services or markets. It includes fraud, dishonesty, bribery, corruption, misuse of information, handling the proceeds of crime and the financing of terrorism, according to the Financial Conduct Authority (FCA), the UK regulator.

Fincrime may generate wealth for the criminal or may intend to conceal the proceeds of crime.

- > Fail fast
- > **Financial Action Task Force (FATF)**
- > **Financial Conduct Authority (FCA)**
- > Financial crime ('fincrime')
- > **Financial Crimes Enforcement Network (FinCEN)**
- > **Financial intelligence unit (FIU)**
- > **Foreign Account Tax Compliance Act (FATCA)**
- > **Foreign and Commonwealth Office (FCO)**
- > **Foreign and Corrupt Practices Act (FCPA)**
- > Fraud

Financial Crimes Enforcement Network (FinCEN)

Financial Crimes Enforcement Network, a bureau of the US Treasury.

See also > **California Consumer Privacy Act 2018**

Financial intelligence unit (FIU)

The FIU is the unit in a bank that investigates suspicious activities identified by the transaction monitoring system. The FIU will either clear the transaction (a 'false positive') or file a Suspicious Activity Report (SAR).

Foreign Account Tax Compliance Act (FATCA)

The Foreign Account Tax Compliance Act 2010 (FATCA) is an influential US law that requires foreign financial institutions and other entities to report on the foreign assets held by their US account holders.

- > Fail fast
- > Financial Action Task Force (FATF)
- > Financial Conduct Authority (FCA)
- > Financial crime ('fincrime')
- > Financial Crimes Enforcement Network (FinCEN)
- > Financial intelligence unit (FIU)
- > Foreign Account Tax Compliance Act (FATCA)
- > Foreign and Commonwealth Office (FCO)
- > Foreign and Corrupt Practices Act (FCPA)
- > Fraud

Foreign and Commonwealth Office (FCO)

The FCO is a department of the UK government. It is responsible for protecting and promoting British interests worldwide. The US equivalent is the Department of State.

Foreign and Corrupt Practices Act (FCPA)

The Foreign and Corrupt Practices Act 1977 (FCPA), an influential US law, is similar to the UK's Bribery Act 2010.

Fraud

Wrongful or criminal deception intended to result in financial or personal gain.

General Data Protection Regulation (GDPR)

Introduced in the EU in 2018, GDPR relates to the handling of personal data and limits its collection, use and storage. GDPR Article 6 allows for personal data collection for AML and sanctions purposes.

- > **General Data Protection Regulation (GDPR)**
- > **Global Slavery Index**
- > **Global ultimate owner (GUO)**
- > **Grid**

Global ultimate owner (GUO)

A GUO is the individual or entity at the top of the corporate ownership structure. Flagged up on Orbis and Orbis Ownership Explorer, GUO identification is increasingly important, given the tightening of supranational sanctions regimes and other compliance considerations. For some applications, it's also useful to identify domestic ultimate owners (DUOs) – the highest owning entity in a country. Note that being a GUO doesn't necessarily imply being either a controlling owner or beneficial owner.

Global Slavery Index

Australia's Walk Free (Minderoo) Foundation compiles a country ranking based on the number of people it estimates to be in modern slavery. This index can be used within Compliance Catalyst to assist in screening third parties.

Grid

Grid is a dataset that combines regulatory and risk intelligence with adverse media screening. It's known as the most comprehensive risk dataset of its kind, and can be precisely customized to risk appetite and risk topics. We apply natural language processing to capture, treat and categorize adverse news, and AI for assessing alerts. We deliver an integrated view of adverse media, PEPs, sanctions, and watchlists and a high level of alert relevance.

See also > **Orbis**



H •

> Her Majesty's Revenue and Customs (HMRC)

Her Majesty's Revenue and Customs (HMRC)

HMRC is a non-ministerial department of the UK government responsible for the collection of taxes, the payment of some forms of state support and the administration of other regulatory regimes including the national minimum wage.

The US equivalent is the Internal Revenue Service (IRS).

- > **Individual – legal term**
- > **Industry Denied Persons List**

Individual – legal term

Individual, person and natural person are usually interchangeable terms used in corporate ownership research to indicate people – as distinct from entities. Individuals can own or part-own entities (as can other entities) and can be directors of them. Human owners and directors of any entity under investigation need to be established in case they are on any sanctions list or are in some other way a compliance concern.

Industry Denied Persons List

This US list includes people or companies whose export privileges have been denied by the Bureau of Industry and Security.

See also > **Export Administration Regulation (EAR)**

Know your customer (KYC)

Closely associated with customer due diligence and client onboarding, know your customer (KYC) deals with 'anti-money laundering policies and procedures used to determine the true identity of a customer and the type of activity that is 'normal and expected'', and 'detect activity that is 'unusual' for a particular customer', according to the Association of Certified Anti-Money Laundering Specialists (ACAMS). KYC is most associated with the banking sector; KYE ('know your everything') and KYS ('know your supplier') are increasingly used.

See also > [Compliance](#)

> **Money laundering**

> **Monitoring**

Money laundering

The Association of Certified Anti-Money Laundering Specialists (ACAMS) describes money laundering as 'the process of concealing or disguising the existence, source, movement, destination or illegal application of illicitly-derived property or funds to make them appear legitimate. It usually involves a three-part system: placement of funds into a financial system; layering of transactions to disguise the source, ownership and location of the funds; and integration of the funds into society in the form of holdings that appear legitimate, though the exact definition varies between countries. Often conducted through the compliance departments of banks and other companies, anti-money laundering (AML) is the practice of detecting money launderers, reporting and preventing their activity, and limiting business with them.

See also > **Anti-money laundering (AML)**

Monitoring

This is the ongoing process of checks carried out following customer onboarding. It is part of wider know-your-customer (KYC) processes and AML measures against associations with sanctioned individuals and entities.

- > **OFAC**
- > **Office for Professional Body Anti-Money Laundering Supervision (OPBAS)**
- > **OFSI**
- > **Orbis**
- > **Ownership Explorer**
- > **Owner/ownership**

OFAC

The Office of Foreign Assets Control (OFAC) of the US Treasury administers and enforces economic and trade sanctions.

Office for Professional Body Anti-Money Laundering Supervision

The Office for Professional Body Anti-Money Laundering Supervision (OPBAS) is a regulator set up by the UK government in 2018 to strengthen anti-money laundering (AML) supervision.

OFSI

The Office of Financial Sanctions Implementation (OFSI) helps to explain and enforce sanctions in the UK.

Orbis

Orbis is the leading entity and event data resource. Coverage includes private and listed companies, banks, insurance companies, marine vessels, sole traders and individuals associated with entities. It also covers risk events, M&A activity and changes in ownership.

It's used to identify and analyze entities and events worldwide for better, faster decision making. Orbis powers Compliance Catalyst, and contains extensive corporate ownership structures that highlight ultimate and beneficial owners, and power and control. These structures are screened against PEP and sanctions watchlists, as well as adverse media algorithms, so you can get a holistic view of risk associated with specific entities and individuals.

See also > **Compliance Catalyst; Grid**



- > OFAC
- > Office for Professional Body Anti-Money Laundering Supervision (OPBAS)
- > OFSI
- > Orbis
- > Ownership Explorer
- > Owner/ownership

Ownership Explorer

Bureau van Dijk's Ownership Explorer is a dynamic visualization tool that provides navigable bottom-up and top-down views of complex corporate ownership structures. It shows: the ownership relationships entities have with other entities and with individuals; direct and indirect ownership percentages; controlling owners and beneficial owners, depending on your chosen ownership percentage thresholds for different levels in a corporate group; and whether entities or individuals are on any politically exposed persons (PEPs) and sanctions lists. It also allows users to set overall percentage thresholds, so that complicated structures can be simplified by removing from the picture individuals and entities with small percentage shares.

Owner/ownership

Ultimately, all entities are owned by individuals, be it private individuals (through partnership or shareholdings) or, in the case of state-owned enterprises, citizens. Ownership is measured in percentage shares, which are usually in proportion to voting rights for key decisions. An important exception is with people of significant control (PSC).

Ownership percentage shareholdings – in some cases combined through integrated ownership; in other cases, simply the percentage at any given level in a corporate ownership structure – are an all-important consideration in many areas of third-party due diligence and compliance.

- > **People with significant control (PSC)**
- > **Politically exposed person (PEP)**
- > **Power Score**

People with significant control (PSC)

AML 4, superseded by AML 6, expanded the EU's definition of beneficial owners to include people with significant control. Examples of people with significant control (PSC) include CEOs, CFOs and company chairpersons; people who don't necessarily own any shares in a company but may nevertheless exert influence.

AML 4 requires national governments to maintain PSC registers and people performing compliance checks on companies must consult with this information.

Politically exposed person (PEP)

A politically exposed person is an individual deemed to be potentially corruptible – through bribes or other means – because of their position of influence in government or the public sphere, or their strong links to people in government, such as spouses.

There is no legislative reason to avoid doing business with PEPs, and no impropriety is automatically implied by being one. But companies should at least be aware if a PEP owns, part-owns or is a director of a third-party entity, or if they are dealing with a state-owned enterprise. PEPs are flagged within Orbis and Orbis Ownership Explorer.

Power Score

The Power Score helps you understand control and influence – regardless of ownership. It reveals the most influential shareholders in a company. And it shows you different permutations of shareholders who can form decision-influencing coalitions. The Power Score is available in Orbis, Compliance Catalyst or via data feed from Bureau van Dijk.



- > RDC
- > RegTech
- > Reputational risk
- > Risk
- > Risk based approach

RDC

RDC (Regulatory DataCorp) was born out of the September 11 terrorist attacks in the US, which drew attention to the need for better screening against terrorists. Banks were subsequently required (under the US Patriot Act) to vet clients in advance of onboarding, leading a consortium of 20 financial institutions to set up RDC to integrate their data screening.

RDC will be known as Bureau van Dijk from early 2021 as a result of its acquisition. Together we offer fast validation and screening of entities, entity data (including corporate structures and beneficial ownership) and curated adverse media.

RegTech

RegTech is the use of new technology to help the delivery of regulatory requirements. It's becoming ever more important as regulation increases and the focus on data and reporting intensifies.

Reputational risk

The actions of your associates can impact your business reputation as heavily as those of your own business and staff. Monitoring for associations with PEPs, sanctioned individuals and entities and confirmed or potential bad actors – those associated with fincrime – is essential in mitigating against reputational risk.

- > RDC
- > RegTech
- > Reputational risk
- > Risk
- > Risk based approach

Risk

A common definition of risk is the exposure to the chance of injury or loss. In a compliance context, loss is usually financial. Financial loss can be direct: if you sell to a company with low creditworthiness, they might not be able to pay you; or if you break the law, you might be fined. Relating to regulatory risk, law-breaking is more directly relevant to considerations of compliance and ownership. (Note, though, that in the case of creditworthiness, a company's ownership 'environment' will affect its 'qualitative financial strength', a type of score on Orbis.)

Financial loss can also be indirect: your reputation, and therefore customers' loyalty, can suffer if you're seen to be acting improperly, regardless of whether you're breaking the rules. This is in addition to any possible fines that do arise from legal violations. Most companies therefore take a risk based approach to their decision making, aided by their compliance staff and influenced by their risk appetite, sector and other external factors. Investigating and assessing the ownership of third parties falls within this framework.

Risk based approach

A risk based approach is where companies prioritise compliance in the areas of greatest risk. It is a strategy supported by most regulatory authorities and involves identifying and quantifying risks, and then implementing policies and procedures to mitigate against them.

- > **Sanctions**
- > **Sanctioned by extension**
- > **Sapin II**
- > **Source of wealth**
- > **Specially Designated National (SDN)**
- > **State-invested enterprise (SIE)**
- > **State-owned enterprise (SOE)**

Sanctions

Sanctions and embargoes are political trade restrictions put in place against target countries by foreign governments. Some sanctions are more particular and apply only to specific individuals, entities and governments within certain countries. Established by the likes of the UN, the EU and the US government, sanctions apply to anyone doing business within any jurisdiction that has put them into their national laws.

See also > **Controlling ownership; OFAC; Sanctioned by extension**

Sanctioned by extension

Sanctioned by extension, sometimes called ‘sanctioned by association’, relates to the general issue of controlling ownership and is referenced in OFAC’s guidance notes on the 50% rule.

Relying on the cascade-down effect, the rule states that a company is sanctioned by extension if: an unbroken chain of ownership links leads to full or part-ownership by a sanctioned individual or entity; and in none of the chains is the ownership share less than 50%.

Note that the stake in a lower company of a sanctioned individual or entity could be tiny but still have the effect of sanctioning that company by extension; crossing just seven levels, each at 50%, reduces one’s share to less than 1%.

Bureau van Dijk identifies companies that are sanctioned by extension according to OFAC and EU lists.



S

- > Sanctions
- > Sanctioned by extension
- > Sapin II
- > Source of wealth
- > Specially Designated National (SDN)
- > State-invested enterprise (SIE)
- > State-owned enterprise (SOE)

Sapin II

The French law Sapin II 2017 places an obligation on companies to take steps to detect corruption through third-party due diligence and other measures.

Source of wealth

This refers to the origin of a person's entire body of wealth, often within the context of KYC checks. For example, ownership of a business, employment, inheritance or investments.

Under the UK Criminal Finances Act 2017, an 'unexplained wealth order' can be issued by the High Court. This requires a person who is suspected of involvement in serious crime to explain the nature and extent of their interest in particular property, especially where there are grounds to suspect that the respondent's known income would be insufficient to allow them to obtain that property. It can also be applied to politicians or officials from outside the European Economic Area, such as politically exposed persons (PEPs). The first Order was issued in October 2018.

Specially Designated National (SDN)

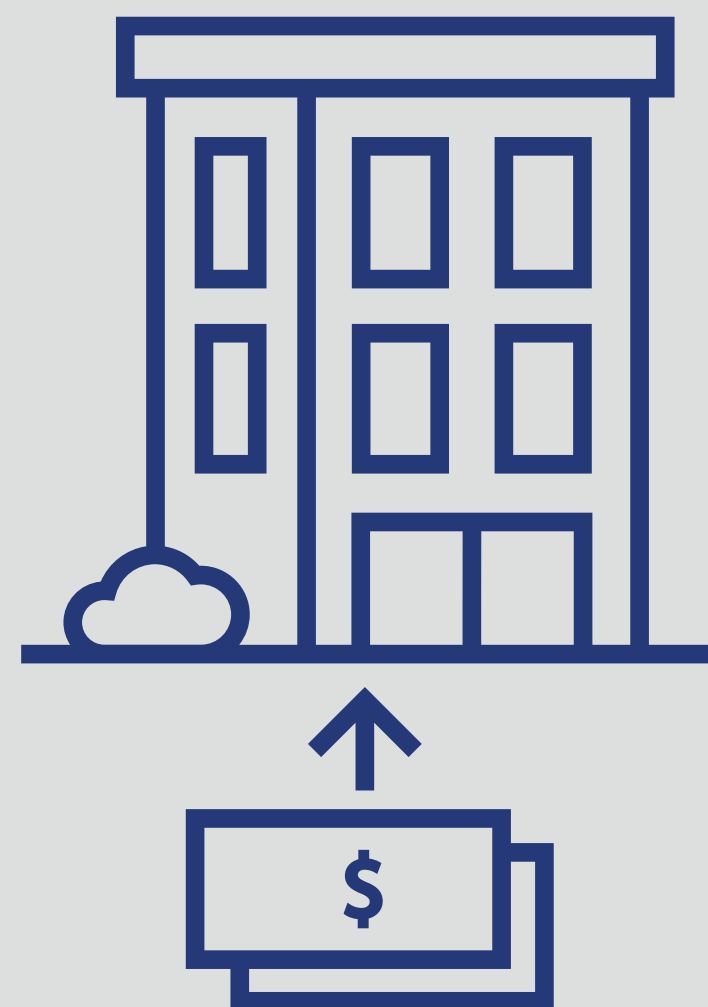
The US Department of the Treasury defines a SDN as an individual acting on behalf of a country targeted by sanctions, or engaged in prohibited activities such as terrorism or drug trafficking. Their assets are blocked and US persons are generally prohibited from dealing with such a person.

- > **Sanctions**
- > **Sanctioned by extension**
- > **Sapin II**
- > **Source of wealth**
- > **Specially Designated National (SDN)**
- > **State-invested enterprise (SIE)**
- > **State-owned enterprise (SOE)**

State-invested enterprise (SIE)

State-invested enterprises are those in which a sovereign state holds a stake, allowing the possibility for influence and, ultimately, the potential risk of corruption.

See also > **State-owned enterprise (SOE)**



State-owned enterprise (SOE)

As their name suggests, state-owned enterprises (SOEs) or state-owned companies (SOCs), are entities owned or part-owned by sovereign states. SOEs engage in commercial activities on behalf of their governments.

Examples include the BBC and Royal Bank of Scotland in the UK, Amtrak in the US, SNCF in France, and ABN AMRO in the Netherlands.

There are several reasons people find this information useful, but from a compliance point of view one of the most important is sanctions screening.

See also > **State-invested enterprise (SIE)**



> **Transaction monitoring**

Transaction monitoring

By monitoring historical and current customer transactions such as transfers, deposits and withdrawals, financial institutions are able to detect potentially suspicious activity that may be indicative of fincrime.

See > **Financial Crime ('fincrime')**

U •

US Patriot Act

Officially named 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT)', the Act aims to deter and punish terrorism, including money laundering and the financing of terrorism.

> US Patriot Act

W •

Wolfsberg Group

The Wolfsberg Group is an association of thirteen global banks, forged in 2000, which aims to develop frameworks and guidance for the management of financial crime risks.

> Wolfsberg Group

Zephyr

Bureau van Dijk's Zephyr, the most comprehensive database of deal information, will be known as Orbis M&A in 2021. Zephyr includes information on M&A, IPO, private equity and venture capital deals and rumours to help you track changes in ownership.

> Zephyr



BUREAU VAN DIJK

A Moody's Analytics Company

Welcome to the business of certainty

bvd@bvinfo.com

© 2020 Bureau van Dijk Editions
Electroniques S.A., Moody's Analytics,
Inc., and/or their affiliates and licensors.
All rights reserved. LON-CMP-11.20