ADS Securing UK advantage

UK FINANCE

SUPPORTED BY

Department for Business & Trade

GUIDE FOR THE DEFENCE AND SECURITY SECTORS ON ACCESS TO FINANCIAL SERVICES IN THE UK

DECEMBER 2023



GUIDE FOR THE DEFENCE AND SECURITY SECTORS ON ACCESS TO FINANCIAL SERVICES IN THE UK

CONTENTS

- ADS Group and UK Finance foreword from Chief Executive Officer's
- Department for Business and Trade foreword
- Introduction

PART ONE

- Things to consider when applying for finance or banking services
- What defence and security sector businesses need to do and demonstrate

PART TWO

- What providers need to consider

- Annex A
- Annex B

CHIEF EXECUTIVE OFFICER'S FOREWORD FROM ADS GROUP AND UK FINANCE

As UK Finance and as ADS, we are honoured to represent our world-leading industries, and proudly advocate for their ability to operate within robust regulatory frameworks. The UK's world-leading financial services sector is renowned for its strong regulatory framework, all while being committed to ensuring that financial services can play an essential role in international security. ADS members deliver innovative and entrepreneurial solutions to combatting global geopolitical challenges, all while adhering to strict international regulatory protocols.

Our member businesses have clear collaboration opportunities, and this document serves to empower our respective industrial bases to deliver stricter, more streamlined adherence to overcoming regulatory burdens. By reducing the perceived burden of regulatory adherence at the get-go, we hope to deliver a stronger, more collaborative and inclusive risk environment.

Collaboration between the ADS Group and UK Finance, demonstrated in part by this joint guide, aims to ensure defence and security businesses have the tools and knowledge they need to innovate, scale and grow.

Kevin Craven, CEO, ADS Group
David Postings, CEO, UK Finance

DEPARTMENT FOR BUSINESS AND TRADE FOREWORD



Kevin Hollinrake MP

Minister for Enterprise, Markets and Small Business

Department for Business and Trade

Access to finance is one of the key enablers for growth. The UK is fortunate to have a world-leading financial services sector, which facilitates payments and channels investment to the rest of the economy. For too many businesses however, even accessing basic banking services is fraught with difficulty.

According to my Department's Inward Investment Client Insight Survey, 56% of new investors to the UK reported setting up a bank account as their biggest challenge. Similar issues are faced by some domestic companies, particularly those in sensitive sectors such as defence. This caution on the part of banks reflects stringent requirements designed to prevent money laundering and other forms of financial crime, with significant penalties for non-compliance.

The regulations that seek to prevent money laundering, breaches of sanctions and other illegal activities also require banks to keep their concerns confidential. If the 'red flags' were widely known, it would not take long for criminals to work out how to avoid raising suspicion. However this prohibition on 'tipping-off' is understandably frustrating for genuine businesses, who are keen to resolve the unknown difficulties that are delaying or preventing their account from being opened.

In short, even where all parties involved are acting transparently and ethically, there may be factors that prevent a bank account from being opened, or lead an existing account to be closed. Tackling this requires a united approach and I commend UK Finance and ADS for their collaboration on the issue. This guide is an excellent start.

Through the Economic Crime and Corporate Transparency Act, which recently became law, we are improving the ability of banks, law firms and accountants to share information with each other. The same Act also gives Companies House new and enhanced powers to improve the quality and reliability of data, including proper identity verification for all company directors and persons with significant control.

With continued collaboration and dialogue I am confident that we can further improve the experience for defence companies of opening and operating a bank account, contributing to the government's goal of making the UK the best place in the world to start and grow a business.

INTRODUCTION

This guidance is aimed at businesses operating in the defence and security sectors in the UK. UK Finance the collective voice for the banking and finance industry and ADS, the trade association for the UK's aerospace, defence, security and space sectors, have developed this document with input from members of both organisations and the Department for Business and Trade (DBT).

The fundamental aim of this document is to explain the factors that businesses need to consider when seeking support from the financial services sector in the UK, whilst explaining the different regulations that the banking sector is required to operate with in which can influence their risk appetite, especially with SMEs.

The UK's defence and security sectors directly employ 285,000 people across the UK with those businesses in turn responsible for £45 billion of turnover. Over 90% of ADS members are SMEs. As there are currently over 9,000 UK companies operating in the defence and security sectors, including Small and Medium Enterprises (SMEs), this is of undeniable significance to the UK economy and ecosystem of businesses.

The current geo-political environment, including ongoing conflicts, has thrown a spotlight on the necessity and value of maintaining a resilient and thriving defence and security industrial base in the UK. In turn, this requires UK-based financial products and services, to enable businesses to operate, invest, innovate, and grow. It is notable that these conflicts are changing public conversations with defence and security sectors recognised as essential endeavours in the ESG landscape.

Financial service providers in the UK are committed to supporting UK businesses, including defence and security organisations through start up, scale up and growth. While lenders have their own risk appetite and specific market focus, there is now a significant range of finance options available.

Despite the various means to provide financial support there are experiences within the defence and security sectors that suggest accessing finance and banking services in recent years has become harder. SMEs in particular have reported experiences of challenges, including the ability to open a high-street bank account in the UK; banks serving notice to terminate business accounts; a requirement for 100% cover for bonds resulting in cashflow problems; and difficulties accessing finance. Whilst acknowledging that each business is assessed for financial services under individual circumstances, SMEs are assessed with additional considerations including debt affordability and adherence to regulations.

This is due, in part, to the significant growth of the regulatory framework that financial service organisations now operate within, and the penalties imposed for non-compliance. For example, several UK lenders have received significant fines for inadequate customer due diligence and monitoring of business customers in relation to money laundering. The UK's regulatory framework plays an important role in crime prevention, including against fraud, despite this over £1.2 billion was stolen by criminals through authorised and unauthorised fraud in 2022.

This guidance has two core elements:

Part one details some actions that companies should consider taking before they apply for a new product or service. This guide aims to help businesses avoid common pitfalls they face when trying to access financial services in the UK.

Part two sets out the range and complexity of factors that financial service organisations need to consider when providing banking services and finance to companies in the defence and security sectors are explored.

Within the annexes there are some sources and signposts to additional advice and support that is available beyond this.

ADS are also working with industry to understand planning within the ESG landscape on a broader level. It is important for businesses to have their own sustainability strategy and ADS are bringing groups together to set collective goals.

As part of this work, ADS has united the defence industry around a new ESG Charter for the future of environmental, social and governance standards in the industry.

THINGS TO CONSIDER WHEN APPLYING FOR FINANCE OR BANKING SERVICES

Many UK based providers can, and do, support those businesses in the defence and security sector that are able to demonstrate they meet certain criteria. Policies will differ across financial service organisations and will change from time to time. Some lenders publish their defence and security policies, although many do not, preferring to make decisions on a case-by-case basis. Some examples of published policies are listed in Annex A.

- **Typical provider approach and policies**
- **Interpretation of International Law**
- **Existence of licenses, including export licenses**
- **Policy framework and ethical responsibility**
- **Provider implementation of regulations and standards**
- **Understanding Confidentiality Clauses**
- **Case Study**

Typical provider approach and policies

There are broad policies on the provision of financial services to all kinds of businesses, which operate alongside the specific checks on the defence and security sectors. Broad policies include on ownership structure, financial viability, and past and predicted performance of businesses.

In relation to the defence and security sectors, providers' risk assessment processes will include whether customers, or prospective customers, appropriately follow internationally accepted standards as well as regional laws and regulations specific to these industries. They will also consider whether businesses adhere to relevant international agreements, guidelines, regulations, and voluntary standards.

The information included in the next part of this guide is based on generalised practices and includes some common approaches taken by providers. Businesses in the sector should contact providers directly if they wish to obtain a copy of specific policies or wish to understand how these policies might apply to them.

Interpretation of International Law

Providers may not offer or continue to offer products and services to a business that is directly or indirectly, through its supplies of parts, components, systems, or services, involved in the production of weapons considered illegal according to international law.

Examples would be anti-personnel mines, cluster munitions, and biological and chemical weapons. This can also include businesses that are involved in the stockpiling, transferring or use of these weapons. Although nuclear weapons, within the Non-Proliferation Treaty, are legal, many providers consider that use of nuclear weapons could have indiscriminate and devastating impacts and could be a violation of human rights and so do not support financing related activity.

Some providers will not offer services or finance to companies engaged in activities in any way contained within the Non- Proliferation Treaty. UK providers have on occasion had policies that prohibit any relationship, or in some cases may depend on the degree to which the business is undertaking military business or arms manufacture.

Existence of licenses including export licenses

Businesses operating in the defence and security sectors producing defence or security related goods and dual-use technology are subject to specialist regulations designed to address the potential risk of products obtained by undesirable third parties. In most nations this is addressed through the implementation of some form of trade controls under which a licence has to be sought and obtained from the government. Known as an export or trade control licence, which in the UK is granted by the Export Control Joint Unit (ECJU) within DBT.

The process to obtain an export or trade control license is complex and requires businesses to submit significant company and product information about the nature of their proposed export. Many businesses who have gone through the process of obtaining a licence feel they have shared significant compliance data with government and stakeholders that should enhance their ability to access UK financial services.

Regardless of the industry, government-issued licenses are not considered to be sufficient in and of themselves to satisfy compliance and due diligence requirements that underpin provision of finance regulations. A provider may not offer or will retract the offer of products and services to a business that is directly or indirectly exporting any type of weapon or component part, to what they regard as being an ‘oppressive regime’.

If sanctions or export controls have a nexus to the goods or transactions, the financial services provider will also have to apply for licences. Frequently this requires a licence from ECJU to facilitate the financial aspect of the goods moving as well as a financial licence from Office of Financial Sanctions Implementation (OFSI) to allow the transaction to be undertaken.

Even with a licence, lenders will still make case-by-case decisions of their own, based on their own internal processes and procedures about facilitating defence transactions, based on the product type, jurisdiction and intended end-use of the products or services.

The Export Control Joint Unit provides a wide range of training-related activities on the complete range of export control-related topics. Details of these are available at:

- Training on export control compliance - GOV.UK (www.gov.uk)
- Compliance code of practice for export licensing - GOV.UK (www.gov.uk)
- Checklist of internal export control compliance procedures - GOV.UK (www.gov.uk)
- Export control compliance case studies - GOV.UK (www.gov.uk)

The financial services licence requirements are hosted by OFSI.
https://www.gov.uk/guidance/licences-that-allow-activity-prohibited-by-financial-sanctions

Policy framework and ethical responsibility

UK financial service providers are committed to responsible lending and ensuring that services and activities have a positive impact on people, communities, and the planet. As such, many lenders are committed to supporting UK businesses in the defence and security sectors, recognising the critical importance of doing so. The sector as a whole is, however, also mindful of the need to comply with regulations and of broader public debate around the manufacture and supply of weapons.

Provider implementation

Providers will typically adopt a risk-based approach, based on carrying out appropriate due diligence when opening accounts or providing credit or other products to the defence and security industries. The due diligence serves to verify whether there is any possible risk of involvement in illegal or controversial activity. It also considers non sector specific issues, such as commercial viability and trading performance.

Customers will sometimes have to go through additional reviews that require providers to obtain further details of their military contracts. This is to ensure they are not dealing with any sanctioned entities or goods subject to Financial or Trade sanctions, or goods controlled under the Export Control Order 2008. Providers prefer to engage with businesses that ensure adherence to higher standards of responsibility and compliance. If a provider is unsatisfied or has any doubts about the integrity of the business, products and services will not be offered or continued.

Understanding Confidentiality Clauses

For any institution lending money to businesses, one of the most important things they need to do is understand the business they are dealing with, including what and to whom they sell. Many transactions taking place within the defence and security sectors are subject to certain levels of confidentiality which restricts the sharing of information required by a provider to enable them to fully understand the business.

For businesses supplying in the defence and security sectors it is important to be aware of and understand the contracts being entered into with buyers. For example, the use of a confidentiality clause such as a Ban on Assignment can affect a business's ability to access finance. The use of Ban on Assignment clauses is quite common within the defence and security sectors.

In 2018 the UK Government introduced legislation prohibiting the use of Ban on Assignment clauses in contracts with SME suppliers but retained a number of exclusions from this legislation. This included contracts that concern national security interests, so many defence-related contracts retain the right to use these clauses.

This means that SMEs, while working under contract for a significant defence or security employer, are often denied access to finance, because they have signed a contract which prohibits them discussing the nature of the work they are undertaking. Whilst this ultimately protects national security because companies are supporting the government with their requirements, this in turn hampers the ability of providers to undertake appropriate due diligence.

CASE STUDY: Invoice Financing

Invoice finance is a widely used form of cashflow finance, which enables businesses to access somewhere between 70% and 90% of the value of invoices outstanding as soon as they have supplied their goods or services (instead of waiting up to 90 days to be paid). It enables growth, stability, and flexibility to many UK businesses. However, these products rely on the assignment of receivables (sales invoices) from the business to the invoice finance provider and is the finance provider's main source of security. If a contract between a supplier and buyer has a Ban on Assignment clause within it, this effectively stops the supplier being allowed to use their invoices to generate cashflow through this method.

WHAT DEFENCE AND SECURITY BUSINESSES NEED TO DO AND DEMONSTRATE

As businesses prepare to request a product or service from a provider, there are some best practice steps to take:

- Make sure that policy statements on lending to the defence and security sector are read where they are available.
  - A list of published policies is set out in Annex A.
  - Many providers, especially smaller and specialist lenders, do not publish their policies and consider applications on a case-by-case basis.
- Business, particularly SMEs, should consider referring to the Institute of Business Ethics (IBE), which provides toolkits, for example, on how to build an ethics framework. In this case, businesses might include as part of their ethics framework the potential ethical issues that may arise for their business based on the goods they make or services they offer, to whom they sell them to, as well the regulations that providers are answerable to. some of these regulations are detailed in this guidance.

If a business believes it meets the lender's criteria and is keen to pursue an application, it will need to ensure that it has the following documents ready and available:

- Information on ownership structure, financial viability, past and predicted performance of the business.
- A statement of how the business complies with the lender's policies and requirements, including a detailed explanation of how it mitigates risk.
- A statement demonstrating effective systems and controls that prevent and deter financial crime, bribery, and corruption.
- Businesses need to be aware that the greater the perceived risk to the financial provider, the more information and transparency they will likely request.

Additionally, providers will run enhanced money laundering and Know Your Customer checks (KYC) for businesses in the defence and security sectors, due to the specific risk factor in the Money Laundering Regulations 2017 and other associated risks of the industry, this may take longer and require more evidence.

Providers will also be subject to UK and international sanctions obligations, many of which are within jurisdictions that operate a strict liability environment under the financial aspect of the prohibitions, including the processing of any transactions.

Some UK focused lenders do not offer a foreign currency account for customers to hold funds in non-sterling currencies. There may also be restrictions on foreign payment products. Businesses should ensure that whichever provider they approach offers all the required products and services.

The defence and security sector, like all other businesses, should be prepared to share information about their companies with their financial service provider. The aim of transparency is to help financial institutions understand the patterns and trends of the businesses, as well as potential future requirements. This information is important to help identify and hopefully reduce the perceived risks.

WHAT PROVIDERS NEED TO CONSIDER

In the UK and internationally, all providers require businesses they work with to satisfy multiple criteria, ranging from criteria that 'applies to all' through to more specific scrutiny. Businesses and operations that are considered as higher risk for the providers will face additional scrutiny.

All providers will want to understand the ownership structure of a business, its financial viability and past and predicted performance. Given the additional societal and regulatory expectations and requirements of providers in relation to the defence and security sectors, there is more scrutiny. Relevant policies are set out below:

- **Understanding Reputational Risk**
- **Awareness of Anti-Money Laundering**
- **Know Your Customer Checks (KYC)**
- **Threats of Countering Terrorism Financing (CTF)**
- **Adherence to Sanctions legislation, both domestically and internationally**
- **Compliance with anti-bribery and corruption rules**
- **Environmental, Social and Governance (ESG) risk**

Understanding Reputational Risk

Financial institutions are subject to highly rigorous obligations and responsibilities regarding the services and products they provide. They are constantly under scrutiny when it comes to who or what they are providing finance for or against.

Providers apply high levels of due diligence when considering new customers and contracts in the defence and security and sectors because of the innate risk that some of the activity could, in some way, directly result in harm or conflict.

Awareness of Anti-Money Laundering

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) requires firms to identify money laundering and terrorist financing risks they may face and how they will mitigate against these risks. The consequence for Anti Money Laundering (AML) non-compliance includes substantial fines, possible prison time and the closure or suspension of business activities. Companies must have processes in place to run AML checks and produce records for auditors. Even if a business unintentionally facilitates money laundering, it is liable.

Typical characteristics of defence manufacturing and supply create specific AML risks that firms are obliged to assess and mitigate. The MLR 2017 explicitly references transactions relating to arms as a specific AML risk factor. There are additional geographic risk factors that may include major defence export markets.

Know Your Customer (KYC) checks

Know Your Customer (KYC) standards are designed to protect financial institutions against fraud, corruption, money laundering and terrorist financing. KYC involves actions to identify customers, understand the nature of customers' activities and determine that the source of funds is legitimate; and assess money laundering risks associated with the customer's activities. To tackle criminal activities that use the financial industry to launder money, governments across the globe have extended the scope and reach of their KYC policies, creating strong regulations with high penalties for breeches, which impact on every aspect of the global financial ecosystem.

The KYC process involves financial institutions asking customers to provide a range of information about their business operations and individuals associated with the business. This includes the names of the company's directors, addresses, trading activities and establishing the sources of revenue and capital. Identification, such as passports, will also be sought. This information is supplemented with publicly available information and checks are made against records of individuals and organisations that have been identified by law enforcement agencies such as the Financial Action Task Force lists (FATF).

After completing these KYC checks, a financial institution will decide whether they are willing to offer products or services to the business. In cases where the information gathered suggests that a greater level of scrutiny is needed, institutions may undertake enhanced due diligence (EDD). Higher risk factors include business involvement with a country that has been identified as having high levels of corruption, money laundering or terrorism financing, countries subject to sanctions, the involvement of politically exposed persons (PEPs) and the business being based in a country identified as not having adequate AML or counter-terrorism systems.

KYC checks are completed when entering into a new relationship with a business, such as opening an account, and on an ongoing basis. This means that financial institutions must contact their customers frequently to request KYC information.

Threats of Countering Terrorism Financing (CTF)

Terrorism financing is the act of providing financial support to terrorists or terrorist organisations to enable them to carry out terrorist acts or to benefit any terrorist or terrorist organisation.

While funds may come from criminal activities, they may also be derived from legitimate sources, for example, through salaries, revenue from legitimate business or donations including through non-profit organisations.

Similar to money laundering, there are generally three stages in terrorism financing: raising, moving, and using funds. Despite the different stages, the ways in which terrorism financing is done is similar and, in some cases, may be identical to the methods used to launder money. In both cases, the perpetrator seeks to misuse the financial or non-financial sectors for illegitimate purposes.

The UK Government expects providers and other firms subject to Money Laundering Regulations to play a robust role in managing and mitigating the risk of terrorism financing.

Terrorism is also subject to sanctions regimes. Terrorist sanctions are a thematic, behavioral measure and thus are not restricted by a jurisdiction. This global application makes them a constant check point, especially within the defence and dual use goods areas.

Adherence to Sanctions Legislation

The international sanctions compliance and enforcement landscape in which providers operate is changing rapidly. The growth of the use of sanctions continues to escalate as does the complexity of the types of sanctions being applied. Sanctions now play a greater role than ever before in foreign policy. Since 2000, US sanctions have increased over 1000% and along with the volumes, the complexity has also had an exponential increase. Russia is a recent example of the expansion of complexity, with trade-based sanctions accounting for >80% of all prohibitions. Financial services providers are liable for trade sanctions breaches if they facilitate the payment, despite not being close to the trades and lacking in specialist market knowledge.

The growing international reliance on sanctions as the 'go to' instrument of coercion, plus the increasing growth of retaliatory counter measures, will continue to shape financial service organisations' operating environment. In response to such divergent requirements, global banks have increasingly committed to complying with the sanctions laws and regulations of the UN, EU, and US as well as jurisdictions in which they operate. In this regard, banks set global sanction policies that define minimum standards for compliance across the group.

Because providers have a legal requirement to comply with all applicable sanctions, it will go against their global policy to undertake business that would not be permitted in other jurisdictions (e.g., the USA/EU) but would be permitted, or even encouraged, by the UK. This means that every lender's approach to sanctions risk will be influenced by a range of factors. For this reason, lenders' appetites to engage in certain activities or within jurisdictions, subject to some level of non-UK sanctions, may vary considerably. More information is available here.

Compliance with anti-bribery and corruption rules

All UK financial service organisations comply with the UK Bribery Act, which prohibits bribery and corruption. This law includes trading relationships and supply chains. Many providers will have a policy that sets out the key principles and minimum control requirements that mitigate against bribery and corruption risk and comply with all laws and regulations, including the UK Bribery Act and equivalent laws and regulation in other countries.

Policies include an expectation that customers will not use products and services to facilitate the payment or receipt of bribes or funds from corrupt activity. This includes customer due diligence, transaction monitoring and customer exit requirements. Publicly available corruption risk indices by the UN and civil society organisations and many commercially provided tools assess the defence and security sectors and many major defence export markets as inherently at higher risk of corruption.

Environmental, Social and Governance (ESG) risk

Many providers in the UK are building their reputation as purpose-driven banks, delivering ‘good’ outcomes for customers and having a positive impact on the environment and wider society.

Over time, there is likely to be increasing focus on ESG from customers, regulators, and other stakeholders, which means that this is of paramount importance to banks. Many providers also have clear policies to support delivery of social and governance goals.

Governments, institutional investors, customers, and NGOs agree that the financial sector has a role to play in mitigating these ethical, social, and environmental risks including those associated with the defence and security industry.

International Conventions have also identified certain weapons that cause, what they have determined to be unacceptable humanitarian harm, that violates a population´s fundamental human rights.

Examples of international frameworks and agreements are listed in Appendix B.

Annex A

Policies on the provision of services to defence and security sector businesses

It should be noted that policies on the provision of services to defence and security sector businesses operate alongside broader policies about the provision of finance and services to all businesses. This could include policies on the ownership structure, financial viability, and past and predicted performance. The policies listed below are ones that were readily available at the time of writing and available in open forum. Other policies from alternative institutions may be available on request.

Provider	Link to policy
Barclays	https://home.barclays/content/dam/home-barclays/documents/citizenship/our-reporting-and-policy-positions/policy-positions/Barclays-Statement-on-the-Defence-Sector.pdf
Co-operative Bank	https://www.co-operativebank.co.uk/values-and-ethics/
HSBC	https://www.hsbc.com/-/files/hsbc/our-approach/risk-and-responsibility/pdfs/221215-defence-equipment-sector-policy.pdf?download=1
Lloyds Banking Group	/www.lloydsbankinggroup.com/assets/pdfs/who-we-are/responsible-business/downloads/group-codes-and-policies/lbg-external-all-sector-statements-may-23.pdf
NatWest	https://www.natwestgroup.com/sustainability/downloads.html
Santander	https://www.santander.com/content/dam/santander-com/en/contenido-paginas/nuestro-compromiso/pol%C3%ADticas/do-Defence%20sector%20policy-en.pdf

Annex B

Financing for defence and security manufacture and supply is affected by a range of international frameworks and agreements, including:

The Convention on Certain Conventional Weapons which bans or restricts the use of specific types of weapons that are considered to cause unnecessary or unjustifiable suffering to combatants or to affect civilians indiscriminately.

The UN's Arms Trade Treaty which regulates the international trade in conventional arms – from small arms to battle tanks, combat aircraft and warships.

The Wassenaar Arrangement which contributes to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations.

The Equator Principles which are a financial industry benchmark for determining, assessing, and managing environmental and social risk in projects.

The 10 Principles of the UN Global Compact which requires signatories to commit to respect and promote universal human rights, implement decent work practices, reduce environmental impact, and ensure zero incidents of corruption within their own operations and spheres of influence.

Global Principles of Business Ethics for the aerospace and defence industry affirms the industry's commitment to ethical business behaviour and a uniform set of standards. The Global Principles address business conduct as it relates to zero tolerance of corruption, use of advisors, management of conflicts of interest and respect for proprietary information.

The UN's Guiding Principles for Business and Human Rights provides an authoritative global standard for preventing and addressing the risk of adverse human rights impacts linked to business activity.

The Principles for Responsible Investment, supported by the United Nations, encourages investors to use responsible investment to enhance returns and better manage risks.

The United Nation's Principles for Responsible Banking, aims to accelerate a positive global transition for people and the planet. Through the Principles, banks take action to align their core strategy, decision-making, lending and investment with the UN Sustainable Development Goals, and international agreements such as the Paris Climate Agreement.

The Task Force on Climate-Related Financial Disclosures, created by the Financial Stability Board (FSB), develops consistent climate-related financial risk disclosures for use by companies, banks, and investors in providing information to stakeholders.

It is generally acknowledged that weapons of certain types are necessary to support globally recognised aims such as peacekeeping activity and many providers are open to supporting UK businesses in the defence and security sectors. But providers do need robust reassurances and evidence that potential and existing customers comply with applicable international conventions, sanctions and embargoes, legislation, and licensing requirements whilst showing a clear commitment to robust Environmental, Social and Governance (ESG) standard and goals and risk management processes.





Aimie Stone
Chief Economist
ADS Group
T: +44 (0) 207 091 4532
Aimie.Stone@adsgroup.org.uk

ADS is the UK trade organisation representing the aerospace, defence, security, and space sectors.

ADSGroupUK
ADS Group Ltd
adsgroup.org.uk

Jennifer Tankard
Principal, Commerical Finance
UK Finance
T: +44 (0) 203 934 1487
Jennifer.Tankard@ukfinance.org.uk

UK Finance is the collective voice for the banking and finance industry. Representing more than 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

UKFtweets
UK Finance
ukfinance.org.uk