ADS Business Ethics Toolkit 2019

NOTE: ***This toolkit seeks to provide some introductory guidance for UK companies (whether operating domestically or internationally) based upon the understanding of ADS of the various elements of legislation and regulation in place at the date of publication of this toolkit. However, it must be recognised that both UK and international legislation on the issue of business ethics, particularly as the UK leaves the EU, may be subject to significant change and revision and that as a consequence any guidance provided herein must not be regarded as a substitute for legal or other professional advice for individual companies.***

Foreword

Paul Everitt

As a world-leading and key UK exporting industry, we must continue to promote, implement and strengthen good practices in business ethics. I am pleased that we are launching this totally revised edition of the ADS Business Ethics Toolkit which includes guidance on anti-bribery, human rights (specifically modern slavery), conflict minerals, the impact of the General Data Protection Regulations and competition law.

The UK has long been recognised as one of the least corrupt countries in the world and at both corporate and government levels has played a leading role in developing international standards on business ethics.

It is likely that ADS Members will continue to expand their export horizons and supply chains overseas. Some expansion will be in markets where business ethics are taken seriously and others where the risk of corruption, malpractices and human rights violations is higher.

All our efforts are framed within our domestic laws and regulations and those of the countries in which we operate. We must be ever mindful of the extra territorial reach of legislation including the UK Bribery Act and the US Foreign and Corrupt Practices Act, and the increasing reach of other country's legislation in respect of overseas subsidiaries and suppliers. Therefore, where there is an increasing worldwide effort to tackle bribery, corruption, enforced and child labour, a strongly embedded culture of ethical compliance will protect your business, its stakeholders, its employees and the reputation of our industry.

I want to thank everyone involved in developing this important work, and especially the Business Ethics Network and our colleagues at Interchange Solutions (who have assisted us enormously in producing this Toolkit). I commend this Toolkit to ADS Members, both small and larger companies, as a tool to ensure the long-term success of the UK aerospace, defence, security and space industries.

ABOUT ADS

ADS Group Ltd is the UK's premier trade organisation for all companies operating in the UK Aerospace, Defence, Security and Space sectors.

The industries represented by ADS are vital to the UK economy and are major drivers of growth and prosperity. The sector activities in ADS are aligned to the priority needs of its Members and where relevant brought to the attention of senior policy makers as set out in our priority objectives.

ADS undertakes to:

- Improve the image and profile of our sector
- Influence the most importance policy debates
- Support UK manufacturing and our sector's supply chains
- Encourage investment in technology and innovation
- Support business development opportunities nationally and in priority international markets
- Provide value to our Members

Further information on ADS is available at www.adsgroup.org.uk.

The **Business Ethics Network (BEN)** is an ADS' "Special Interest Group" which provides ethics-related advice and assistance to UK companies in the Aerospace, Defence and Security sectors. Its scope includes but is not limited to bribery and corruption, and corporate social responsibility, such as human rights, anti-slavery, conflict minerals, data protection, tax evasion, diversity and other areas relevant to our industry.

The Network has produced this latest edition of the "**Business Ethics Toolkit**" to offer guidance to organisations on how to introduce and implement procedures dealing with effective anti-bribery and corruption and other relevant policies.

Further information on the BEN is available at:

https://www.adsgroup.org.uk/membership/groups-committees/business-ethics-network/

Introduction

What do we mean when we talk about business ethics?

Put simply it's about doing the right thing.

A bit of background

Responsible business practice and evidence of compliance with legislation, regulation, codes of conduct and good ethical practices are required to meet the expectations of primes, customers, shareholders and other stakeholders, and are observed closely by civil society. Given an increasing number of criminal prosecutions under the UK Bribery Act and civil claims relating to overseas suppliers or subsidiaries (including those against SMEs), steps have been taken worldwide to develop codes of behaviour for companies and their supply chains. Many new legislative instruments apply not just domestically but have extra territorial reach, such as that embodied in the UK Bribery Act 2010, the Modern Slavery Act 2015 and the Criminal Finances Act 2017.

With regard to competition law, the consequences of breaching the applicable regulation can be severe both for companies and individuals, ranging from significant fines and reputational damage to the risk of criminal liability. A growing number of jurisdictions have wide-ranging powers and can pursue both companies and individuals for a breach of competition law.

How does this Toolkit help you?

It will provide practical guidance to help your company implement, improve and embed good business ethics policy, processes and practices into your corporate DNA; making your ethics compliance programme ***a part of and not apart from*** the business strategy; robustly securing commercial opportunities and gaining competitive advantage in existing and new markets.

Whilst there is considerable focus in the Toolkit on bribery which remains the most damaging business risk (especially in new and unfamiliar markets), this updated version is broader in scope, and incorporates other areas as set out below:-

The sections in this toolkit are:-

- Part 1 Case for business ethics
- Part 2 Bribery compliance and the law
- Part 3 Human rights, including modern slavery
- Part 4 Conflict minerals
- Part 5 Data protection and privacy
- Part 6 Export controls
- Part 7 Tax evasion
- Part 8 Competition law
- Part 9 Conclusion
- Part 10 References

Each section provides a summary of the risks to be addressed and offers guidance on how these risks can be prevented. Within each section there are hyperlinks to more detailed information and guidance.

As you move through this Toolkit, you will realise that much of the guidance on addressing bribery risk, such as a zero tolerance, risk assessment and due diligence, is equally applicable to other areas of business ethics.

Part 1 Case for business ethics

This section sets out the case for implementing a robust business ethics programme, the harm caused by failure, the benefits of a strong and embedded programme and how ADS is supporting its Membership.

1.1 A quick summary

- **Your customers, banks, insurers and regulators want assurance that you're doing business in the right way**
- **Newer markets can be prone to greater risk of things not being done in the right way e.g. corruption, human rights abuse, etc**
- **Demonstrating you're doing things in the right way can give you a competitive advantage – more countries are taking a positive attitude to business ethics**
- **Costs of getting this wrong are substantial compared with the investment in getting it right**
- **ADS, through the special interest group of Business Ethics Network (BEN), can offer support**

1.2 The detail

1.2.1 Why bother with Business Ethics?

The UK aerospace, defence, security and space industries have a global reputation for first-class manufacturing, quality, service and innovation, positioning the UK as a worldwide leader. The sectors' importance as major British exporters will continue to increase in the future.

Our industries, many involving world-leading technologies, support some 310,000 jobs across all regions of the UK. The combined revenue of over 2,000 companies in the sector is more than £50 billion. Aerospace is the UK's second fastest growing industry, second in its growth only to food and beverage exports. Aerospace exports are expected to grow by £796m a year.

The sustainability of these exports, and supporting the UK supply chain, is vital to the UK national economy and the jobs, including some 11,500 apprentices. As established markets shrink and sources of global supply open-up, there is considerable opportunity for companies of all sizes.

The greater risk of corruption and human rights abuse, particularly child and enforced labour in some markets is a business challenge for primes and smaller companies, alike. This has led to greater demand for vendors to provide evidence of their anti-bribery, data protection, human rights and conflict minerals compliance to buyers, be they public or private organisations.

It is no longer acceptable and potentially damaging for companies to justify unethical behaviour in believing *"that's the way of doing business in ……"* or *"it's the culture of that country"*

Smaller companies and their directors may not be able to withstand the fallout of defending a criminal allegation or prosecution, let alone suffer a criminal conviction and the huge costs.

1.2.1.1 What harm can the wrong behaviour do?

- Corruption and human rights abuses damage reputations be that corporates or individuals; it may cause the loss of customers, suppliers and adversely impact insurance, the market share price and financing facilities;
- Causes, contributes or links you or your products to an adverse human rights situation for which you will be responsible for providing remedies;
- Drives out competition and cultivates corrupt behaviour;

- May lead to unsafe products for customers, e.g. via counterfeit components or parts;
- Exposes companies to shareholder disputes and the directors to liability;
- Leads to criminal charges or civil claims against you, the company or your parent company;
- An investigation, let alone a prosecution, can destroy or seriously disrupt a business, adversely affecting the morale of employees, and taking out key people during an investigation;
- Ethical weaknesses are likely to open the door to criminal (including organised crime) and rogue state activity, such as the theft of sensitive IPR and confidential data, extortion and money laundering;
- Data theft may lead to loss of business, prosecution of the "victim company" and large fines on both the company and associated individuals for not taking sufficient steps to protect the data they control;
- Customers, primes, suppliers and lenders are less likely to take the risk of dealing with ethically weak or blatantly disreputable companies;
- If a company (corporate liability) and/or individuals are convicted, they could face unlimited fines, recovery of the proceeds of crime, barring from national and international tenders and contracts and, for individuals, imprisonment of up to 10 years.
- Turning a blind eye to enforced or child labour in a supply chain, (e.g. in the manufacture of components, low cost facilities management such as cleaners), may violate the Modern Slavery Act. Aside from human rights considerations, unethical behaviour may lead to adverse media coverage and damage to reputation.

1.2.1.2 What are the benefits of ethical behaviour?

- Underpins the integrity of the sector, an individual company, its employees, builds trust and confidence with internal and external stakeholders;
- Creates competitive advantage and is a business differentiator when working with primes and bidding directly for overseas contracts;
- Avoids harm to others;
- A risk-based approach enables companies to identify and better manage opportunities in those markets where the risks of corruption and human rights abuse are higher;
- Really knowing with whom companies are doing business helps them to drive more value out of the business partner channels (agents, advisers, distributors, etc.) and supply chain, while mitigating ethical risk and ensuring the supply of safe products to customers;
- Assures banks, export credit agencies and insurers that company is not engaged in criminal activity or has reputation damage (both may depress the share price);
- Employees, particularly those who are younger, are increasingly likely to be loyal to a "*clean/ethical*" business than a "*tarnished*" one;
- Investors and stakeholders are more confident when they have a high degree of certainty that there is unlikely to be any costly litigation due to bribing to win overseas contracts or using child labour;
- Many companies will need to broaden their supply chains outside the EU post-BREXIT. Mapping and understanding the elements of the supply chain and gaining suppliers' support for a company's business ethics programme, reduces the risk of unanticipated interruption;
- Incorporating business ethics into business strategy, making anti-bribery and human rights compliance **a part of – and not apart from** the operations of the company will drive beneficial changes in sales and market entry strategies, supplier acquisition, in mergers and acquisitions, and other business ventures.

1.2.3 Which laws govern Business Ethics?

There are a number of international conventions which establish the behaviour of signatory countries in the area of business ethics.

These conventions include:-

Organisation for Economic Development (OECD) Convention on Combating Bribery of Foreign Public Officials in International Business Transactions;
UN Convention against Corruption;
International Covenant on Civil and Political Rights;
European Convention on Human Rights
United Nations Guiding Principles on Business and Human Rights;
Voluntary Principles on Security and Human Rights; and
OECD Guidelines on Multinational Enterprises

Signatory countries to these conventions are increasingly legislating and introducing regulation governing the behaviour of companies and individuals.

Legislation and regulation will vary from country to country and is subject to amendment. It is therefore strongly recommended that companies seek specialist professional or legal advice if uncertain.

1.2.4 Are Business Ethics programmes costly?

Before you eschew doing anything, calculate the cost of doing nothing! The cost of implementing effective policies and business processes by embedding them into normal business practices is small compared with the legal, IT, accountancy, and personal costs, as well as those costs incurred by the disruption, management distraction and the potential loss of business. This is before the substantial fees in defending a criminal prosecution.

Part 2: Bribery compliance and the law

This section sets out in detail the UK law and guidance to companies on the Bribery Act 2010 and, information on the US Foreign and Corrupt Practices Act given that many companies may have a US association. The section includes bribery risks and relevant issues concerning third parties, especially intermediaries and offset. It concludes with anti-bribery tools and standards.

2.1 A quick summary

- ***Two main areas of legislation which you need to be aware of:***
  - ***UK Bribery Act 2010***
  - ***US Foreign and Corrupt Practices Act***
- ***Key elements of UK Bribery Act are:***
  - ***Bribing another person***
  - ***Being bribed***
  - ***Expectation test***
  - ***Bribery of a foreign public official***
  - ***Failure of a commercial organisation to prevent bribery***
  - ***Offences of bodies corporate***
- ***Getting it wrong can mean large fines and imprisonment for both individuals and the company***
- ***The UK Bribery Act and the Foreign Corrupt Practices Act don't just apply in the UK and US respectively, if a business performs any part of its operation in UK/ US, it's activities worldwide can be caught by the relevant act***
- ***There are other aspects of UK legislation of which you should also be aware***
- ***It's important to read the Ministry of Justice Guidance[1] since you must be able to demonstrate adequate procedures in any defence, and having an anti-bribery programme is an important part of this***
- ***It's not just money in a brown envelope anymore, bribery can take many forms, so keeping up-to-date with what is now happening is important***
- ***Offset is a mechanism used in government procurement that requires foreign supplying companies to reinvest in the economy of the purchasing country as a condition of undertaking a contract. There can sometimes be corruption risks associated with offset.***
- ***There are many other tools available to companies to help develop an anti-bribery programme***

2.2 The detail

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/181762/bribery-act-2010-guidance.pdf

2.2.1 United Kingdom Bribery Act 2010 (the "Bribery Act" or the "Act")

Key elements of the Bribery Act

The Bribery Act has been in force in England, Wales, Northern Ireland and Scotland since 1st July 2011. The key offences are (in summary): -

2.2.1.1 Section 1 - Bribing another person: To offer, promise or give a financial or other advantage to another to induce or reward a person for the improper performance of their function (regardless of whether such person personally performs the requested action or inaction) or knowing that acceptance of such advantage would be improper

➔ ***to offer or pay a bribe***.

2.2.1.2 Section 2 - Being bribed: To request, agree to receive or accept a financial or other advantage so as to be induced to perform or as a reward for performing a relevant function or activity improperly, where the request, agreement or acceptance is, itself, improper or improper performance in anticipation of securing such an advantage

➔ ***to request, solicit or receive a bribe***.

It does not matter whether the bribe is paid directly or through a third party (such as an advisor or agent). These offences also address so called "private bribery" that is between individuals of two companies/organisations and cover all forms of "one-to-one" bribery including individual employees, company officers, public officials, etc.

In simple terms, "improper performance" means behaviour which actively breaches a duty of good faith, impartiality or a position of trust whether in public office (which would cover a wide spectrum of public fields), business, employment or in connection with any collective body of companies or individuals.

2.2.1.3 Section 5 - Expectation Test: extract s5.

Some companies have an entrenched view that *bribery is the way business is done in certain countries – and, if we do not pay bribes, we will lose out to others who pay*.

Section 5 of the Act disregards this view/excuse and states that *"any local custom or practice is to be disregarded unless it is permitted or required by the written law applicable to the country or territory concerned"*. There are few, if any, countries that permit bribery under these circumstances and, therefore, a defence of **local custom and practice is highly unlikely to constitute a legal defence.**

2.2.1.4 Section 6 - Bribery of a foreign public official: To promise, offer or give a financial or other advantage to a foreign public official directly or through a third party with the intention of obtaining or retaining a business advantage in the conduct of business where such advantage is not legitimately due. There is no requirement for improper performance on the part of the official, just that they are not permitted to receive the advantage. Foreign public officials include:-

- Holders of legislative, administrative or judicial positions of any kind, whether appointed or elected of a country or territory outside the United Kingdom,
- Employees in a public agency or public enterprise (e.g. a state-owned company) and international organisations, (e.g. United Nations, NATO).

In many countries, key industries are owned by the government (e.g. state-owned enterprises) although they may appear to be a normal commercial concern. For example, the bribing of a manager of a foreign state-owned defence company would constitute an offence of bribing a foreign public official.

2.2.1.5 Section - 7 Failure of a commercial organisation to prevent bribery: A company or partnership would be guilty of this offence where a person associated with the company bribes another person (intending to obtain or retain a business advantage).

It is a legal defence for the company if it can evidence it has "adequate procedures" in place to prevent any associated persons from giving or receiving bribes on its behalf. An associated person could be anyone performing services on behalf of the company including agents, advisers, employees, etc. The Ministry of Justice Guidance (the "Guidance") to the Act provides guidance as to what procedures a company might adopt to prevent bribery. However, the simple adoption of a policy in line with the guidance does not guarantee a safe harbour from prosecution (this is discussed further in the Guidance section).

2.2.1.6 Section – 14 Offences by bodies corporate: If an offence under section 1, 2 or 6 is proved to have been committed with the consent or connivance of a senior officer or a person of the company or partnership, they as well as the company are guilty of the offence and liable to prosecution. This offence addresses the actions of company directors, managers and others who might be categorised as a "director" or "senior person" or, if in relation to a Scottish partnership, a partner in that partnership.

Important considerations: -

2.2.1.7 Section - 11 Penalties: An individual, depending on which offences he/she has committed, could be liable for penalties of imprisonment up to 10 years, a fine, or both. A company convicted under Section 7 may be fined and subject to further penalties under the Proceeds of Crime Act 2002 which could include recovery of any dividends paid to shareholders. Consequential penalties may include sanctions. Convicted company directors are likely to be disqualified.

2.2.1.8 Section - 12 Territorial Application: The Act applies to all activities which take place in the UK. It also has extra-territorial reach. If an offence is committed outside of the UK, but the individual involved qualifies under one of the varying degrees of UK citizenship set out in the Act or is ordinarily resident in the UK (be they UK citizens or foreign nationals), such an individual may be prosecuted.

An offence is committed under Section 7, irrespective of whether it took place in the UK or overseas, as long as the company carries on business, or a part of its business, in the UK.

"The UK Bribery Act 2010 has global reach. Strict anti-bribery laws apply both in the UK and when you travel overseas. The Act is applicable to:

- ***UK Nationals***
- ***Foreign Nationals resident in the UK***
- ***UK Companies***
- ***Foreign companies doing business in the UK"***

www.nationalcrimeagency.gov.uk/bribery

2.2.1 UK Bribery Act 2010 – Further detail

Further detail on the UK Bribery Act can be found in the Appendix A and the Ministry of Justice Guidance is at : - http://www.justice.gov.uk/downloads/legislation/bribery-

act-2010-guidance.pdf

2.2.2 Other relevant UK legislation & regulation

Includes:

- The Civil Service Code of Conduct (Duty to disclose)
- Theft Act 1968 (false accounting)
- Company Directors Disqualification Act 1986
- Proceeds of Crime Act 2002
- Fraud Act 2006
- Companies Act 2006
- Modern Slavery Act 2015
- Criminal Finance Act 2017
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

Note - where there is weak bribery and corruption prevention within an organisation, other crimes, such as money laundering, fraud and cybercrime (including data and intellectual property theft - both criminal and a third state) may also occur. All of these are increasingly likely to have unseen connections to organised crime and, worse still, terrorism.

Bribery and other unethical behaviour can develop from within any part of a company. Most bribery cases prosecuted to date have involved a third-party intermediary such as sales advisors, agents, consultants or distributors.

Companies engaging in offset arrangements should proceed with care and apply their risk management principles from the outset, in the same manner as they would in other projects/parts of their business. This approach should also be adopted in mergers or acquisitions, with particular attention paid to the integrity of key individuals and, especially, identifying the ultimate beneficial owner(s), during the commercial due diligence processes.

2.2.3 United States Foreign Corrupt Practices Act 1977 (FCPA)

The US Foreign Corrupt Practices Act 1977 (FCPA) is particularly significant. It has extra-territorial reach for non-US companies doing business in the USA and/or with US subsidiaries. In certain circumstances, the US may seek extradition of UK nationals (under the UK's Extradition Act 2003) and/or a company's third-party representatives - to stand trial in the USA.

Contrary to the UK Bribery Act, the FCPA contains an explicit exception to the bribery prohibition for "facilitating payments" for "routine governmental action" and provides "affirmative defenses" which can be used to defend against alleged violations of the FCPA. The statute lists examples, such as:

- Obtaining permits, licenses, or other official documents;
- Processing governmental papers;
- Visas and work orders;
- Providing police protection;
- Mail pick-up and delivery;
- Provision of phone service, power and water supply,
- Loading and unloading cargo;

- Protecting perishable products;
- Scheduling inspections associated with contract performance or transit of goods across country.

However, as evidenced in the 2010 US conviction of the Swiss freight forwarder Panalpina, the regular use of facilitation payments cannot be assumed to be free from the risk of potential prosecution under the FCPA (see http://www.justice.gov/opa/pr/oil-services-companies-and-freight-forwarding-company-agree-resolve-foreign-bribery)

Bribing of a foreign public official on a larger scale ("grand" bribery) to secure a contract is likely to be prosecuted under the FCPA, if the US can establish its jurisdiction. Companies need to be mindful that any improper electronic communication from outside the USA to/from US companies, subsidiaries or individuals may be intercepted under the FISA Amendments Act of 2008, thereby providing incriminating evidence for a criminal indictment. Other areas to be mindful of are overseas financial transactions involving US dollars or other clearly territorial acts such as meetings on US soil, use of US e-mail servers or the US Mail. The domestic bribery of a United States public official would generally be prosecuted under the Anti-Kickback Act of 1986.

2.3 Guidance to consider when creating an Anti-Bribery programme

Section 7 of the Bribery Act is an offence of a commercial organisation ("company") failing to prevent bribery for which the key defence is evidencing "adequate procedures" to prevent bribery. As currently set out in the Bribery Act, a Section 7 offence is one of strict liability where in practical terms the defendant [company], not the prosecution, is obliged to satisfy the prosecuting authority or, ultimately, the jury in court, that it had "adequate procedures" in place to prevent bribery.

Guidance to the Act was published by the Ministry of Justice to help companies ensure compliance with the Act. It is business-oriented and practical, but it does need to be interpreted, adapted and implemented to suit an individual company, its sector, business activities and markets.

An underlying theme in the Guidance, is bribery risk assessment, i.e. taking a "risk-based" approach to diligently assess bribery risk and managing the potential of bribery in an informed way, proportional to the likely risk. Ordinarily this can be included in the company's risk register and regularly reviewed by senior management/the board.

The Guidance promotes six principles that companies should consider when creating their anti-bribery programmes. However, be mindful they are *principles* and **not** *rules or regulations*, and, therefore, complying with such principles will not automatically guarantee that the UK prosecuting authorities[2] will decide that the defendant [company] had, in good faith and reasonable belief, embraced and instituted "adequate procedures".

Firms authorised by the Financial Services Conduct Authority (FCA), are required to put "adequate procedures" in place to prevent bribery. The FCA does not enforce the Bribery Act 2010 but will act where authorised firms fail to address corruption and bribery risk, including where those risks arise from intermediaries acting on their behalf. The FCA does not need to obtain evidence of corrupt conduct to take regulatory action against a firm, simply the absence of "adequate procedures" within their compliance regime.

Guidance from the SFO and Director of Public Prosecutions makes it clear that the

[2] Crown Prosecution Service, Her Majesty's Revenue and Customs and the Serious Fraud Office.

existence (or not) of "adequate procedures" will be a key factor in the decision to prosecute a company under Section 7 of the Act. The six principles set out in the Guidance are:

2.3.1 Principle 1 - Proportionate Procedures

"A commercial organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation's activities. They are also clear, practical, accessible, effectively implemented and enforced."

Key points:

- Develop bribery prevention policies and procedures which articulate that the company's anti-bribery stance and disclosure mechanism (whistleblowing) are implemented throughout the organisation;
- They should be proportionate to the risks faced, not just the size of the company, and attention should be paid to operating in high risk of corruption environments or where business associates and other third parties are employed to act on behalf of the organisation;
- The procedures should include the selection, appointment, contracting and managing of business associates (e.g. sales agents, advisers, distributors, other intermediaries[3]) and be effectively communicated to them;
- Policies and procedures should cover all areas of risk where perceptions of or actual bribery may occur. These should include, but are not limited to, gifts, hospitality, entertainment, sponsorship, promotional expenditure, political and charitable donations, facilitation payments, separation of duties and conflicts of interest;
- How the policies and procedures are to be implemented, and communicated including to associated persons (e.g. employees, suppliers, contractors, business associates, etc.);
- Reporting, whistleblowing and sanctions for wrongful behaviour by an employee.

2.3.2 Principle 2 – Top-level Commitment

"The top-level management of a commercial organisation (be it a board of directors, the partners, the owners or any other equivalent body or person) are committed to preventing bribery by persons associated with it. They foster a culture within the organisation in which bribery is never acceptable."

Key points:

- The purpose of this principle is to encourage the top-level management to be involved in the determination of bribery prevention procedures; and
- To ensure top level involvement in any key decision-making relating to bribery risk, where appropriate for the organisation's management structure;
- To lead the culture change ("*tone from the top*") through internal and external communication of their commitment to their zero tolerance of bribery;
- Engagement with relevant associated persons, trade bodies and the media, to articulate the organisation's policies;
- To review the processes on a regular basis and be informed of any bribery-related incidents.

[3] More than 80% of UK/US bribery prosecutions to date have involved a company's third-party intermediary, such as a local sales agent or similar intermediary.

2.3.3 Principle 3 - Risk Assessment

"The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented"

Key points:

- Anti-bribery and any other ethics risk assessment (e.g. modern slavery) should be conducted under the umbrella of the normal risk assessment processes of the company. The approach should be proportionate, according to the nature of the business, its scale and markets;
- Commonly encountered external risks can be categorised into country, sector, specific transactions, projects (including JVs, M&A and Offset), business opportunity and business partnership risks. Internal structures and procedures may either compound or mitigate the level of bribery risk, especially in the areas of employee training and skills, the bonus culture, lack of clarity and implementation of relevant policies and financial controls;
- Risk assessment should be a continuous process which is fully documented and regularly reviewed by the top management (including the board of directors);
- Supported by a clear anti-bribery message from top-level management.

2.3.4 Principle 4 – Due Diligence

"The commercial organisation applies due diligence procedures, taking a proportionate and risk-based approach, in respect of persons (both individuals and companies) who perform or will perform services for or on behalf of the organisation in order to mitigate identified bribery risks."

Key points:

- Really know with whom you are doing business or associating with and properly understand their business activities and key people. This should include, but is not limited to customers, suppliers, sales advisers, agents, brokers and consultants;
- Use a risk-based approach, proportionate to the perceived nature of the risk, market, etc. Useful tools to provide indicators of corruption levels may be the annual Transparency International Perceptions of Corruption Index or the Business Anti-Corruption Portal, amongst others;
- Where more than a low risk of bribery is assessed, more information may be required through an enhanced due diligence process on both the company(s) and individuals involved;
- Due diligence can be undertaken internally or externally, dependent on the perception of the level of risk;
- It is important to confirm the legal registration of the third party, identify the Ultimate Beneficial Owner(s) (UBO) and the shareholders of a potential business partner. This may be required by banks under anti-money laundering rules in some jurisdictions;
- A company's employees, agents and subsidiaries are presumed to be "associated persons" for the purposes of the Bribery Act;
- Where local law mandates the use of agents or similar, be aware that the nature of that potential relationship assumes even greater importance. Exiting such a relationship may be very difficult and costly.

2.3.5 Principle 5 – Communication (including training)

"The commercial organisation seeks to ensure that its bribery prevention policies and

procedures are embedded and understood throughout the organisation through internal and external communication, including training that is proportional to the risks it faces"

Key Points:

- Must clearly convey the "tone from the top";
- The purpose is to increase the awareness of everyone associated with the company; it informs of the policy, procedures, how to recognise bribery and what to do in the event of a bribery incident and how to report;
- It must clearly articulate the anti-bribery stance to both internal and external "associated persons" and other relevant stakeholders;
- Training provides the knowledge to identify and address bribery situations;
- Communicating the message will differ according to language, the nature and geographic spread of the company;
- Training may be face-to-face and/or using web-based e-learning tools and should include scenarios and tests;
- A record should be kept of all those who have undertaken training. The training should be refreshed to keep it relevant and those at particular risk should undergo more frequent training;
- It is especially important to explain the speak-up/disclosure ("whistleblowing") procedures.

2.3.6 Principle 6 – Monitoring and Review

"The commercial organisation monitors, and reviews procedures designed to prevent bribery by persons associated with it and makes improvements, where necessary"

Key Points:

- The bribery risks may change, or breaches of policy occur - therefore, the procedures need to be updated and amended, accordingly;
- Monitoring and review are necessary, as circumstances might change in markets (e.g. the law); the nature of risk may also change depending on the commercial landscape, such as new business/customers/suppliers, geographical expansion, etc;
- Provide periodic reviews and reports to top management (and the board);
- Set out clear procedures for the reporting and actions to be taken in the event of a suspected bribery incident;
- Staying abreast of best practices and advice, for example from trade organisations;
- Consider external verification or assurance of the effectiveness of anti-bribery procedures (e.g. ISO: 37001:2016 anti-bribery management system).

2.4 Bribery risks

This section sets out some specific risks and indicators of bribery. Bribery is a serious criminal offence and may be associated with other crimes such as theft, fraud, money laundering and tax evasion, any or all of which may compound the offence. Worse still, the act of bribery may have the unintended consequences of aiding organised crime, the funding of extremism/terrorism or an unwelcome interaction with foreign state players.

2.4.1 How can a bribe be contrived or concealed?

Whilst many perceive bribery to be a primarily sales-initiated offence it may also arise in procurement and contracting or the connivance or involvement of the senior management of a company; especially if there is a long-standing senior management personal relationship with a particular customer/supplier.

Bribes may be contrived or concealed in imaginative ways, beyond the offering and receiving of a "brown envelope" or an expensive gift. Some examples are: -

- Overstated bills of quantity (e.g. "*deliver five loads and invoice for six*" - common in the construction industry) or the supply of consultancy services (often difficult to quantify exactly what was delivered);
- Collusion between vendor and buyer in over-invoicing services and labour such that the excess amount can be skimmed off and shared by the criminally colluding parties;
- Overcharging for raw materials and commodities; skimming off the additional amounts;
- Financially engineering surpluses on sales agency/adviser commission ledgers then transferring surpluses to less visible accounts for payment of bribes through commissions ("slush funds");
- Transferring overstated commission provisions (where not required) for one agent/adviser to increase the commission level on another to finance a bribe;
- Rental of property or other services from a government official or his/her closely-related parties/company at above market rates to conceal illicit payments;
- Payments/arrangements through wholly unconnected agencies, professional advisors (including "facilitating professionals" - lawyers and accountants), travel agents, bogus charities, etc. Illicit funds may be layered and laundered through several offshore accounts;
- Payment into the foreign and/or personal bank accounts of officials or persons connected to them;
- Hiring the relatives of government officials in return for favouring that particular supplier;
- The provision of "personal services" – questionable recreational activities, including drugs, educational fees and gifts or holidays; and
- Trading confidential information from government officials or third parties relating to tendering process in exchange for consultancy fees.

2.4.2 Director/employee risk

Dishonest actors typically have one or more of the following attributes, prior to committing an offence:

Opportunity to engage in and gain from bribery, corruption, fraud or other unethical behaviour, for example:

- Being in a position of authority/power to take advantage for personal gain, while overruling others, – often manifested by bullying/patronising/connivance;
- Ineffective or non-existent company compliance regime and/or inadequate checks and balances open to exploitation and/or an ineffective internal audit function;
- Regular (uninhibited) access to accounts, cash, computer systems and sensitive information, through weak segregation of duties, oversight and internal controls;

- Too long in same job, well respected – does not take holidays – covers for others, therefore has "trusted and uninhibited access";
- Unhealthy/secretive personal business relationship with influential Politically Exposed Persons (PEPs) and customer decision makers;
- In "the right place at the right time", working as temporary staff or extorted/bribed by external parties to obtain information, IP etc.);
- Weak controls easily overridden or bypassed; individual limits of financial authorisation unreasonably high; poor financial and governance oversight leading to expense claim fraud and concealing bribes; lazy, inefficient, subservient, internal auditing;
- Exploiting a conflict of interest – e.g. a company's buyer has an undisclosed interest/benefit in a supplier company – or a sales employee having an undisclosed financial or other interest in a company's distributor/sales agent.

Motive, which drives their actions, such as:

- Financial pressures; at home, high lifestyle demands (including gambling), internal company issues - not "*making their numbers*", bonus-driven;
- The risk of being caught bribing for a contract, perceived less than the material gain from a bonus/incentive or share-price increase/dividend;
- Individual feels under-rewarded, therefore illicit gains seen as a justifiable "perk" or "payback";
- Personal reasons, a grudge or feeling undervalued/resentful against a manager, director or the company itself;
- Professional, peer and family pressure; need to be seen to succeed;
- Individual engineers illicit reward from a deal, e.g. splitting the commission with a sales agent, a supplier kickback – believing they "*will not be caught*".

Rationale or personal justification:

- "*Everyone else is at it and would do the same in my situation*";
- "*Not likely to be found out*";
- "*I can justify my actions if caught*" - crime blamed on company culture and/or a lack of direction or policy;
- "*I work all hours*" - "*have to travel to risky places*" - "*I'm entitled to take some additional compensation*";
- "*I needed a short-term financial fix – I will pay it back*".

Through following instructions, naivety, or being "*groomed*" an otherwise honest person can become complicit in corrupt or fraudulent activities. A personal moral test under these circumstances might be "*would I do this normally*?" - "*what would my family and colleagues think if my actions were published in a newspaper?*" or "*what would this look like all over Twitter, Facebook or Instagram?*".

2.4.3 Bribery and extortion risk

Many companies do little to prepare their employees for the risk of being extorted. Whilst the most likely area is a demand for a facilitation payment from an errant customs/police officer or a local government official, both employees and companies can become victims of being extorted to pay a bribe through: -

- *Not properly knowing their customers, intermediaries, suppliers or business partners, especially when outsourcing manufacturing to some foreign countries;*

Practical steps – Conduct a thorough risk assessment, obtain full written details and supporting information (e.g. company registration, etc) during the onboarding process for all third parties which can be verified through a due diligence process. Visit, check veracity with UK embassy, seek business references, etc.

- *Being duped into donations (passing a bribe) to dubious causes;* **Practical steps –** Is the donation aligned to the company's charitable giving policy and not at the time of a contract or seemingly gaining a similar advantage? Do due diligence on the organisation, individuals, their cause, etc, to ensure it is legitimate.
- *Flattered by association with powerful business introducers or government "sponsors";* **Practical steps –** Step back and assess genuine value of the relationship(s) and be realistic as to whether this is a route that will lead to their soliciting a bribe – most likely through a third party.
- *Personal risk engendered through compromising relationships and inappropriate recreational activities;*

  Practical steps – in connection with your business, curtail any personal traits which might lead to unintentional publicity or extortion of an individual. Company has clear rules and training to alert all at risk individuals. (e.g. sales persons who may travel alone)
- *Conceding to threats (perhaps about their personal lifestyle) and making payment to prevent an IT denial of services/ransomware attack (e.g. on a company's website);*

  Practical steps – Company has rules, training of employees and contingency plans to alert, educate and act to mitigate the risks both IT and extortion.
- *Requests are made for an unusual or extraordinarily high tax payment on a contract;*

  Practical steps – Seek advice from competent local [tax] lawyers, report to the senior level of the company and, if the situation is clearly the extorting of a bribe, inform the UK Embassy/High Commission so they can create a case for collective action if similar demands have been made to other companies.

2.4.4 Third party risk

While the commercial benefits of business associates are well recognised as an effective means of developing, expanding and maintaining a company's business, all sales agents, advisers, consultants and distributors, when performing services on behalf of a company, are "**associated persons**" in the context of Section 8 of the UK Bribery Act.

Without an appropriate level of pre-appointment risk assessment and due diligence, these associates may create considerable harm to a company's reputation and trigger judicial proceedings, even if the company is totally unaware of any impropriety.

As set out in the Guidance to the Bribery Act, in this Toolkit, there are a number of key steps where the risk of the engagement of third parties might be assessed and mitigated; the key areas are: -

2.4.4.1 Third Party Risk Assessment – areas to consider

- What is the business purpose of appointing the potential third party?
- Is this potential appointment aligned with the "go to market strategy"?
- What expertise do they have to support the company?
- What value will they add to the bottom line? and

- At what ongoing cost?

To inform the risk assessment, many companies have a formal application form which requests key information on the third party, including their legal status, identification of the ultimate beneficial owner(s), capabilities and market strengths. Other important considerations in the risk assessment would include the risks in the country itself, especially the levels of potential corruption.

2.4.4.2 Third party due diligence

- An appropriate level of due diligence should be conducted where there is more than a low risk of bribery.
- Given greater access to information, the level of due diligence for a third party only working in the UK, may be lower than that required in a highly corrupt country.
- Conduct due diligence before offering/concluding any agreement or dealing in any way with them (be that verbal or on paper), and certainly before their engagement in any sale or tender.
- Use all available information, sources and records to assess their business and personal standing including but not limited to their company, ethics culture (policies, processes, certifications, (e.g. ISO37001, etc.) technical, financial, market background and of the key individuals' personal histories (e.g. from LinkedIn, Facebook, etc).
- Ascertain their knowledge of the principal's company environment and products.
- Obtain details of Company registration, share ownership (particularly of the 'Ultimate Beneficial Owner') and any past or ongoing allegations/court cases.
- Periodically refresh the due diligence e.g. at the time of a major tender, a large commission payment or the renewal of an agreement.
- If the third party is an individual, the due diligence should be modified accordingly, seeking out any untoward associations or adverse history.
- A simple Google or credit rating agency report will not suffice!

The risk assessment, due diligence and the authorisation process, to appoint or otherwise, should be fully documented and compliant with the company's table of authorisations. All records should be kept including those relating to payments and in accordance with the company's data retention policy.

Note: *Be mindful of GDPR* - the third party must provide affirmative consent for any due diligence and, where applicable, a copy of the appointing company's privacy policy should be provided to them.

2.4.4.3 Third party contracts and legal provisions

A simple letter of representation is often used to appoint but can store up commercial, legal and bribery risks for the future, leaving the principal company open to having not contractually managed the relationship properly. After due process, a legal agreement should be concluded between the principal and the third party.

The third party should be made aware of and sign up to (i) the anti-bribery policies of the company, (ii) the Bribery Act 2010 and Foreign and Corrupt Practices Act, and (iii) all relevant directives, legislation or regulations in place in any country in which the third party will operate in conjunction with its obligations under the contract. The third party should contractually agree that:

- No part of any payment originating from the principal's company will be promised or paid as a bribe,

- They will not use their own funds or advantages at their disposal to make a bribe.

- They will not receive or solicit any bribes and accepts that any material breach would lead to immediate termination of the agreement.

The agreement should also incorporate, where appropriate, sales targets/business objectives (the bona fide commercial justification for the appointment) and a process for regular reporting to the company on the accomplishment of those targets, tasks and duties.

The compensation offered to the third party should be clearly set, commensurate with the level of work to be undertaken, and not subject to alteration. There should be a right to terminate for convenience in favour of the company and the contract should not have an unduly long term (allowing for a refresh of due diligence, commercial terms), ideally not exceeding every two years.

2.4.4.4 Third party remuneration

Whether the remuneration is a fee, commission, discount against volume of product sold, etc., it should be pitched at an appropriate level for the rendering of legitimate services on behalf of the company and in line with the company's accepted market practice.

Percentage-based commissions are common but often agreed with little consideration of the gross monetary sum that might be paid out against success. Potential third parties may also try to persuade the company "*that x% commission is the going rate in my country…*"; any company receiving such persuasion should independently verify such a claim and stick to its guns!

Where the payment mechanism is not thought through and if remuneration is clearly not commensurate with the level of services rendered, this leaves the company open to the risks of illicit payments and the possibility of bribery allegations.

Payments should always be made to a bank (save exceptional and documented circumstances) in the country where the third party is active, or their business is registered. All payments must be properly recorded in the company's books and records.

Remuneration paid offshore from third party's domicile, provide latitude for the transfer of funds for illicit purposes and may also create an offence of tax violation. Whichever form or method is used for payment, it should be based on the most objective elements possible and withstand enforcement or forensic scrutiny.

2.5 Offset

While there is no universal definition of "offset", this is broadly understood to be a mechanism used in government procurement that requires the foreign supplying companies to reinvest in the economy of the purchasing country as a condition of undertaking a defence contract awarded by that country's government. They are frequently used as industrial (sometimes even economic or social) policy tools and can take different forms; for example, requiring companies to transfer technology/know-how, provide education and training, provide investment, develop infrastructure and facilities, subcontract work or licence production. The scale of offset obligations varies from country to country but is typically expressed as a percentage of the value of the main contract.

Offset is often categorised as “direct” and “indirect”. The definition of these categories varies from country to country, but, in general, companies refer to “direct” offsets as being directly related to the subject of the defence acquisition or the products that they make; “indirect offsets” are likely to be something unrelated, such as the building of a road or school, etc.

The approaches to offset vary from country to country regarding, in particular, the choice between direct or indirect offset and the amount (percentage of the total offset package) of direct offset that a country requires. It is important to note that the offset value is denominated not in actual currency but in offset credits. Multipliers can also be used to reflect the degree of importance assigned by the purchasing government to the offset project and can refer to the potential impact of the offsets in the purchasing country or even be unrelated to any type of economic indicator.

An example might be a country’s procurement of a fleet of aircraft from a foreign contractor in relation to which an offset obligation is placed on the contractor. The offset authority of the purchasing country may agree that offset credits may be awarded to the contractor in order to satisfy the obligation if it sets up local production/assembly under license.

2.5.1 Offset risks

Offset transactions carry potential risks of corruption which will vary depending on the country, the nature and value of the project being proposed and the identity of any local industrial partners, as well as the overall transparency of their offset regulations and their implementation. It is important that such risks are identified in the risk assessment and due diligence processes and mitigated before setting up and establishing an offset project.

2.5.2 Offset risk mitigation

To identify and mitigate potential risks, companies subject to an offset obligation should carry out a project risk assessment covering all aspects of the potential project and due diligence on those participating companies/individuals. The purposes are to understand:

- There is a legitimate business case for the proposed project;
- The nature of those parties involved in the project particularly the involvement of any local business associates and other partners;

- Through the due diligence process the ownership structure, and beneficial interests of all involved parties/the entity;
- And identify any potential conflicts of interest; and
- Whether the proposed offset deal complies with the legislation in all the relevant jurisdictions.

2.6 Anti-bribery standards and tools

Information on available anti-bribery standards and tools can be found in Appendix B.

Part 3: Human Rights and Modern Slavery

This section sets out the importance of human rights in the context of the company and the conduct of business and covers the conventions and the UK law – the Modern Slavery Act 2015. It also provides guidance both on the Act, the indicators of modern slavery and the steps that can be taken to identify and mitigate the risks.

3.1 A quick summary

- ***Universal Declaration of Human Rights adopted by the UN in 1948 states the basic rights and freedoms that all human beings are entitled to***
- ***There are five articles in the Declaration:***
    - ***Right to equality***
    - ***Right to life, liberty and personal security***
    - ***Freedom from slavery***
    - ***Freedom from torture and degrading treatment***
    - ***Right to recognition as a person before the law***
- ***Companies have a responsibility to respect human rights and should have such a policy as an integral part of their Code of Ethics or similar.***
- ***Human rights are taken into consideration in the granting of export licences to certain countries by many nations***
- ***Need awareness of the UK Modern Slavery Act 2015 that criminalises the employment by anyone or any organisation of enslaved workers in the UK***
- ***If your company has an annual turnover of £36 million or above, you must prepare a slavery and human trafficking statement for each financial year***
- ***It's important that relevant members of staff are aware of signs of slavery as it can take many forms***

3.2 The Detail

3.2.1 Background

Respect for human rights at home and in overseas operations has long been established through international conventions and through legislation in the UK and other countries. This respect should be embedded into an organisation's DNA as a part of doing business at home or overseas.

3.2.2 UK Human Rights Act 1998

The UK Human Rights Act 1998 sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic British law. The Human Rights Act came into force in the UK in October 2000 and enshrines the Universal Declaration of Human Rights. The most relevant parts of the Act are: -

- Article 6, (right to fair trial)
- Article 4, (prohibition of slavery or forced labour)
- Article 8, (right to privacy)
- Article 9, (freedom of thought, conscience and religion)
- Article 10, (freedom of expression)
- Article 11, (right to freedom of association, including joining a trade union)
- Article 14, (prohibition of discrimination)

Companies have a responsibility to respect human rights and should have such a policy as

an integral part of their Code of Ethics or similar. The human rights policies and practices should be cascaded down to include their supply chain and in their interaction with local authorities, especially security authorities, and to audit their effectiveness. Many companies now include Human Rights Impact Assessments as part of their core policy for operating in any country in order to prevent, mitigate and, where necessary, remedy any adverse human rights impact.

Abuse of human rights can range from modern slavery (see 3.2.4) to failing to take account of the impact on local communities and local culture. Incidents may occur internally such as harassment, bullying (e.g. of juniors by more senior personnel), integrating and managing those of different ethnicity or predilections and the disabled, always in the context of local culture and law. (Note: Homosexuality is illegal in some countries and, for instance, freedom of expression is highly qualified).

3.2.3 UN Guiding Principles on Business and Human Rights

UN Guiding Principles on Business and Human Rights ("Protect, respect and remedy") were adopted in 2011 and provide companies with a reporting framework to demonstrate how they are giving effect to human rights requirements, whether legal obligations or voluntary codes. Such reports are increasingly required whether by stakeholders - clients, shareholders and civil society - or in legislation. This is a voluntary framework and should be considered alongside other industry initiatives, that set best practice standards for responsible business such as the OECD guidelines.

The on-going migrant crisis around the World, linked to the plethora of shocking media exposés of labour issues in global supply chains, has heightened public attention to modern slavery, forced labour and human trafficking. Children working in cobalt mines for the Apple and Samsung supply chains; NHS rubber gloves being made in factories in Malaysia by exploited immigrant workers; Syrian refugees working under terrible circumstances for garment supply chains in Turkey; Rohingya refugees working as slaves in the Thai fishing industry; and North African migrants working in agriculture in Italy and Spain. These are just some of the very many stories which reveal the extent of the current global problem. But it is not just overseas where these things happen, and similar allegations have been made here in the UK involving: cleaning staff; nail bar staff; car washing staff; agricultural workers, and others.

3.2.3 OECD Guidelines for Multinationals on Responsible Business Conduct

The OECD Guidelines for Multinationals on Responsible Business Conduct contain recommendations for companies, on how they should carry out effective supply chain due diligence to address this matter. Whilst the OECD Guidelines are non-binding, they are accompanied by a unique grievance mechanism, the National Contact Points (NCPs). NCPs in the 46 countries that adhere to the guidelines facilitate dialogue and mediation with companies that allegedly do not observe their recommendations.

Governments are increasingly seeking to promote more effective due diligence in global supply chains and civil society and the media continue to be instrumental in exposing human rights issues.

All companies are under increasing pressure to be seen to conduct effective due diligence to ensure that they are not linked to forced labour in their supply chains, particularly that existing in large migrant populations.

3.2.4 Modern Slavery Act 2015

The UK Modern Slavery Act 2015 criminalises the employment of enslaved workers by anyone or any organisation in the UK. Human Trafficking is a form of Modern Slavery and is the movement of people by means of force, fraud, coercion or deception, with the aim of exploiting them or their families through debt bondage.

The International Labour Organisation (ILO) estimated that in 2018 there were 40.3 million victims of modern slavery worldwide, some 71% of whom are female, with 24.9 million in forced labour including an estimated 10 million children, some of whom are exploited in the sex industry. Those enslaved may also have been trafficked by organised criminal gangs and find themselves in bonded labour where their families are extorted for payment too.

While the aerospace, defence and security industries operate in a highly regulated and mostly high-tech sector, high risks still prevail in areas such as forced and child labour in the mining of key/conflict minerals (e.g. lithium, cobalt, tantalum etc) or in the manufacture of components and military clothing, especially in SE Asia and Asia Pacific.

Closer to home this could include workers in lower paid and "*hidden*" jobs such as drivers, in warehousing, construction, maintenance, catering and cleaning. It is, therefore, not beyond the bounds of possibility that a company may unknowingly encounter modern slavery within its own operations and face reputation risk.

3.2.4 Modern Slavery Act 2015 – Reporting Obligations

Under the Act, part 6 s.54 - Commercial Organisations, it states they *"must prepare a slavery and human trafficking statement for each financial year of the organisation"* if the organisation is providing goods and services in the UK and, has an annual turnover (of the entity and its subsidiaries) of £36 million or more. However, companies are entitled not to provide a statement and can still be compliant provided they set out the reasons for not publishing one.

The Statement must set out –

- Steps the organisation has taken during the financial year to ensure that Slavery and Human Trafficking is not taking place in:
    - any of its supply chains and;
    - any part of its own business or a statement that the organisation has taken no such steps;
- Published on the website with a link on the homepage;
- Must be approved by the Board and signed by a Director.

The Statement should include information about:

- The organisation's structure, its business and its supply chains;
- Its policies in relation to slavery and human trafficking;
- Its due diligence processes in its business and its supply chains;
- The parts of its business and supply chains where there is a risk of slavery and human trafficking taking place and the steps taken to assess and manage that risk;
- Its effectiveness in ensuring that slavery and human trafficking is not taking place in its business and its supply chains, measured against performance indicators it considers appropriate;
- The training available to its staff about slavery and human trafficking.

3.3 Human rights and the aerospace and defence sector

Human rights can have a negative impact on the sector such as the use of weapons and

security products by third countries. The perceived or actual misuse of weapons may lead to civil action and adverse media reporting including by NGOs. Examples of adverse media include the past manufacture in the UK of anti-personnel landmines and cluster munitions, or the sale of legitimate arms shipments to unstable parts of the World which they are used in internal conflicts.

Human rights are also taken into consideration in the granting of export licences to certain countries, *and civil society (NGOs) is very active in monitoring such exports and promoting greater transparency.*

However, the sector can also capitalise on the positives such as satellites used in humanitarian support, as well as ships, vehicles, aircraft and helicopters used to transport humanitarian aid.

3.4 Human Rights and the security sector

If employing security providers, whether local or international, companies should seek to ensure that the private security company (PSC) or private maritime security company (PMSC) subscribes to the International Code of Conduct for Private Security Providers (ICOC.2011) which is based on the Universal Declaration but cascades that down to practical application at company level. The PSC should also have accredited certification to ISO 18788, ISO 28007 or PSC1 which make the ICOC principles auditable. ISO 18788, in particular, allows for the auditing not only of the security provider but also of the client who employs them.

3.5 Awareness and training

In addition to setting out anti-slavery policies and procedures, communicate them to all employees and as appropriate to the supply chain and document all these steps.

3.6 Guidance on Modern Slavery due diligence and risk assessment

Guidance can be found in Appendix C

Part 4: Conflict Minerals

This section explains "conflict minerals" and the applicable legislation which may affect a company which purchases conflict minerals, incorporates them into its products or purchases components or assemblies which include conflict minerals.

4.1 A quick summary

- ***Key minerals used in manufacture of electronic and many other components used in our sectors are classed as "conflict minerals"***
- ***Sourcing and managing of conflict minerals are not necessarily about avoiding certain mining countries but about how good are a company's controls and reporting of the mineral's usage from the mine to the final incorporation in a product***
- ***If you're a UK company getting ready now for new legislation in 2021 will help manage the risk in this area***

4.2 The detail

4.2.1 Background

"*Conflict minerals*," as defined by US legislation, currently include the metals tantalum, tin, tungsten and gold, which are the derivatives of the minerals cassiterite, columbite-tantalite and wolframite, respectively. Downstream companies often refer to the derivatives of these minerals as 3TG. These minerals are essential elements in the manufacture of electronic and other components in the aerospace and defence industries.

Conflict minerals are extracted in many countries including the Democratic Republic of Congo (DRC). Conflict minerals are commonly mined in conditions of armed conflict and human rights abuses and are often sold or traded by armed groups. This has for some years been a particular problem in the DRC, where its mineral wealth is enormous. It is estimated that the country contains between 65-80% of the world's columbite-tantalite (coltan) reserves, 49% of its cobalt reserves, and 3% of its copper reserves. Gold and diamond deposits remain under-explored. Industrial Diamond reserves are estimated at 25% of world reserves.

The US Securities and Exchange Commission (SEC) rules define conflict minerals as 3TG metals, wherever extracted. For example, tin extracted in Canada, Russia or Argentina is considered a conflict mineral by definition. In the SEC rule, "DRC conflict-free" is defined as minerals that were extracted and did not directly or indirectly benefit armed groups in the covered countries. Therefore, tin extracted from Canada is considered "DRC conflict-free" under the definitions of the SEC rule.

The internationally-recognized OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, has a broader scope and covers all minerals, not only 3TG.

Sourcing and managing of conflict minerals are not necessarily about avoiding certain mining countries but about how good are a company's controls and reporting of the mineral's usage from the mine to the final incorporation in a product.

4.2.2 Key legislation

The US Dodd-Frank Act 2010 requires the disclosure of the use of 3TG in supply chains by US or US-related companies and specifically whether originating from the DRC or countries covered by the SEC. Companies may be required to file reports with the Securities Exchange Commission under the US Exchange Act.

Companies in the UK will be regulated under the EU Conflict Minerals Regulation which covers all conflict areas, not just the DRC. This comes into force on 1 January 2021 and aims to ensure that EU importers of 3TG (tin, tungsten, tantalum and gold) meet international responsible sourcing standards, set by the Organisation for Economic Co-operation and Development (OECD). The EU Regulation will impose supply chain due diligence obligations on EU-based importers of 3TG originating from conflict-affected and high-risk areas that reflect the five-step process introduced by the OECD Guidance. Its applicability to UK companies may change after the UK leaves the European Union.

Part 5: Data Protection and Privacy

This section sets out the key areas of data protection law under the General Data Protection Regulation and the Data Protection Act 2018, to which all companies in the UK are now subject. Breaches of this law, such as a loss of customer personal data, are likely to result in heavy financial penalties.

5.1 A quick summary

- ***There can be many forms of personal data; some common examples are names, addresses, personal details, digital footprints, photographs etc.***
- ***The main legislation setting out the rules that apply to processing of personal data is the Data Protection Act 2018 which brought into force the EU General Data Protection Regulations (GDPR)***
- ***The EU General Data Protection Regulation (GDPR) sets a high standard for personal data processing throughout the EU, imposes a raft of new (and sometimes onerous) obligations on those handling the data and provides for a much more punitive enforcement regime for non-compliance***
- ***The term "processing" is defined very broadly and covers any operation or set of operations which is performed on personal data, including collection, recording, organising, storing, adapting, altering, retrieving, transmitting or deleting data.***
- ***Guidance is available for companies to help them develop a policy for this area and links to the guidance available from the UK Information Commissioner's Office (ICO) are provided in the References section to this toolkit.***
- ***You need to make sure you're aware of and can respond to rights of individuals when you are collecting and/or processing the data***
- ***The legislation requires mandatory reporting of personal data breaches to the appropriate data protection officer without undue delay and, where feasible, within 72 hours. In the UK the data protection officer is the Information Commission Officer.***
- ***You need to ensure you comply with the DPA and the GDPR and are aware of your obligations under the legislation, including responding to rights of individuals whose personal data you process***

5.2 The Detail

5.2.1 Background

During its business, a company obtains, processes and communicates information. This information includes offline or online data that may identify a natural person. Such data ("personal data") may include, but is not limited to, names, addresses, personal details, digital footprints, photographs, financial and other identifying data, etc.

The use and processing of personal data is regulated in the UK by the Data Protection Act 2018 ("DPA" as amended from time-to-time) which brought into effect the EU General Data Protection Regulations ("GDPR"). Both the DPA and the GDPR came into force in May 2018 and sets out the rules that apply to the retention and processing of personal data in the UK and the requirements for the safeguarding of data and information within a company.

The safeguarding of data, especially personal data, is a key element of business ethics and companies would be wise to ensure that their GDPR compliance is embedded in both their business ethics and compliance approaches.

To be compliant with GDPR, a company must be able to demonstrate accountability for the

personal data that it processes. A company is required to be committed to protecting the rights and freedoms of data subjects and to safely and securely process all data in accordance with their legal obligations and good data security practices. This is normally set out in a company policy of which there are many open source examples.

5.2.2 Data protection guidance

Guidance on the GDPR has been made available by the European Data Protection Board and the UK's Data Protection Regulator, the Information Commissioner's Office ("ICO"). When read together with Part 3, Chapter 2 of the DPA and the principles set out the basis for a policy:

1. Fairness, lawfulness and transparency

Personal data must be processed fairly, lawfully and transparently in accordance with the rights of individuals. Data subjects have the right to have any data that has been unlawfully processed erased.

2. Limited for its purpose

The processing of personal data must be limited to that purpose for which it was transparently obtained and not further processed or disseminated for any incompatible or unauthorised purposes.

3. Data minimisation

The extent of personal data collected shall be adequate, relevant and limited to that which is necessary to fulfil the purposes for which it was obtained and processed. A company can neither collect any unnecessary personal data on a 'just in case' basis nor process personal data obtained for one purpose for another unconnected purpose, unless the provider has agreed or would otherwise reasonably expect this.

4. Accuracy

The processing of personal data must be accurate, adequate, relevant and not excessive, given the purpose for which it was obtained, and a company must expediently action any individual's request to correct inaccurate personal data relating to them.

5. Retention

A company must not retain personal data for longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reason that the personal data was obtained and retained in the first place. All individuals whose personal data is held, are entitled to request a copy of their data and, in some cases, to prevent a company from using it for particular purposes, or to have it deleted. If the company cannot establish a valid legal, business or other reason for retaining personal data, it should be securely deleted or destroyed in accordance with the company's retention policy.

6. Integrity and confidentiality

Both physical and digital data must be held in a safe and secure environment. The data should be protected against any unauthorized or illegal access either by internal or external parties. Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2.3 Company data protection responsibilities

GDPR and the DPA set out responsibilities for the control and management of data within the company through the appointment of data controllers and data processors.

- A controller determines the purposes and means of processing personal data;
- A processor is responsible for processing personal data on behalf of a controller;
- GDPR places specific legal obligations on a processor, for example, to be required to maintain records of personal data and processing activities. The processor has a legal liability if they are responsible for a breach.

In addition to complying with the data protection principles, companies must ensure that they have a lawful ground for processing personal data. Although this is not a new requirement under data protection legislation, it is now much more important to understand and record the grounds upon which personal data is processed. A company needs to decide and document (including setting out an explanation of the privacy notices) which of the following grounds are the basis for each separate processing activity that will be undertaken:-

1. Consent of the data subject for one or more specific purposes
2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
3. Processing is necessary for compliance with a legal obligation to which the controller is subject
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.2.4 Rights of individuals

Whilst a company may hold and manage data, GDPR and the DPA sets out specific rights for individuals and responsible companies will comply with the rights of individuals in relation to their data as follows:

- Right to be informed - Individuals have the right to be informed about the collection and use of their personal data;
- Right of access - Individuals have the right to access their personal data and invoke that right by making a subject access request;
- Right to rectification - Individuals have the right to correct their personal data without undue delay. A company must correct an error or inaccuracy as soon as practically possible;
- Right to erasure (“to be forgotten”) - Individuals have the right to request a company to erase all their held data in certain circumstances;
- Right to restrict processing - Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances;
- Right to data portability - Individuals may obtain and reuse their personal data for their own purposes across different services;

- Right to object - Individuals have the right to object to the processing of their personal data in certain circumstances. In addition, individuals have an absolute right to stop their data being used for direct marketing;
- Right to object to the processing of their personal data in certain circumstances, particularly where the processing involves an element of fully automated individual decision-making and profiling.

5.2.5 Reporting breaches

If, following investigation after a breach, non-compliance with the company's policy is evident, that the breach is likely to result in a risk to the rights and freedoms of individuals, the breach must be notified to the ICO without undue delay and, ideally, within 72 hours of discovery Where a data breach is likely to result in a "high risk" to the rights and freedoms of individuals, a company is obliged to notify the affected individuals without undue delay.

Part 6: Export and Trade Controls

This section sets out the basic requirements for companies that may be subject to UK, US or other national export controls relating to restricted goods/technology and services for military or civil use and, the support that ADS provides through the special interest group – the Export Group for Aerospace, Defence & Dual-Use (EGADD).

6.1 A quick summary

- ***Export control regulations are the legal requirements controlling the export of and trade in goods/technology and services (items) which are deemed to be sensitive***
- ***Under UK regulations, since 2004, any UK person who engages in "trafficking and brokering" type activities whereby controlled military goods move between two or more overseas countries, which do not come from, through or via the UK, requires a Trade Control Licence from the UK Government***
- ***You will need an export or trade control license for any goods or service that are classified in this way***
- ***You need to be mindful of any export-controlled goods/technology or services you are purchasing, and ensure you understand any restrictions and obligations that will result***
- ***Many other countries operate export controls, so it's vitally important you understand any other relevant legislation***
- ***It's important to understand who you are conducting business with, where your goods/technology will be routed through and where your customers and any end-users or ultimate beneficiaries are located to make sure there are no applicable sanctions***

6.2 The Detail

6.2.1 Background

Export and Trade Control regulations are the legal requirements controlling the export of and trade in goods and services (items) which are considered to be sensitive because of what they are, where they are going and what they are to be used for. The regulations that will affect aerospace defence and security companies with goods originating from the UK are those which are exercised by the Export Control Joint Unit (ECJU). It is the UK exporter's responsibility to take advice in these sensitive areas and ADS has a special interest group, Export Group for Aerospace, Defence & Dual-Use (EGADD), which can support and advise ADS Members on these issues.

The UK (as with most countries) has a system to address issues over Security and Political Influence which considers the following issues/criteria: -

- Respect for the UK's international commitments, in particular sanctions decreed by the UN Security Council and those decreed by the European Community, agreements on non-proliferation and other subjects, as well as other international obligations;
- The respect of human rights and fundamental freedoms in the country of final destination;
- The internal situation in the country of final destination, as a function of the existence of tensions or armed conflicts;
- Preservation of regional peace, security and stability;
- The national security of the UK, or territories whose external relations are the UK's

responsibility, and of allies, EU Member States and other friendly countries;

- The behaviour of the buyer country with regard to the international community; in particular its attitude to terrorism, the nature of its alliances and respect for international law;
- The existence of a risk that the equipment will be diverted within the buyer country or re-exported under undesirable conditions;
- The compatibility of the arms exports with the technical and economic capacity of the recipient country, considering the desirability that states should achieve their legitimate needs of security and defence with the least diversion for armaments of human and economic resources

The regulations control the export of and trade in certain military, security and software items – especially designed or modified for military use – as well as certain dual use items – items (and, if relevant, components) that have been designed originally for civil purposes, but can have a potential military usage, and meet specified technical standards. The shipping of such items is controlled through the granting of a licence by the Government which permits their export to an approved customer.

In the UK the ECJU (part of the Department for International Trade) is responsible for the review and issuing of all export licences. Information on the items which are controlled and the licences which are available can be found through the UK Government Export Control Organisation website.

6.2.2 Items procured from outside of the UK

If items are procured from suppliers in other countries, those items will be subject to the export control regulations of the country of origin, and these regulations may restrict the ability to export the goods from the UK or even to transfer the goods to other parties within the UK. The supplier of the items concerned should advise of any such restrictions and, to avoid the risk of contravening such regulations, it is advisable to check before procuring to determine if there are any potential restrictions. Under the UK MoD's DEFCON 528 – Overseas Expenditure, Import & Export Licences, all contractors to the UK MoD are required to inform their customer of any re-export requirements that might relate to the materiel that is being provided, down to and including at the component level.

The US export controls are more complex and have a broader and extra-territorial impact. There are a number of US Government departments which implement US Export Controls but there are two which are likely to be of most concern to companies in the UK.

- US Department of State, through Directorate of Defense Trade Controls (DDTC), controls items governed by International Traffic in Arms Regulations (ITAR) and covers the more significant military items
- US Department of Commerce, through Bureau of Industry and Security (BIS), controls export of items governed by Export Administration Regulations (EAR), which covers less significant military items as well as dual-use and non-military items

The relevance of these US export control regulations and "Business Ethics" particularly relate to the ITAR, and especially ITAR Part 129 (covering trafficking and brokering activities) and Part 130 (covering political contributions, fees and commissions).

6.2.3 Sanctions

Many countries including the UK, Japan and the US, as well as international organisations, such as the EU, UN, World Bank and other organisations, may place restrictions (sanctions) on countries, regimes, individuals, companies or other organisations. These sanctions may range from embargoes on the trading of goods and services, to financial sanctions including asset freezes. If a company or individual breaches these sanctions, there may face very severe penalties and they may also be subject to sanctions including having their assets frozen.

It is incumbent upon all companies, through due diligence, to know who they are directly or indirectly dealing with whether it be a customer, end-user, supplier, agent, broker, adviser or independent consultant; what their goods/ technology or services will be used for and how they will be routed.

Sanction lists are published and maintained by the various countries and organisations so that checks can be made on the status of a sanction on a particular country or third party. There are commercial subscription services which provide information on sanctions and listed persons etc.

Part 7: Tax Evasion

This section briefly sets out the risks of tax evasion and provides links to guidance from the British Government. Companies need to take professional advice on taxation, whether or not they are exporting into EU and non-EU countries, as existing tax arrangements with the UK are likely to change post-BREXIT.

7.1 A quick summary

- ***Tax efficiency can be described as "minimising tax liability when given many different financial decisions. A financial decision is said to be tax efficient if the tax outcome is lower than an alternative financial structure that achieves the same end." But is not illegal if it conforms to the relevant tax regulations***
- ***Tax evasion is a criminal act and can be described as "the illegal evasion of taxes by individuals, corporations, and trusts"***
- ***The Criminal Finances Act 2017 part 3, makes companies and partnerships criminally liable if they fail to prevent the facilitation of tax evasion***
- ***There is a lot of guidance available from the British Government***

7.2 The detail

7.2.1 Tax Evasion

Tax evasion by companies and individuals in the UK is investigated by HMRC, (which also has the powers to prosecute under the Bribery Act 2010). A tax evasion allegation may reveal other unethical behaviour and has been the source of discovery of bribery cases in the USA.

An example would be an overseas sales agent acting on behalf of a UK company in a specific country but commissions for that work are paid by the company principal into an offshore account (e.g. Cayman Islands), therefore, helping the agent to evade paying local taxes. Such an arrangement may be flagged up by the company's bank.

Or, in reverse, payments made by a UK company are diverted through an offshore account. Whilst some of this may be legitimate, it may be picked up by the authorities who will seek to determine whether there has been tax evasion, money laundering or other criminal activity.

Given the UK's current position as a destination for financial services and easy access to the purchase of property and other valuable assets which are used for the laundering or depositing of illicit funds, the **Criminal Finances Act 2017 came into force.**

"*Criminals exploit financial transactions to serve their wicked ends. In an ever-growing digital world, they continually try to find new ways in which money can enter and leave the economy looking legitimate. Reforms are needed to protect individual victims and the economy.*
***The Criminal Finances Bill provides an opportunity for the public and private sectors to get ahead of the criminals and clamp down further on money laundering and corruption*."** CEO, British Bankers Association.

7.2.2 The Criminal Finances Act 2017 part 3,

This makes companies and partnerships criminally liable if they fail to prevent the facilitation of tax evasion by either a member of their staff or an external agent, even where the business was not involved in the act or was unaware of it. The Act covers tax payable in the UK or overseas (where there is a UK element).

The penalty for failure to prevent tax evasion by a company is an unlimited fine and confiscation of assets.

For a conviction it must be shown that there was:

- criminal tax evasion by a taxpayer
- criminal facilitation of the offence by a representative of the company
- the company failed to prevent its representative from committing the criminal act.

In its defence the business may claim that:

- It put in place reasonable prevention methods to prevent evasion; or
- It is unreasonable or unrealistic to expect it to have such procedures in place.

The Act also covers Unexplained Wealth Orders, where individuals whose assets are disproportionate to their known income will need to explain the origin of their wealth.
In addition, Disclosure Orders, where a Company or Financial institution must disclose details of accounts and transactions to UK Authorities, is extended to money laundering investigations.

The Criminal Finances Act 2017 introduced two new strict liability corporate offences in the UK of failing to prevent the facilitation of tax evasion.

Both offences require there to have been an underlying, predicate offence of tax evasion; the first requires an offence to have been committed in relation to the evasion of a UK tax (the UK offence) and the second requires an offence to have been committed in relation to the evasion of a foreign tax (the foreign offence). However, there is no need for a conviction to have been secured for the underlying predicate offence; it is sufficient for the enforcement authority to prove beyond reasonable doubt that both the evasion and the facilitation have occurred.

The corporate liability bites where a person associated with the corporate entity facilitated the tax evasion. It is a defence for a company to be able to evidence 'reasonable prevention procedures'. The key is therefore for companies to ensure they have robust policies, procedures and training programmes in place. HMRC has issued explanatory guidance for companies in deciding what are reasonable prevention methods to have in place

The UK tax evasion offence is very broad and can be committed by a company, whether or not it has a UK nexus. The foreign tax evasion facilitation offence requires some UK nexus, although the UK nexus does not have to relate to the tax evasion itself. The tax evader does not for example have to be located in the UK. There is also a dual criminality requirement – the tax evasion AND the facilitation must be offences under local AND English law.

The penalty for companies that fail to prevent tax evasion is an unlimited fine and confiscation of assets.

HMRC has issued explanatory guidance for companies in deciding what are reasonable prevention methods to have in place.

Part 8: Competition Law

This section sets out the basic principles applicable to the UK and EU competition law regimes (although increasingly the vast majority of countries worldwide implement similar regimes prohibiting anti-competitive behaviour). In particular, it looks at the rules prohibiting anti-competitive agreements and abuse of dominance, as well as practical tips on how to avoid breaching such rules.

8.1 A quick summary

- ***The purpose of competition law rules is to ensure that companies compete vigorously in the market and do not collude with competitors or engage in anti-competitive practices to drive competitors out of the market.***

- ***Competition law infringements can be broadly classified into two categories: anti-competitive agreements and abuse of dominance. However, both of these concepts can be interpreted broadly to cover a wide range of potentially infringing conduct.***

- ***Consequences of breaching competition laws can be severe, including criminal prosecutions for individuals; significant fines for companies and individuals; reputational damage; contracts being found to be void and unenforceable; and third-party claims for damages.***

- ***The risk of liability is not just theoretical. In a growing number of jurisdictions (including the UK and the US) individuals can be found guilty of a criminal offence for breaching applicable competition laws.***

8.2 The Detail

8.2.1 Anti-competitive agreements

Article 101 of the Treaty on the Functioning of the European Union (**Article 101 TFEU**) and the corresponding UK provision at Chapter 1 of the UK Competition Act 1998 set out the basic principle that companies and individuals are prohibited from entering into any agreement or concerted practice which has the object or effect of preventing, restricting or distorting competition.

8.2.1.1 Article 101 TFEU:

1. The following shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which:

(a) directly or indirectly fix purchase or selling prices or any other trading conditions;(b) limit or control production, markets, technical development, or investment;

(c) share markets or sources of supply;

(d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

2. Any agreements or decisions prohibited pursuant to this Article shall be automatically void.

3. The provisions of paragraph 1 may, however, be declared inapplicable in the case of:

- any agreement or category of agreements between undertakings,

- any decision or category of decisions by associations of undertakings,

- any concerted practice or category of concerted practices,

which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:

(a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;

(b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

8.2.1.2 Chapter I of the UK Competition Act 1998:

Chapter I of the UK Competition Act 1998 provides a corresponding prohibition in relation to agreements or concerted practices preventing, restricting or distorting competition within the UK.

It is important to note that under both EU and UK legislation the concept of an "agreement" is interpreted extremely widely, regardless of its form, and can catch conduct that may not even appear to be an agreement, including: written and oral agreements; agreements that are not legally binding or not implemented; informal arrangements and understandings; exchanges of commercially sensitive information (even if one-way); and decisions by trade associations.

Agreements between competitors acting at the same level of the supply chain (e.g. between competing manufacturers of aerospace components) are most likely to give rise to antitrust issues, particularly where they involve a number of industry players. However, agreements between companies operating at different levels of the supply chain may also be problematic in certain circumstances.

Common examples of agreements that could be found to infringe antitrust law include: price fixing; market sharing; bid rigging; resale price maintenance; and information exchange. The risks of information exchange are particularly acute in a trade association context and companies should be careful not to exchange competitively sensitive information, even if this does not form part of a formal agreement. As a general rule, this includes not discussing or agreeing the following with competitors:

- Prices, discounts or timings of pricing changes
- Allocation of customers or regions
- Capacity, supply terms or output
- Product cost information
- Strategic or marketing plans
- Intended bids

Individuals should also be aware that engaging in concerted practices can lead to prosecutions for of the cartel offence. In summary, it is an offence for an individual to agree with one or more other persons to make or implement, or to cause to be made or implemented, an arrangement which amounts to price fixing, bid rigging or market sharing.

8.2.2 Abuse of dominance

Article 102 of the Treaty on the Functioning of the European Union (**Article 102 TFEU**) and the corresponding UK provision at Chapter 2 of the UK Competition Act 1998 provides that companies in a dominant position on a particular market (assessed on a case by case basis but typically with a market share greater than 40%) have a special responsibility not to engage in conduct that constitutes an abuse of that dominant position.

8.2.2.1 Article 102 TFEU:

Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.

Such abuse may, in particular, consist in:

(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;

(b) limiting production, markets or technical development to the prejudice of consumers;

(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

8.2.2.2 Chapter II of the UK Competition Act 1998:

Chapter II of the UK Competition Act 1998 provides a corresponding prohibition in relation to an abuse of dominance that affects trade within the United Kingdom.

As with the restrictions on anti-competitive agreements, it is important to note that under both EU and UK legislation merely holding a dominant position on a particular market is not a breach of antitrust law. It is the abuse of that dominant position that is problematic.

“Dominance” is generally viewed as the ability of a company to act in a way that is independent of its competitors, customers and consumers. Assessing dominance is a complicated analysis and it is rarely possible to come to a firm view in any particular case. Caution should also be exercised in sectors where markets are capable of being construed narrowly (which could result in a company having a high market share on such narrow definition).

If a company is found to be dominant on a particular market, it is at risk of breaching competition law if it engages in certain conduct that constitutes an abuse of that market power. Notable examples of abusive conduct include refusal to supply; predatory pricing; price discrimination; excessive pricing; tying and bundling; and margin squeeze.

Part 9: Conclusion

There is a positive change in public attitudes towards companies that adopt good business ethics. This is driven by an increased awareness of the cost of malfeasance to society at large, and global and publicly accessible communications via digital devices. Underpinning this are the challenges to all organisations posed by Non-Governmental Organisations (NGOs) and investigative journalism. Leading global anti-corruption NGOs include Transparency International, Corruption Watch and the Campaign Against the Arms Trade amongst others There have been many headline-grabbing media investigations, such as "the Panama Papers" and the Cambridge Analytica and Facebook exposés. Unethical behaviour cannot be kept a secret – it is not **if it will be exposed, but rather when** and of course by whom, over which companies will have little control.

All of this activity has driven the introduction of new laws and regulations to hold individuals, companies and their directors to account. Customers, banks and regulators are increasingly demanding evidence of a company's compliance programmes, and how they have been implemented.

Therefore, given the rapidly increasing worldwide effort to tackle unethical and criminal behaviour, this Toolkit is designed to help companies and individuals operating in the aerospace, defence and security sectors, to strongly embed a culture of ethical compliance that will protect their businesses, stakeholders, employees and the reputation of the industry.

"*It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently*". Warren Buffett

Part 10: References

Defense Industry Initiative (DII) Toolkit for SMEs - DII has developed several complimentary tools to assist companies involved with government contracting with establishing and maintaining effective ethics and compliance programs
https://www.dii.org/featured-tools

International Forum on Business Ethical Conduct (IFBEC)
IFBEC Global Principles of Business Ethics for the Aerospace & Defense Industry – The purpose of IFBEC is to promote and foster through the Global Principles the development of global, industry-wide ethical standards for companies that are active in the aerospace and defence business sector. These include both codes of business ethics and for supplier conduct
https://ifbec.info/wp-content/uploads/2013/06/IFBEC-Global-Principles.pdf

IFBEC Model Supplier Code of Conduct
https://ifbec.info/wp-content/uploads/2018/.../Final-IFBEC-Model-Supplier-Code.pdf

UK Bribery Act Guidance
This is a great resource to use to help you understand the UK Bribery Act. It provides practical guidance to companies large and small on what they should consider in building an anti-bribery compliance programme.
https://www.gov.uk/government/publications/bribery-act-2010-guidance

UK General Data Protection Regulations (GDPR) Guidance
The guide to cover the key points that organisations need to know to comply with the Data Protection Act 2018 and where it is relevant, includes links to relevant sections of the GDPR itself.
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Modern Slavery Statistics and Guidance
Provides important background statistics on modern slavery and useful links to be able to identify and understand the risks of modern slavery.

Global Estimates of Modern Slavery - International Labour Organization
https://www.ilo.org/wcmsp5/groups/public/@dgreports/.../wcms_575479.pdf

Anti-Slavery International
https://www.antislavery.org/slavery-today/modern-slavery/

Transparency in Supply Chains – Practical Guide
A practical guide to managing the risks of modern slavery and enforces labour in the supply chain.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/649906/Transparency_in_Supply_Chains_A_Practical_Guide_2017.pdf

Business and Human Rights

A number of useful resources including the UN Guiding Principles on Business and Human Rights which set out guidelines for companies to prevent, address and remedy human rights abuses committed in business operations.
https://www.business-humanrights.org/en/un-guiding-principles
UN Guiding Principles – Reporting Framework with Implementation guidance

Voluntary Principles on Security and Human Rights

http://www.voluntaryprinciples.org/

Security providers and human rights

The Montreux Document
https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies

The International Code of Conduct for Private Security Service Providers (ICOC)
https://www.icoca.ch/en/the_icoc

ISO 18788 – Management systems for private security companies: Requirements with Guidance
https://www.iso.org/standard/63380.html

ANSI/ASIS PSC1
https://www.acq.osd.mil/log/PS/.psc.html/7_Management_System_for_Quality.pdf

UN Guiding Principles – Reporting Framework with Implementation guidance

Data Protection and Privacy

There is guidance on the ICO website to assist companies to determine whether they are a controller or processor. This has significance as the obligations of the parties will vary depending on their role.

Guidance can be found at the following links:-

Controller or Processor checklist - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

Detailed guidance on Controllers and Processors - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/

Contracts and liabilities between Controllers and Processors - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/

APPENDIX A

Further information on the UK Bribery Act 2010[4]

A.1 Bribing another person (Section 1)

It is an offence for a person ("A") to offer, promise or give a financial or other advantage to another person ("B") in circumstances where: (i) A intends to induce or reward a person for the improper performance of a function (regardless of whether B personally performs the requested action or inaction); or (ii) A knows or believes that the simple acceptance such advantage by B would be improper.

Facilitation payments, often referred to as grease payments, are generally small amounts of money paid to others as a means of ensuring they perform a function or activity. Such payments also constitute the offering, promising or giving of a financial advantage and amount to bribery under the Bribery Act.

A.2 Being bribed (Section 2)

It is an offence for:

a) A person ("B") to request, agree to receive or accept a financial or other advantage:

   (i) intending that a relevant function or activity should be performed improperly (whether by B or another person); OR

   (ii) where the request, agreement or acceptance is, itself, improper; OR

   (iii) as a reward for the improper performance (whether by B or another person) of a relevant function or activity

It is also an offence where in anticipation of, or in consequence of B requesting, agreeing to receive or accepting a financial or other advantage, a relevant function or activity is performed improperly by B or by another person ("C") at the request of B, or with B's assent or acquiescence.

In the above cases, it does not matter whether the bribe is offered or paid directly through a third party (such as an advisor or agent). These offences also address so called "private bribery" that is between individuals of two companies/organisations including via third parties, intermediaries or agents and cover all forms of "one-to-one" bribery including individual employees, company officers, public officials etc.

Save for (a)(i) above, it also does not matter whether B or C knows or believes that the performance of the function or activity is improper.

A.3 Improper performance and the expectation test

In simple terms, "improper performance" under sections 1 and 2 of the Bribery Act means behaviour which breaches an expectation of good faith, impartiality or a position of trust in respect of the function or activity carried out. The test of what is expected is a test of what a reasonable person in the UK would expect in relation to the performance of the type of function or activity concerned. The Bribery Act 2010 does not contain much more by way of explanation on this point. Instead, the Law Commission has indicated that a jury is required to apply the

[4] Source: Allen and Overy

ordinary meaning of these words in any given situation. It is therefore for people of moral integrity to decide what, in a given set of circumstances, would be expected in relation to the performance of the type of function or activity concerned.

In deciding what such a person would expect, Section 5 of the Bribery Act 2010 does contain some guidance on what cannot be taken into account. Section 5 explicitly disregards the view that *bribery is the way business is done in certain countries – and, if we do not pay bribes, we will lose out to others who pay*. Instead, Section 5 states that in applying the expectation test, *"any local custom or practice is to be disregarded unless it is permitted or required by the written law applicable to the country or territory concerned"*. There are few, if any, countries that permit bribery under these circumstances and, therefore, **local custom and practice will not constitute a legal defence.**

A.4 Bribery of a foreign public official (section 6)

If is an offence to:

- offer, promise or give a financial or other advantage to a foreign public official (or to another at the request of the foreign public official, or with the assent or acquiescence of the foreign public official);

- directly or indirectly through a third party (such as an advisor or agent); and

- with the intention of obtaining or retaining a business, or an advantage in the conduct of business.

Whilst an omission or use of influence on the part of the foreign public official will constitute an offence, there is no requirement for improper performance; where the simple acceptance of the advantage is improper, an offence is committed. A facilitation or grease payment made directly or indirectly to a foreign public official with the intent to influence them in that capacity therefore amounts to bribery under the Bribery Act regardless of any improper performance.

Foreign public officials include:-

- Holders of legislative, administrative or judicial positions of any kind, whether appointed or elected of a country or territory outside the United Kingdom,

- Employees in a public agency or public enterprise (e.g. a state-owned company) and international organisations, (e.g. United Nations, NATO).

In many countries, key industries are owned by the government (e.g. state-owned enterprises) although they may appear to be a normal commercial operation. For example, the bribing of a manager of a foreign state-owned defence company would constitute an offence of bribing a foreign public official.

A.5 Offences by bodies corporate (Section 14)

If an offence under section 1, 2 or 6 is proved to have been committed with the "consent or connivance" of a senior officer of a body corporate (or a person purporting to act as a senior office), both the corporate and the individual senior officer are liable to prosecution for the same offence.

This offence addresses the actions of company directors, managers and other similar persons who might be categorised as a "director" or "senior person" and, in relation to Scottish partnerships, a partner in that partnership.

A.6 Corporate offence of failing to prevent bribery (Section 7)

It is an offence under the Bribery Act for a relevant commercial organisation to fail to prevent a person associated with it from bribing another (with the intention of obtaining or retaining business, or a business advantage, for the relevant commercial organisation).

This offence can be committed by relevant commercial organisations, meaning companies and partnerships:

- formed in the UK and carrying on business anywhere (i.e. within the UK or elsewhere); and
- formed outside of the UK and carrying on business in the UK.

The definition of "associated person" is very broad and captures anyone performing services on behalf of the company including agents, advisers, employees, etc. Whether or not a person is associated with a relevant commercial organisation is to be determined in light of all the relevant circumstances and not merely by reference to the nature of the relationship. Employees are presumed to performing services on behalf of their employer, unless the contrary can be shown.

It is a legal defence for the relevant commercial organisation to prove it had in place "adequate procedures" designed to prevent those who perform services for it from committing bribery.

The Ministry of Justice Guidance (the "Guidance") to the Act provides guidance as to what procedures a company might adopt to prevent bribery. However, the simple adoption of a policy in line with the guidance does not guarantee a safe harbour from prosecution (this is discussed further in the Guidance section).

A.7 Penalties (Section 11)

An individual found guilty of an offence under the Bribery Act faces up to 10 years' imprisonment, an unlimited fine, or both. Additional consequences may also flow, for example, an individual's disqualification from acting as a company director.

A company or partnership convicted under the Bribery Act also faces an unlimited fine.

Since bribery is a criminal offence, funds (including profits) which can be said to derive from a bribe or a corrupt transaction will amount to criminal property under the Proceeds of Crime Act 2002. In addition to liability under the Bribery Act, both individuals and entities may therefore face further criminal penalties and civil recovery under the Proceeds of Crime Act 2002. This could include the recovery of any dividends paid to shareholders.

A.8 Territorial Application (Section 12)

The Act applies to all activities which take place in the UK. It also has extra-territorial reach. If an offence is committed outside of the UK, but the person or entity involved has a close connection with the UK, the act or omission can still be prosecuted in the UK.

An individual has a close connection with the UK if they qualify under one of the varying degrees of UK citizenship set out in the Act or is ordinarily resident in the UK (be they UK citizens or foreign nationals). An entity has a close connection with the UK if it is incorporated here or is a Scottish partnership.

The corporate offence of failing to prevent bribery (section 7) can be prosecuted in the UK where the act or omission took place anywhere in the world, as long as the company carries on business, or a part of its business, in the UK.

APPENDIX B

Anti-bribery standards and tools

B.1 ASD Common Industry Standards (CIS)

In July 2006 the AeroSpace and Defence Industries Association of Europe (ASD) established an Ethics and Anti-Corruption Working Group, having recognised the growing importance of good practice in ethical issues. After consultations involving independent advice from experts of the International Chamber of Commerce Anti-Corruption Commission, ASD developed the Common Industry Standards (the "CIS").

The essence of the CIS and other anti-bribery initiatives, especially those of the NGOs, including Transparency International, is to improve the standard of business ethics and its implementation in the defence and security sectors, to ensure the long-term success and sustainability of the industry. The CIS can be found at: - www.asd-europe.org/about-us/ethics/

B.2 IFBEC Global Principles of Business Ethics

The International Forum on Business Ethical Conduct (IFBEC) was created by member companies of the Aerospace Industries Association of America (AIA) and the AeroSpace and Defence Industries Association of Europe (ASD) in 2010. It provides a forum to exchange information on best practices in business ethics and global trends and to promote and foster through the Global Principles the development of global, industry-wide ethical standards for companies in the aerospace and defence business sector.

The IFBEC Global Principles affirm the sector'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. Companies that formally adhere to the principles commit to including programs and policies that foster ethical business conduct consistent with the Global Principles in their corporate business practices.

In addition, IFBEC provides a model Supplier Code of Conduct which incorporates a number of topical business ethics areas including Bribery and Corruption, Fraud and Human Rights.

B.3 ISO37001:2016 Anti-bribery management system

The ISO37001:2016 anti-bribery management system was published October 2016 . It is being considered in Singapore and Peru, amongst others. More than 100 companies worldwide have certified to the standard across many sectors, including aerospace and defence.

Certification to ISO37001 provides an internationally recognised benchmark of an organisation's commitment to an anti-bribery programme. Certification provides clear evidence to all stakeholders, of the veracity of an organisation's anti-bribery intent, its processes and controls. It demonstrates that the organisation and its leadership has adopted, embedded, is practising and constantly improving its anti-bribery measures. This will not only strengthen internal compliance to mitigate bribery risk, but also catalyse those key cultural changes which will influence others, both internal (employees) and external (customers and suppliers), to behave and stay on the right side of the law.

While compliance with ISO37001 cannot provide legal assurance that bribery will not occur and is not a defence to a charge of having committed a bribery offence, implementing the standard will help the organisation prevent bribery, positively change its ethics culture and provide verification and demonstration to third parties, be they customers or law enforcers, that it has implemented an anti-bribery management system.

B.4 Other useful anti-bribery tools

Transparency International's Business Principles for Countering Bribery provides a framework for companies to develop comprehensive anti-bribery programmes. These tools are useful for both large and small companies and can be found at:
http://www.transparency.org/whatwedo/tools/business_principles_for_countering_bribery

APPENDIX C

Modern slavery due diligence and risk assessment

C.1 Due diligence

Detecting modern slavery is a complex task, given that most instances are hidden in an opaque network of tiers and sub-contractors. Given the reputation and legal risks associated with being accused of involvement with modern slavery, companies must undertake due diligence on their supply chains This means identifying and assessing human rights impacts, acting upon the findings, tracking these measures, and communicating how impacts are addressed. To root out modern slavery companies should focus on:

- **Sub-contracting**: Sub-contracting without the knowledge and permission of buyers is one of the primary obstacles to identifying and combating modern slavery. Map your supply chains. Also, engage with your suppliers. Then draft supplier codes and put clauses in supplier contracts to ensure that all suppliers down the chain are required to do due diligence and avoid involvement with slavery.

- **Ethical recruitment practices**: The opaque conditions of the recruitment processes are another obstacle to identifying modern slavery. Too many sub-contractors, temporary employment agencies or the involvement of middlemen provide fertile ground for abusive working conditions and exploitation. Audit and assess suppliers' recruitment practices, as well as suppliers' recruitment agencies' practices.

- **Access to Remedy**: Feedback from workers helps to identify and manage slavery risks in supply chains. Establish grievance mechanisms that covers your supply chain.

- **Purchasing practices**: Modern slavery arises from purchasing practices that put pressure on suppliers, like tight production windows, short-term contracts, last-minute or short-term orders and severe payment terms. Assess your own business model, including purchasing practices such as contracting terms and prices, to ensure they are not inadvertently generating grounds for modern slavery.

C.2 Risk assessment

Notwithstanding the obligations under the UK Modern Slavery Act, companies need to ensure their own human rights business ethics are in order and be ready to positively respond to requests for due diligence by primes or customers further up the supply chain. Measures that may be taken include a risk assessment (which may feed into the overall risk register) and asking questions about your organisation, its suppliers and customers including but not limited to:

- Start at home - where do you procure your office supplies and equipment?
- How do you employ and recruit local suppliers, like cleaning staff? If through an agency, how are those staff recruited, paid and treated?
- Map out the extent of your own supply chain – especially those critical to the business and in higher risk jurisdictions.
- Enquire where your suppliers source their own products?
- Where are your products manufactured and from what raw materials – could they include undisclosed conflict minerals?

- In what types of industries do your customers do business, and where, and which, of those industries have a propensity for enforced or child labour?
- Generally - the less information a supplier divulges about itself, the greater the risk of concealing slavery.
- Visit suppliers, especially in countries where the risk is higher: look at the way they operate and observe their workers; ask the difficult questions; share best practices – and document.

As a consequence of the risk assessment where there is more than a low risk of modern slavery, conduct due diligence on the other party.

C.3 Modern slavery red flags

Because modern slavery is hidden, it is notoriously difficult to detect. Communicating the message can be done through training, focused campaigns, face-to-face meetings and digital media. Everyone in the company should be made aware of the common indicators of modern slavery, when visiting a customer, business partner or supplier. These will include: -

- **Supplier offers offsite meetings only:** encourages you to meet in the hotel lobby or an office clearly chosen to be separate from the work site.
- **Restricted movement:** workers appear to be held against their will or unable to escape
- **Overtime:** little/no breaks just to make minimum wage
- **Recruitment fees/loans:** charged to workers; high living costs/accommodation deducted from wages
- **Personal documents:** withheld from workers by employer so they cannot leave (e.g. passports, ID cards, etc)
- **Resistance to any form of audit:** be that of operations or relevant books and records
- **Payment:** in cash or through a third-party vs a documented system showing rates, hours worked, taxes, etc
- **Workers subcontracted:** throughout supply chain, increased risk of exploitation
- **No complaints procedure:** workers unable to raise grievances/protect their rights
- **Living conditions:** living together on site or in poor employer-provided accommodation
- **Transport:** does the company operate a bussing system for workers to low grade accommodation for particular groups e.g. other nationals
- **Slave behaviour:** workers fearful of retaliation, prevented from speaking, few possessions

To ensure a high level of ethical integrity, it is important that companies conduct due diligence and audit their suppliers and contractors themselves or use trusted and reputable auditors; suppliers can hide evidence of enforced labour/slavery, especially if locally examined.

Practical guidance on the UK Modern Slavery Act and how to ensure transparency in supply chains can be found in Part 10 References.

Interchange has been an active Member of the ADS Business Ethics Network since 2007 and is honoured to compile this updated Business Ethics Toolkit.

We have supported the aerospace and defence sector for more than 10 years, providing our large and small customers with risk management and compliance advice on business ethics, the prevention of bribery, corruption and modern slavery.

Companies cannot assume that the business culture in many new markets is the same as closer to home. **Interchange** helps its customers address those hidden ethics challenges - providing them with the tools to succeed in those markets, while building trust with their customers, suppliers and other stakeholders and, delivering business sustainability. We are thrilled to have been selected as an Approved Provider for the new SC21/NMCL programme for the delivery of the Ethical Performance and Corporate Social Responsibility modules. The SC21/NMCL programme supports small and medium size companies in the aerospace, defence and automotive sectors.

Interchange provides its customers with:
Advice and Risk Audit – business ethics gap analysis including in preparation for ISO37001 Anti-bribery Management System and SA8000 Social Accountability
ISO37001 and SA8000 standards – implementation
Enhanced Due Diligence – risk-based integrity due diligence on associated persons
Policy and business process – tailored to your needs and compliant with the relevant laws
Export compliance – support for regulatory compliance and licence issues
Training – anti-bribery, modern slavery at all levels and functions

Find out how **Interchange** can strengthen your compliance programme while letting you get on with successfully running your business. Contact us at:-

Interchange Solutions Ltd | 10th Floor | 88 Wood Street | London | EC2V 7RS
T: +44 (0) 203 745 4995 | E: info@interchange-solutions.co.uk | W: www.interchange-solutions.co.uk
"Turning Risk into Business Value"