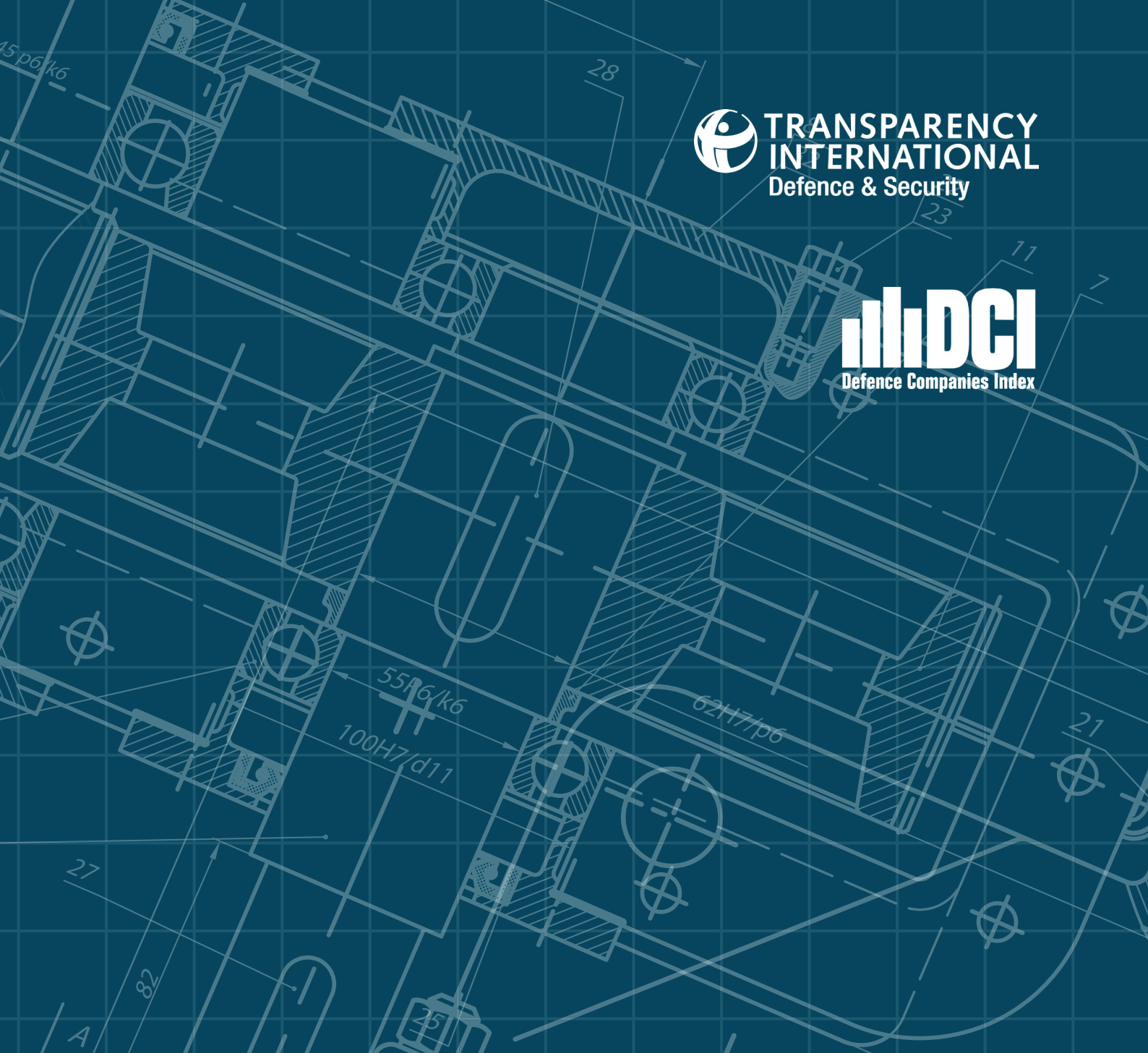


TRANSPARENCY INTERNATIONAL
Defence & Security

DCI
Defence Companies Index

DEFENCE COMPANIES INDEX ON ANTI-CORRUPTION AND CORPORATE TRANSPARENCY 2020

Key Findings

Transparency International (TI) is the world's leading non-governmental anti-corruption organisation, addressing corruption and corruption risk in its many forms through a network of more than 100 national chapters worldwide.

Transparency International Defence and Security (TI-DS) works to reduce corruption in defence and security worldwide.

This report is based on data from the Defence Companies Index on Anti-Corruption and Corporate Transparency (DCI), published on 9 February 2021. The full data is available at www.ti-defence.org/dci

We would like to thank the UK Foreign Commonwealth & Development Office (FCDO) for their generous financial support that made this research possible.

Authors: Charlie Linney

Contributors: Najla Dowson-Zeidan, Mia Paukovic

Editors: Natalie Hogg, Stephanie Trapnell

Published November 2021.

CONTENTS

ACRONYMS

CEO Chief Executive Officer

DCI Defence Companies Index on Anti-Corruption and Corporate Transparency

ESG Environmental, Social and Corporate Governance

OECD Organisation of Economic Co-operation and Development

TI-DS Transparency International – Defence & Security

SOE State-owned enterprise

SIPRI Stockholm International Peace Research Institute

THE INDEX AT A GLANCE

The Defence Companies Index on Anti-Corruption and Corporate Transparency (DCI) assesses the level of commitment to transparency and anti-corruption standards in 134 of the world's largest defence companies across 38 countries.

Based on in-depth discussions with anti-corruption and defence experts, Transparency International Defence & Security (TI-DS) identified 56 distinct indicators where stronger controls and greater transparency can reduce corruption risk. These indicators are grouped into 10 key risk categories, which form the basis for the assessment questionnaire:

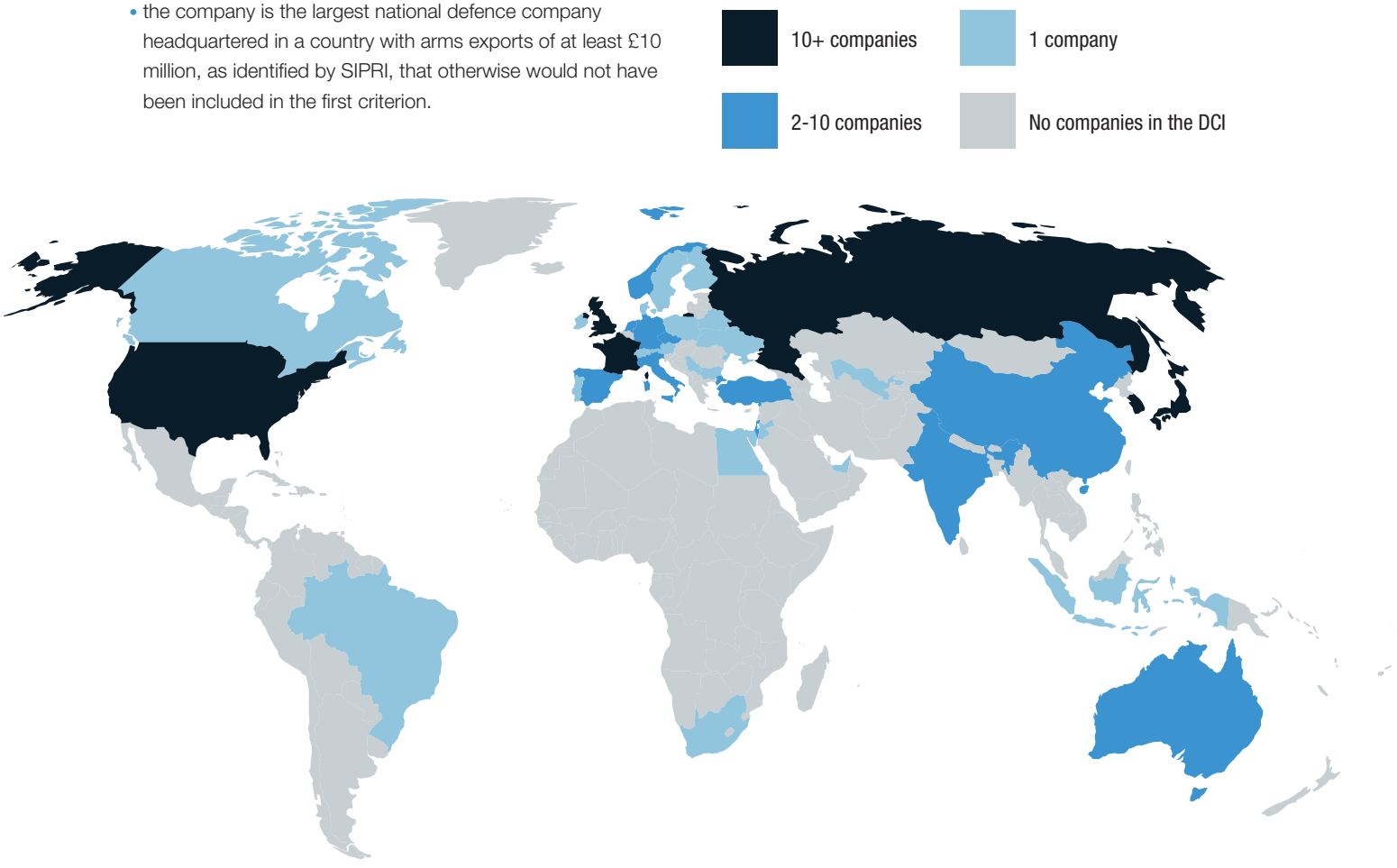
Leadership & Organisational Culture	**Supply Chain Management**
Internal Controls	**Agents, Intermediaries & Joint Ventures**
Support to Employees	**Offsets**
Conflict of interest	**High Risk Markets**
Customer Engagement	**State-owned Enterprises**

Company selection

The companies subject to assessment on the 2020 DCI were selected on the basis that:

- the company features in the top 100 arms-producing company listings produced by the Stockholm International Peace Research Institute (SIPRI) and/or Defense News; or
- the company is the largest national defence company headquartered in a country with arms exports of at least £10 million, as identified by SIPRI, that otherwise would not have been included in the first criterion.

The countries with the most arms-producing companies in the index are the United States, Russia, the United Kingdom, Japan, France and South Korea, with an overall geographic spread as shown below:



Scoring

For each question, a company receives a score of '2', '1' or '0' depending on the extent to which the company's publicly available information meets the good practice standards of anti-corruption and transparency outlined in the scoring criteria. The final results for each company are presented as a total score out of 100 based on the points awarded in the assessment. These scores correspond to an overall band, which is mapped out using the following classifications:[1]

Band	Commitment to anti-corruption and transparency
A	Very High
B	High
C	Moderate
D	Limited
E	Low
F	Very Low

Company Engagement

Companies were asked to nominate a point of contact at the start of the assessment process, and were invited to engage at multiple stages.

All companies were given the opportunity to provide feedback on a draft version of their assessment to review the evidence, provide feedback and make changes to their publicly available information where appropriate. 44% of companies chose to engage actively in the DCI process by providing feedback in this way.

DCI
Defence Companies Index
on Anti-Corruption & Corporate Transparency

What is the DCI?

The Defence Companies Index on Anti-Corruption and Corporate Transparency (DCI) is the world's leading assessment of anti-corruption transparency in defence companies.

Produced by Transparency International Defence & Security, the DCI provides a unique insight into the level of commitment to transparency and anti-corruption standards in 134 of the world's largest defence companies. By analysing what companies are publicly committing to in terms of their openness, policies and procedures, the DCI seeks to drive reform in the defence sector, thereby reducing corruption and its impact.

Each assessment of a company's anti-bribery and corruption record is based **entirely on publicly available information**. In particular, assessors review the information published on a company's website – including any relevant webpages, reports or documents – to determine the extent to which the company meets the level of commitment to transparency outlined in the scoring criteria. In reviewing company materials, assessors evaluate the completeness and accessibility of the information to promote transparency as an essential tool to mitigate corruption risks.

The DCI is not a measurement of corruption, nor a substitute for internal audit. It does not provide a measurement of the most or least corrupt companies, nor does it indicate that those with a high commitment to transparency are free from corruption risks and vice-versa. The DCI is an assessment of the level of transparency and standards of anti-corruption in a company's publicly available policies, procedures, and documents, which helps to reduce the risk of corruption in the sector overall. The Index focuses solely on information that companies make available in the public domain; it therefore does not attempt to provide a comprehensive overview of all components of a defence company's internal compliance programme or its effectiveness.

[1] For more details on the scoring and calculations, see the DCI Methods Paper. Transparency International Defence & Security, Defence Companies Index on Anti-Corruption and Corporate Transparency 2020: Methods Paper (TI-UK: London), February 2021, https://ti-defence.org/publications/methodology-defence-companies-index-on-anti-corruption-and-corporate-transparency-2020/ [accessed 7 April 2021].

THE RESULTS AT A GLANCE

Most of the world's largest defence companies have publicly available ethics and anti-corruption programmes, with robust policies and procedures in place for employees to follow.

77% of companies show evidence of a formalised approach to anti-corruption, either as a standalone policy or embedded as part of a wider ethics and compliance programme.[2]

85% of companies publicly indicate that they have, at least, a basic whistleblowing system in place.[3]

However, many major defence companies are still not transparent about their procedures to deal with the highest corruption risk areas, such as their supply chains, agents and intermediaries, joint ventures and offsets.

69% of companies show no evidence of a clear policy to regulate the use of agents and address the corruption risks associated with their use.[4]

Only **8%** of companies acknowledge the corruption risks related to offsets and indicate that they have a dedicated body, department, or team in place to manage such projects.[5]

DCI
Defence Companies Index
on Anti-Corruption & Corporate Transparency

Even where policies and procedures do exist, the DCI finds that many companies do not publish any information to indicate that they take steps to assure themselves of their effectiveness and implementation.

Only **19%** of companies worldwide publicly indicate that they measure the effectiveness of their anti-bribery training and communications through specific mechanisms, such as employee surveys.[6]

Only **34%** of companies publish high-level, anonymised, data to indicate that their internal investigation process functions in practice;[7] for example the number of complaints received, number of investigations launched, and number of disciplinary actions taken as a result.

The DCI finds examples of good practice among companies regardless of their varying operational sizes and geographies.

Only five of the 16 companies that score in bands A and B are ranked within the top 10 largest companies by defence revenue, according to the latest rankings published by Defense News.[8] These companies vary greatly in terms of their yearly defence revenue, from US$461 million to US$57 billion, and from positions 1 to 94 in the top 100 rankings.

Companies in bands A and B represent a range of arms-producing geographies, including not only the United States and United Kingdom but also Italy, Germany, South Korea, Switzerland and Finland among others.

[2] Data calculated from results on Question 1.2
[3] Data calculated from results on Question 3.7
[4] Data calculated from results on Question 7.1.1
[5] Data calculated from results on Question 8.1

[6] Data calculated from results on Question 3.3
[7] Data calculated from results on Question 2.6
[8] Defence News, 'Top 100 for 2020', https://people.defensenews.com/top-100/ [accessed 19 March 2021].

RESULTS FOR ALL COMPANIES BY BAND (A-F)

A Very High | B High | C Moderate | D Limited | E Low | F Very Low

A (2)
- Leonardo S.p.A
- Raytheon Technologies

B (14)
- BAE Systems PLC
- Bechtel Corporation
- Boeing
- General Electric Aviation
- Hanwha Aerospace
- Huntington Ingalls Industries Inc.
- Lockheed Martin Corporation
- Northrop Grumman Corporation
- Patria Oyj
- Rolls Royce PLC
- RUAG Holding Ltd.
- Serco Group PLC
- Terma A/S
- ThyssenKrupp AG

C (21)
- AAR Corporation
- Airbus Group
- Babcock International Group PLC
- Cobham Limited
- Day & Zimmerman
- Fincantieri S.p.A
- Fluor Corporation
- Hewlett-Packard Enterprise Company
- Indra Sistemas S.A.
- KBR Inc.
- Kongsberg Gruppen ASA
- L3 Harris Technologies
- Meggitt PLC
- Nammo AS
- Naval Group
- Navantia S.A
- QinetiQ Group
- Rafael Advanced Defense Systems Ltd.
- Rheinmetall A.G
- Saab AB
- Vectrus

D (23)
- Accenture PLC
- Aerojet Rocketdyne
- Aselsan A.S.
- Booz Allen Hamilton Inc.
- CAE Inc.
- Chemring Group PLC
- Damen Schelde Naval Shipbuilding
- Diehl Stiftung & Co. KG
- Elbit Systems
- Embraer S.A
- Fujitsu Ltd.
- Hindustan Aeronautics Ltd.
- Honeywell International
- Israel Aerospace Industries Ltd.
- Korea Aerospace Industries
- Leidos Inc.
- MBDA Missile Systems
- Oshkosh Corporation
- Poongsan Corporation
- Safran S.A
- Textron
- Thales Group
- Ultra Electronics Holdings PLC

E (31)
- AECOM
- Bharat Dynamics
- Bharat Electronics
- CACI International Inc.
- Cubic Corporation
- Daewoo Shipbuilding & Marine Engineering
- Dassault Aviation
- DynCorp International
- Excalibur Army
- General Dynamics Corporation
- IHI Corporation
- IMI Systems Ltd.
- Kawasaki Heavy Industries Ltd.
- Komatsu Ltd.
- LiG Nex1 Co.
- ManTech International Corporation
- Mitsubishi Electric Corporation
- Mitsubishi Heavy Industries Ltd.
- NEC Corporation
- Nexter Group
- OGMA – Indústria Aeronáutica de Portugal SA
- Perspecta
- Rostec State Corporation JSC
- RTI Systems
- Russian Helicopters
- Science Applications International Corporation (SAIC)
- ST Engineering
- Tactical Missiles Corporation
- Toshiba Infrastructure Systems
- United Aircraft Corporation
- United Shipbuilding Corporation

F (43)
- Abu Dhabi Shipbuilding
- Almaz-Antey
- Arab Organisation for Industrialisation (AOI)
- Arsenal JSCo.
- Austal
- Aviation Industry Corporation of China (AVIC)
- Ball Aerospace & Technologies Corporation
- Battelle Memorial Institute
- BelTechExport Company JSC
- CEA Technologies
- China North Industries Group Corporation (NORINCO)
- China State Shipbuilding Corporation
- Curtiss-Wright Corporation
- Denel SOC
- General Atomics
- GKN Aerospace
- Glock
- High Precision Systems
- Hyundai Rotem Company
- Indian Ordnance Factories
- Japan Marine United Corporation
- King Abdullah II Design and Development Bureau
- Krauss-Maffei Wegmann GmbH & Co.
- Massachussetts Institute of Technology (MIT)
- Moog Inc.
- Oki Electric Industry
- Polish Defence Holdings
- PT Dirgantara Indonesia (Indonesian Aerospace)
- Roketsan
- STM Savunma Teknolojileri Muhendislik ve Ticaret A.S.
- Tashkent Mechanical Plant
- Tatra Trucks A.S.
- Telephonics Corporation
- The Aerospace Corporation
- The MITRE Corporation
- Triumph Group Inc.
- Turkish Aerospace Industries
- Ukroboronprom
- United Engine Corporation
- United Instrument Manufacturing Corporation
- Uralvagonzavod
- ViaSat Inc.
- Zastava Arms

KEY RECOMMENDATIONS

1. Transparency International – Defence & Security calls on **companies** to increase corporate transparency through meaningful disclosures of their:
   - corporate political engagement – a particularly high-risk issue in the defence sector – including their political contributions, charitable donations, lobbying and public sector appointments for all jurisdictions in which they are active;
   - procedures and steps taken to detect, prevent and address corruption in the highest risk areas, such as their supply chain, agents and intermediaries, joint ventures and offsets;
   - procedures for the assessment and mitigation of corruption risks associated with operating in high-risk markets, as well as acknowledgement of the corruption risks associated with such practices;
   - beneficial ownership, as well as publicly advocate for governments to adopt data standards on beneficial ownership transparency;
   - all fully consolidated subsidiaries and non-fully consolidated holdings, and to state publicly that they will not work with businesses that operate with deliberately opaque structures; and,
   - nature of work, their countries of operation and the countries of incorporation of their fully consolidated subsidiaries and non-fully consolidated holdings.
2. Transparency International Defence & Security calls on **other private sector actors** to put anti-corruption transparency at the core of on the corporate agenda, as well as to initiate and promote discussions on how to raise standards in their different organisational, national and regional forums in which they participate.
3. Transparency International Defence & Security calls on **investors** to emphasise anti-corruption transparency as an essential cross-cutting issue embedded within Environmental, Social, and Corporate Governance (ESG) initiatives, and to urge the companies in which they hold shares to increase meaningful disclosures of their ethics and anti-corruption programmes.
4. Transparency International Defence & Security calls on **governments** to demand high standards of corporate transparency and reporting from defence sector companies, as well as to address weaknesses in national and regional frameworks through clear guidelines, especially, but not exclusively, in relation to high-risk areas such as supply chains, beneficial ownership, procurement and offset contracting.

WHO CAN USE THIS INFORMATION?

Assessing 134 companies across 56 distinct indicators, the DCI provides a wealth of information on anti-corruption and transparency initiatives in the defence sector. The DCI data is publicly available and can be used by a wide range of actors to increase the accountability of both corporates and governments.

PRIVATE SECTOR:

- **CEOs and board chairs** can use the DCI to put anti-corruption transparency on the agenda, as well as to initiate and promote discussions on how to raise standards within a company's operations.
- **Senior executives and compliance officers** (or equivalent) working in companies assessed as part of the DCI can use it as a framework to improve their programmes, especially in the highest risk areas. These individuals can also use the data in the DCI to learn from other companies and share good practice standards. Senior compliance professionals working for defence sector companies not assessed in the DCI can use it as a reference point when designing or improving their compliance programmes. In addition, those employed by companies entering the defence market can use the DCI to identify the high-level controls they should have in place to counter any sector specific corruption risks.
- **Investors** can use the DCI to urge companies to increase meaningful disclosures of their ethics and anti-corruption programme and to improve their policies and procedures in the highest risk areas. Investors can also enter into constructive dialogue with companies on their anti-corruption and transparency standards as an essential part of ESG initiatives.
- **National and international industry associations** can use the DCI to share good practice and facilitate a constructive dialogue between their members on how to improve standards in their own companies or other regional and national networks. Collective benchmarking in this way helps to reduce risk in the defence sector worldwide, thereby levelling the playing field and increasing market competition.

GOVERNMENTS:

- **Procurement officials in arms-importing countries** can use the DCI to evaluate and assess bidding companies, and to encourage companies to request the same standards from lower-tier subcontractors. Procurement officials can also use the DCI to raise their own expectations and understanding of both the standards and specific risks facing contractors operating in the defence sector.
- **Arms exporting governments** can use the DCI to better understand the least transparent areas of the arms trade and to adopt standards that national companies must follow. Those involved in arms export decisions can also use the DCI to identify anti-corruption controls as part of the licensing process, particularly in the highest risk areas, and to open a dialogue with the defence industry on how to raise standards.

OTHER ACTORS:

- **Civil Society Organisations** can use the DCI as an advocacy tool to raise awareness of the role of corporate transparency to mitigate corruption risks in exposed sectors such as defence, including with investors, trade associations, experts, governments, and companies themselves.
- **Journalists** can use the DCI as a starting point when conducting investigations into specific companies, networks or importing or exporting governments.
- **Employees** can use this information in the public domain to hold companies to account in the course of business and to advocate for improved standards within their company. Employees of subsidiaries or joint ventures can use the DCI to encourage the flow down of standards from the parent company.

THE RESULTS BY SECTION

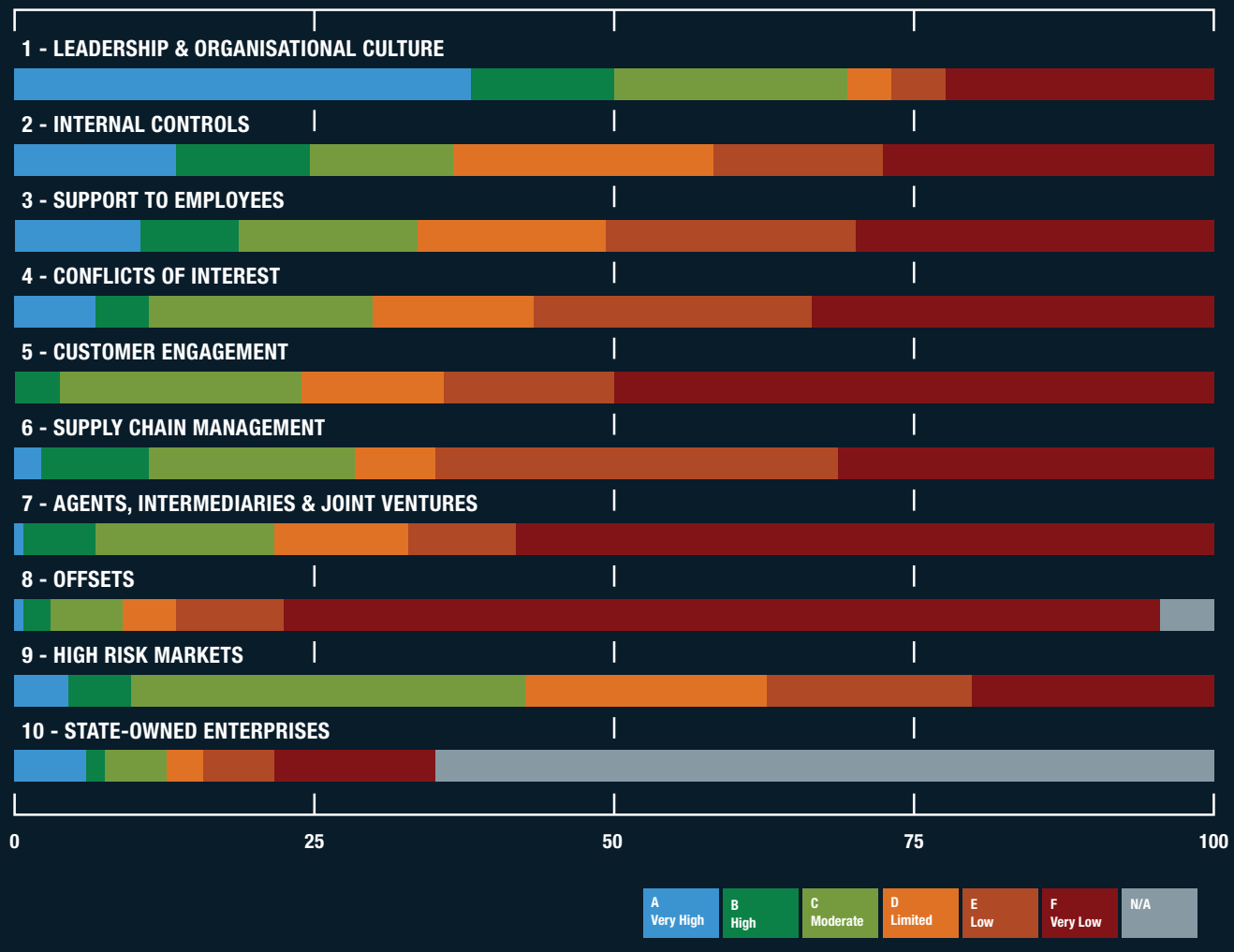
The DCI 2020 is composed of 56 indicators across 10 key risk categories,[9] which TI-DS have identified as areas where stronger controls and greater transparency can reduce corruption risk in the defence sector overall.

The following sections of this report will address each of the 10 key risk categories, providing context on the subject and drawing out key findings from the analysis.

Overall, the results by band (A-F) for all companies across each of the risk categories can be visualised as below:

Band	Commitment to anti-corruption and transparency
A	Very High
B	High
C	Moderate
D	Limited
E	Low
F	Very Low

OVERALL RESULTS BY BAND PER RISK CATEGORY (%)

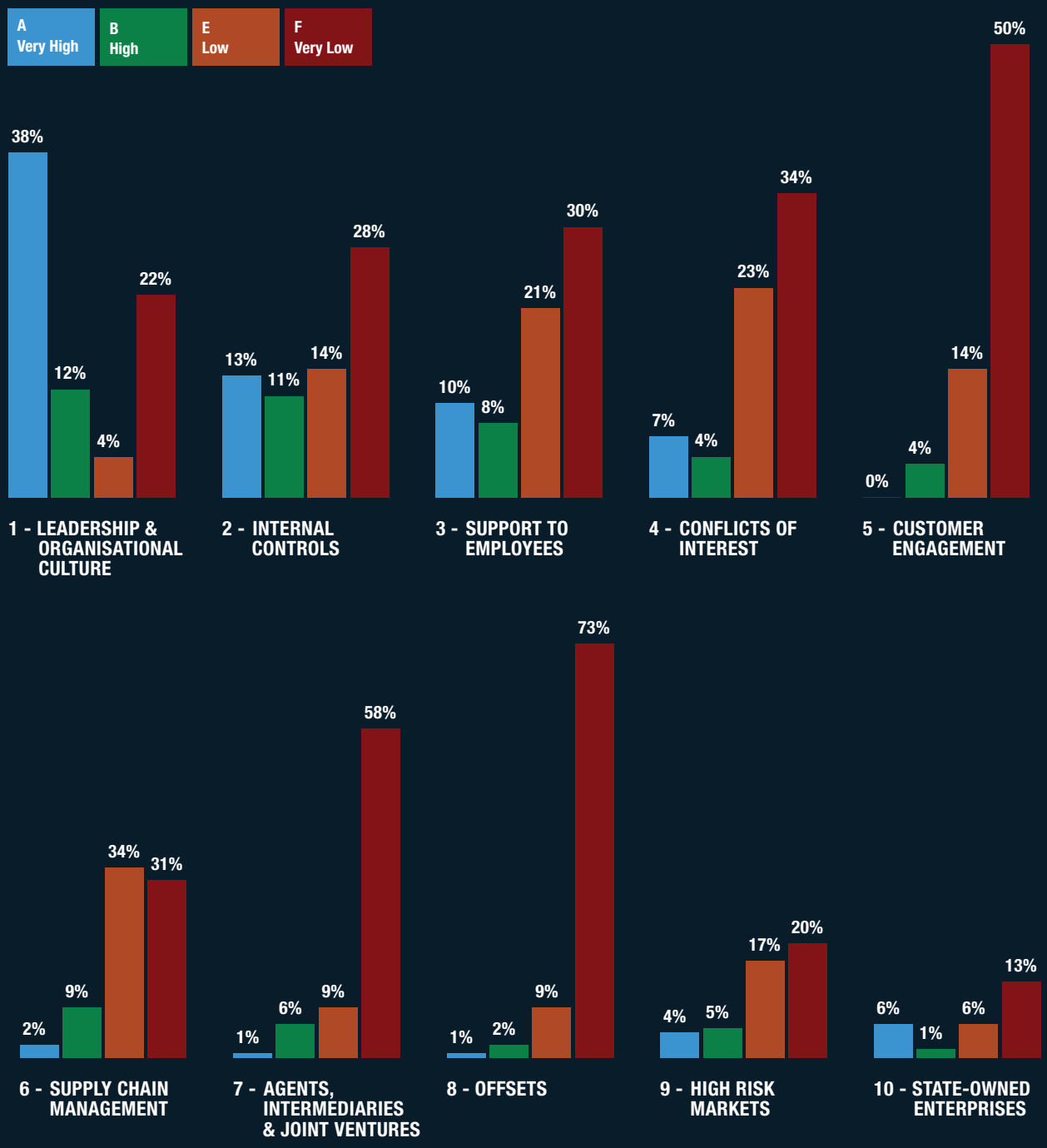


[9] For a full list of the indicators and scoring criteria, see the DCI Questionnaire & Model Answer document. TI-DS, Defence Companies Index on Anti-Corruption and Corporate Transparency 2020: Questionnaire and Model Answers, (TI-UK: London), February 2021, https://ti-defence.org/publications/defence-companies-index-on-anti-corruption-and-corporate-transparency-2020-questionnaire-and-model-answers/ [accessed 7 April 2021].

The results across each of the 10 risk categories indicate that companies on average received higher scores for their policies and disclosures relating to the first four risk categories than the latter six. The first four categories relate to traditional anti-corruption programme components that have featured in compliance literature and numerous enforcement actions in the past two decades, such as leadership commitment, whistleblowing systems, training and conflicts of interest. Meanwhile, the latter risk categories cover standards for emerging and sector-specific risks facing companies operating in the defence and security arena.

The data below visualises this pattern; it contrasts the proportion of companies in the top two bands (A-B) with those in the bottom two bands (E-F) for each risk category.

COMPARING TOP BANDS (A-B) AGAINST BOTTOM BANDS (E-F) PER CATEGORY



1. Leadership and Organisational Culture

Company leadership comes under significant scrutiny in corruption cases. While it might be convenient for companies to point to a few 'rogue employees', accountability – if not always culpability – lies at the top. Effective and ethical supervision at every level of a company is crucial if staff are to have the confidence and support to make ethical decisions, even if it affects the company's bottom line. According to OECD good practice guidance, companies should adopt a comprehensive anti-bribery and corruption policy – prohibiting corrupt practices such as the bribery of foreign officials and facilitation payments – that applies to, and is accessible by, all employees across the organisation. A company's leadership must also go beyond simply publishing a policy; senior management should proactively reinforce the anti-corruption message wherever possible, to publicly demonstrate their personal commitment to anti-corruption and build trust both within and outside of the company.

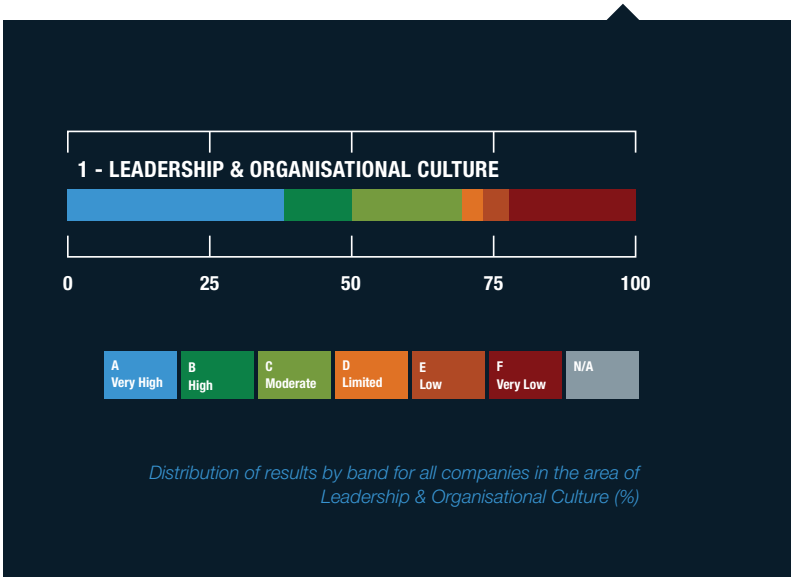
Key findings:

Overall, companies score well in this risk category: **93 out of 134** (69%) companies score in the top three bands for their high-level commitment to anti-corruption (A-C). 39% of companies demonstrate a commitment to anti-corruption through the endorsement of their anti-corruption programme at the highest levels of company leadership,[11] which is the foundation of any ethical corporate culture.

While this is positive, it is concerning that in **23%** of companies there is no evidence of an anti-corruption policy in the public domain.[12] A robust, publicly available anti-corruption policy signals to everyone – both internally to employees and externally to shareholders, investors, suppliers and others – that the company is serious about tackling corruption and that it has clear principles in this regard.

In addition, the seniority of the individual responsible for anti-bribery and corruption within an organisation is a positive indicator of the degree of seriousness with which the company approaches anti-corruption. It is essential that any compliance function is well-resourced and empowered to operate effectively across the business. In addition, making this information public reassures employees that a company's leadership at the highest levels are committed to combatting corruption.

However, many companies also lack evidence of senior oversight and ownership of anti-corruption initiatives. In almost a third (32%) of companies,[13] there is no public evidence that a specific senior individual is responsible for the anti-corruption programme. A further **21%** of companies show some evidence of a responsible individual but it is not clear whether they have a direct reporting line to the body responsible for oversight of the programme.[14]



Distribution of results by band for all companies in the area of Leadership & Organisational Culture (%)

[10] Organisation for Economic Co-operation and Development (OECD), Good Practice Guidance on Internal Controls, Ethics, and Compliance, (OECD: Paris) February 2010, p.3, https://www.oecd.org/daf/anti-bribery/44884389.pdf [accessed 7 April 2021].

[11] Data calculated from results on Question 1.1

[12] Data calculated from results on Question 1.2

[13] Data calculated from results on Question 1.4

[14] Ibid.

2. Internal Controls

Anti-bribery and compliance programmes play a vital role in safeguarding companies against corruption. Embedding anti-corruption ethics into the culture of an organisation and integrating compliance into the business model is essential in both practice and law. Enforcement agencies and prosecutors have made it clear that anti-bribery programmes that exist only on paper will not be sufficient to reduce hefty penalties on the grounds of adequate procedures.[15] Thorough and regular risk assessments are the foundation of successful anti-corruption programmes; the most responsible companies will periodically assure themselves that programmes are still fit for purpose, and will update their policies and initiatives on this basis. The ultimate test of whether a company is meaningfully committed to high ethical standards will be whether it chooses to self-report incidents of wrongdoing to the relevant authorities and to publish data on the functioning of its programme, such as the number of investigations launched and the number of reports received through whistleblowing channels.

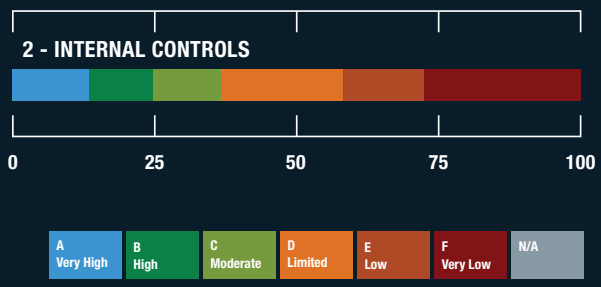
Key findings:

Risk assessments form a key component in the design of any anti-bribery and corruption programme, to ensure that it is tailored to the size, needs and specific risk profile of the business. However, the DCI finds that only **36%** of companies publicly indicate that they conduct dedicated risk assessments on an annual basis and that the results of such assessments are used to update and inform the anti-bribery and corruption programme.[16] A further **27%** show some evidence of risk assessments, but either these are not specifically related to anti-corruption or are not conducted or reviewed on an annual basis.

Internal investigations are the backbone of an effective ethics and anti-corruption programme, yet **22%** of companies do not publish any clear information on their processes for conducting such investigations.[17] Evidence of a robust and transparent process for internal investigations acts as a strong, public indicator of a company's willingness to address possible bribery and corruption concerns within its divisions.

Moreover, over half (**51%**) of companies in the DCI show no evidence of a clear public commitment to providing whistleblowers with updates on the outcome of investigations if they so wish.[18] Informing and providing regular feedback to employees – and any third party – on their report is essential to reassure individuals that their concerns will be acted upon, and signals to all parties that the company is serious in pursuing all allegations.

In addition, only one third (**34%**) of companies publish high-level, anonymised data on their internal ethics investigations,[19] such as the number of complaints received, number of investigations launched and number of disciplinary actions taken as a result. Placing even such high-level and anonymised information in the public domain acts as a clear indicator of the proper functioning of the programme, and reassures both employees and external stakeholders that the company is willing to take necessary action to tackle ethical violations.



Distribution of results by band for all companies in the area of Internal Controls (%)

[15] Transparency International Defence & Security, Out of the Shadows: Promoting Openness and Accountability in the Global Defence Industry (TI-UK: London), September 2018, p.5-6, 10, https://ti-defence.org/publications/out-of-the-shadows/ [accessed 7 April 2021].

[16] Data calculated from results on Question 2.1

[17] Data calculated from results on Question 2.3

[18] Ibid.

[19] Data calculated from results on Question 2.6

3. Support to Employees

Robust internal controls do not exist in isolation; these controls need to be accessible and tailored to all employees, across all divisions and areas of operation. Ethics training forms a central part of this support system, promoting an understanding of corruption, bribery and the type of ethical business conduct expected from employees, which contributes to their capacity to identify, avoid and resist unethical behaviour. However, training alone is insufficient. Several of the most recent investigations into defence corruption are a result of reports from whistleblowers;[20] yet in many cases, employees may be reluctant to do the right thing for fear of retaliation or may simply not know how or where to raise their concerns. Defence companies should consider whether they are doing enough to support employees who refuse to behave unethically. Companies should, at minimum, adopt an explicit policy of non-retaliation against whistleblowers in all circumstances, as well as establish accessible whistleblowing channels and regularly monitor their use.[21]

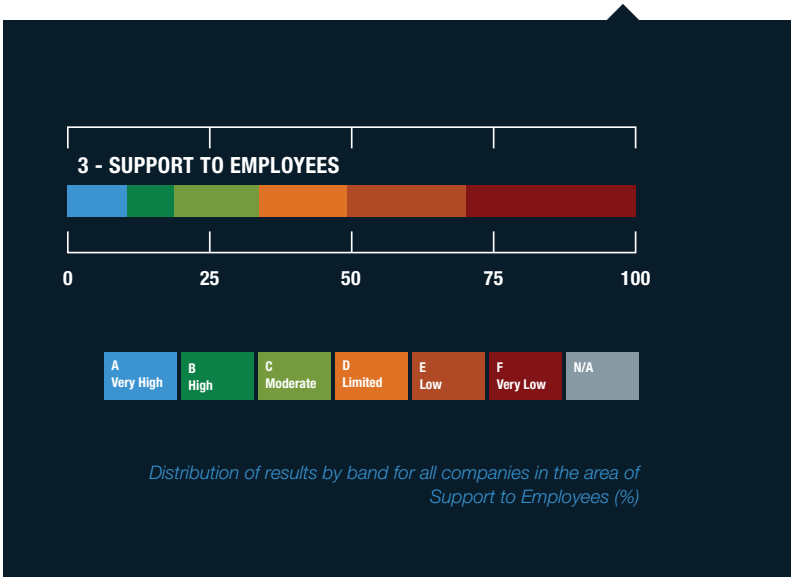
Key findings:

Although many companies provide information on their anti-corruption training activities for employees, a significant majority (**71%**) fall short of good practice standards in at least one way.[22] This includes: not clearly specifying that such training highlights the whistleblowing options available to employees; not indicating that employees must refresh their learning on a regular basis; or not clarifying whether they provide such training to all employees in all countries of operation and relevant languages.

In addition, nearly half (**46%**) of companies show no evidence of providing tailored anti-corruption training to employees based on an assessment of their potential exposure to corruption risk or their role in ensuring anti-corruption measures are appropriately implemented.[23] These positions could include, for example, those working in sales, government relations, middle management or on the board of directors. Recognising the different levels of risk facing employees in different positions, and adapting anti-corruption training accordingly, is an essential part of ensuring that all employees within a company are properly equipped to act ethically in the course of business.

A key finding is that the majority of companies do not publish any information to indicate that they actively review and measure the effectiveness of their training and communications. Fewer than 1 in 5 (**19%**) companies publicly demonstrate that they have clear procedures in place to measure the effectiveness of anti-bribery training and communications.[24] This is despite the importance of monitoring and reviewing anti-bribery training and communications to ensure that they are impactful, appropriate and functioning as intended.[25]

Companies also publish very little information on incentive structures for employees. Three-quarters (**75%**) of companies fail to mention anything about the way that they incentivise their employees to encourage ethical behaviour,[26] while **19%** provide some information on this subject,[27] and only **5%** publish comprehensive details of their approach to establishing incentive structures.[28] These details are a crucial indicator of corporate culture; by designing reward structures in a way that promotes ethical behaviour and discourages corrupt practices, companies signal to their employees that they value ethical behaviour.



Distribution of results by band for all companies in the area of Support to Employees (%)

[20] For example, the ongoing GPT Special Project Management case in the UK. See: Transparency International Defence & Security, Out of the Shadows, p.11 (cit. 15)

[21] Transparency International UK, Open Business: Principles and guidance for anti-corruption corporate transparency, (TI-UK: London), March 2020, p.25, https://www.transparency.org.uk/publications/open-business-anticorruption-governance-disclosure-guidance [accessed 19 March 2021].

[22] Data calculated from results on Question 3.1

[23] Data calculated from results on Question 3.2

[24] Data calculated from results on Question 3.3

[25] Transparency International UK, Make It Count: Understanding the current and emerging trends in measuring the effectiveness of corporate approaches to anti-corruption (TI-UK: London), May 2021, https://www.transparency.org.uk/make-it-count-anti-bribery-corruption-measuring-effectiveness-guidance-companies [accessed 21 May 2021].

[26] Data calculated from results on Question 3.4

[27] Ibid.

[28] Ibid.

Spotlight on: Whistleblowing

Whistleblowing refers to any disclosure made in the public interest by an employee, director or external person, in an attempt to reveal neglect or abuses within the activities of an organisation (or one of its business partners) that threaten the public interest, as well as its integrity and reputation.[29]

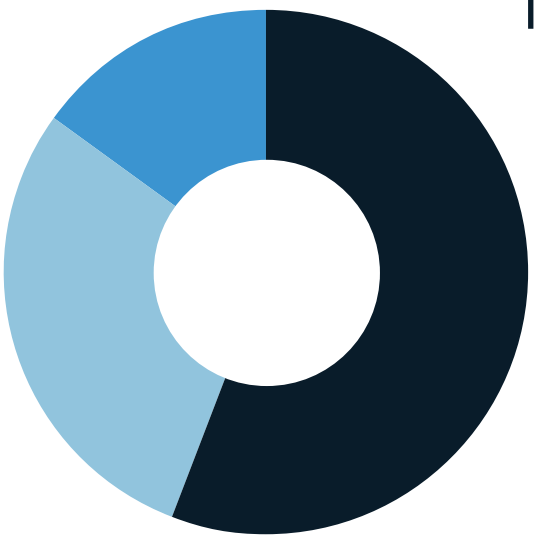
Despite the widespread international recognition of the importance of whistleblowing systems,[30] the DCI finds that **15%** of companies show no public evidence of any whistleblowing hotline for employees to report potential bribery and corruption concerns.[31] Of the **85%** that do offer reporting mechanisms, it is not clear in over a third (38%) of cases that such channels are available for use by all employees in all relevant jurisdictions and languages, including those of suppliers and third parties.[32] Companies are responsible for providing visible, accessible and effective whistleblowing systems for all employees not only to give confidence to such employees that they can speak up if necessary, but also to detect any signs of possible wrongdoing within the organisation.

The DCI reveals that **56%** of companies provide both internally and externally operated whistleblowing channels,[33] while **29%** provide internal channels only. An external channel in this context refers to any reporting mechanism controlled by an entity outside of the management chain, for example a hotline operated by an independent third party or a direct line to a relevant ombudsman.

The most responsible companies will go beyond internal only systems and provide an external, independent reporting channel for any individuals to report concerns without fear of negative repercussions.

Finally, a key component of any whistleblower protection system is non-retaliation. Companies around the world have an ethical – and often legal – responsibility to ensure that whistleblowers do not suffer negative treatment for raising concerns in good faith. Despite this, the DCI finds that almost a third (**31%**) of companies show no evidence of a public commitment to protect whistleblowers from retaliation.[34] Placing such a commitment in the public domain signals to all entities interacting with the company – including employees of suppliers and other third parties – that any concerns will be taken seriously, thereby building employee trust and increasing the chance that employees will speak up when necessary.

DIFFERENT TYPES OF WHISTLE-BLOWING CHANNELS PROVIDED BY COMPANIES, BASED ON PUBLICY AVAILABLE INFORMATION



NO EVIDENCE OF A WHISTLEBLOWING CHANNEL
15%

INTERNAL CHANNEL(S) ONLY
29%

INTERNAL AND EXTERNAL CHANNELS
56%

[29] Transparency International UK, Open Business, p.9 (cit. 21)

[30] See recommendations in, for example: OECD, Guidelines for Multinational Enterprises; OECD, Good Practice Guidance on Internal Controls, Ethics, and Compliance; Transparency International UK, Open Business.

[31] Data calculated from results on Question 3.7

[32] Ibid.

[33] Ibid.

[34] Data calculated from results on Question 3.6

4. Conflicts of Interest

Conflicts of interest are a major risk in the defence sector, where a small number of companies compete for high-value, opaque and relatively infrequent contracts with a small number of customers. The movement of employees between the public and private sector – also known as the 'revolving door' – also presents significant risk. Individuals who have recently joined a company from public sector positions may be able to influence their former colleagues to make policy or procurement decisions that favour their new employer. At a minimum, companies can manage these risks through comprehensive policies and procedures to identify and manage actual, potential and perceived conflicts of interest. A designated body, department or senior individual should hold responsibility for overseeing such declarations, as well as deciding which measures will be taken to mitigate any risks identified. Beyond this, responsible companies must implement clear policies covering the movement of employees between the public and private sector in all jurisdictions in which they operate, to reduce the underlying conflict of interest risks posed by the 'revolving door'.

Key findings:

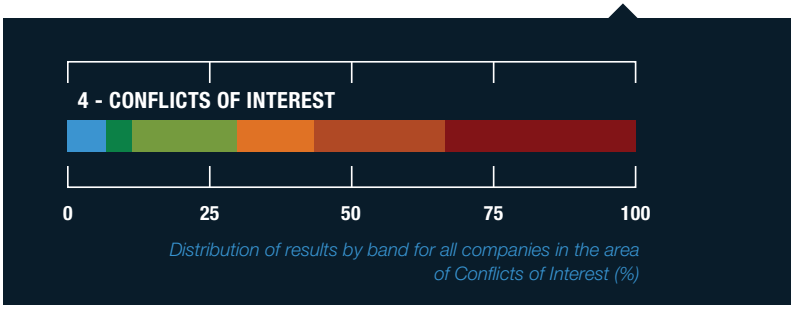
Although many companies show some evidence of having policies in place that recognise the corruption risks associated with conflicts of interest, only **32%** of companies publish comprehensive information on this subject, including the specific types of relationships that may pose a conflict in actual, potential or perceived terms.[35] A robust conflict of interest policy should cover, at minimum, employee relationships, financial interests, outside employment and relationships with government officials; yet the majority of companies assessed by the DCI fall short on one or more of these areas based on their publicly available information.

In addition, few companies publish further information on how they handle such conflicts of interest when they do arise. The DCI finds that **39%** of companies show little to no public evidence of procedures in place to identify, manage and declare conflicts of interest,[36] such as senior review of actual or potential conflicts, oversight of case information and ensuring that all declarations are appropriately documented and recorded in a central register.

Despite the risks associated with the 'revolving door', the majority (**60%**) of companies show no public evidence of policies and procedures to regulate the appointment of employees from the public sector.[37] Only **6%** of companies publish comprehensive information on this issue,[38] while the remaining **34%** show some evidence of a policy that falls short in some way.[39] In such a high-risk and opaque sector as defence, that by its nature has close ties with senior public figures, it is not enough to rely on governments to set their own regulations. The most responsible companies should proactively take measures to reduce the possible risks from public sector appointments, such as implementing cooling-off periods and placing restrictions on activities that may present a conflict of interest.[40]

Of the companies that do publish comprehensive information on the appointment of employees from the public sector, **6 out of 8** are headquartered in the United States.[41] In fact, over half (57%) of companies that provide any information on this subject are based in the US. This can be – at least in part –explained by the existence of clear 'revolving door' regulations in the United States, which stem from a political system in which private and public interests are more closely intertwined than in many other jurisdictions due to the prevalence of corporate lobbying and political financing.[42] It is also important to note that the companies assessed by the DCI that are headquartered in the US are overall larger in operations and revenue than other countries represented, leading them to have more interactions with government officials and therefore increased risk.

The DCI finds that a significant majority (**86%**) of companies do not provide any information to indicate whether or not they contract serving politicians to act on their behalf, nor do they publish details of such individuals where appropriate.[43] In contrast, 11% of companies publish a clear statement that they do not engage or contract the services of current politicians in the course of business.[44] While some jurisdictions regulate this practice, the most responsible companies should proactively provide details of these engagements or clearly state that they do not engage such individuals as a matter of policy. This is especially relevant for multinational enterprises operating in jurisdictions where regulations may be lacking or where oversight and enforcement mechanisms are weak.



Distribution of results by band for all companies in the area of Conflicts of Interest (%)

[35] Data calculated from results on Question 4.1

[36] Data calculated from results on Question 4.2

[37] Data calculated from results on Question 4.3

[38] Ibid.

[39] Ibid.

[40] Transparency International UK, Open Business, p.46 (cit. 21)

[41] Ibid.

[42] Lee Drutman, 'How Corporate Lobbyists Conquered American Democracy', (The Atlantic, 20 April 2015), https://www.theatlantic.com/business/archive/2015/04/how-corporate-lobbyists-conquered-american-democracy/390822/ [accessed 21 May 2021]; Bill Wallheimer, 'Should we stop the 'revolving door'?' (Chicago Booth Review, 7 August 2017), https://review.chicagobooth.edu/public-policy/2017/article/should-we-stop-revolving-door [accessed 21 May 2021].

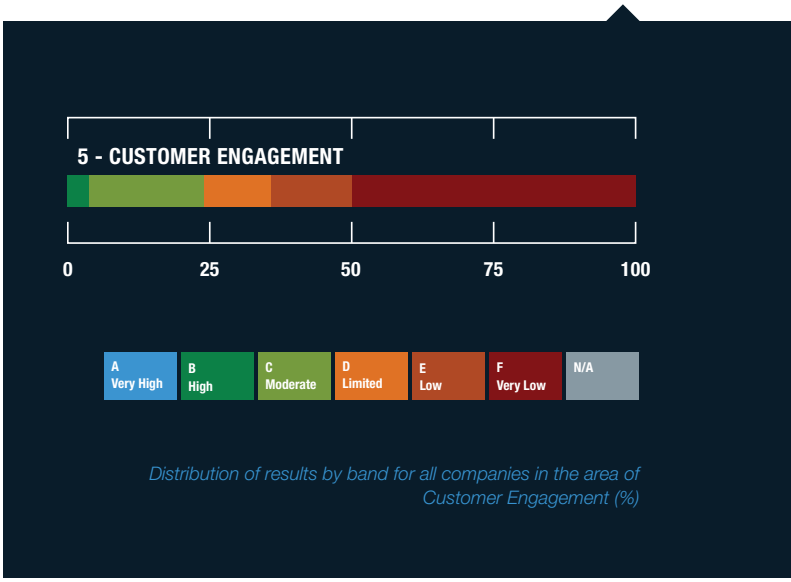
[43] Data calculated from results on Question 4.4

[44] Ibid.

5. Customer Engagement

Closed-door meetings between public officials and defence companies can be legitimate and sometimes necessary, but they also create opportunities for bribery, influence peddling and the development of relationships that could lead to potential or actual conflicts of interest. Arms manufacturers may seek to exert influence on national governments through strategic lobbying, to increase their likelihood of being selected for a specific high-value tender or to influence policymaking. While some of these interactions may be legitimate business strategies, some may jeopardise the integrity of public office and decision-making. Furthermore, charitable donations, political contributions, gifts and hospitality can all be used as vehicles for bribery and corruption if not closely monitored or regulated. The risks associated with inappropriate customer engagement are best mitigated through robust procedures and increased public disclosure. Responsible companies should adopt clear policies to regulate political contributions, charitable donations, sponsorships, gifts, hospitality, expenses and lobbying, to protect against the exertion of undue influence on policymakers.

It is crucial that these companies implement robust policies and procedures on gifts and hospitality, both to reduce their own risk exposure and to signal to outside parties – customers, regulators, third parties, sub-contractors and investors – that unethical behaviour in this area is not tolerated.



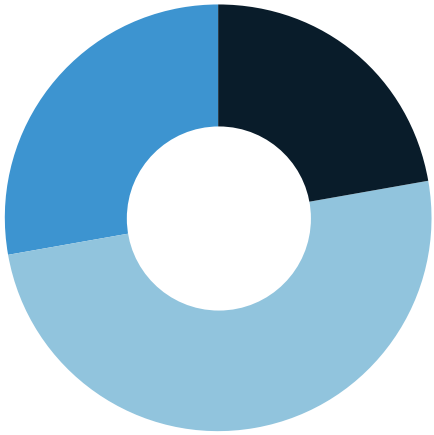
Distribution of results by band for all companies in the area of Customer Engagement (%)

Key findings:

The DCI finds that over half (**55%**) of companies do not publish any information about their charitable donations and sponsorships.[45] A minority (**45%**) of companies publish some basic information on their policies to regulate such contributions,[46] alongside some narrative details of their donations made, yet few publish a clear policy with specific controls to mitigate risks, or a full list of all donations made. When not appropriately transparent and regulated, charitable contributions and sponsorships can act as vehicles for active or passive bribery in the form of kickbacks or undue influence. Greater transparency helps to mitigate the risks that such contributions may fuel or facilitate corrupt activity and helps improve trust in a company's community participation.

In addition, only **22%** of companies publish comprehensive procedures to regulate the giving and receipt of gifts and hospitality in the course of business.[47] The most responsible companies show evidence of a clear policy establishing financial limits and approval procedures for different types of promotional expenses, as well as a central gifts register and measures to address the risks associated with gifts to or from public officials. Half of companies (**50%**) assessed show some evidence of policies and procedures on gifts and hospitality but fall short in some way,[48] while **28%** show little to no evidence of addressing the risks associated with these practices.

COMPANY APPROACHES TO GIFTS AND HOSPITALITY, BASED ON PUBLICLY AVAILABLE INFORMATION



COMPREHENSIVE GIFTS AND HOSPITALITY PROCEDURES AND REGISTER
22%

SOME EVIDENCE OF A GIFTS AND HOSPITALITY PROCEDURES
50%

LITTLE TO NO PUBLIC EVIDENCE OF A GIFTS AND HOSPITALITY PROCEDURES
28%

[45] Data calculated from results on Question 5.1.3
[46] Ibid.
[47] Data calculated from results on Question 5.3.1
[48] Ibid.

Spotlight on: Traditional Lobbying

When conducted responsibly, lobbying can be a legitimate and beneficial activity. It may allow companies to provide policymakers with information, expertise and resources, as well as stimulating and contributing to public debate.[49] However, lobbying is also an area regarded with suspicion by the public and subject to high levels of opacity, and therefore a heightened risk of corruption. The DCI finds that companies publish surprisingly little information on their approaches to mitigating corruption risks associated with traditional lobbying.

A majority (**60%**) of the companies assessed on the DCI show no public evidence of policies and procedures to appropriately regulate and reduce corruption risks in lobbying activities.[50] Only **12%** of companies clearly demonstrate a responsible lobbying approach with specific controls and oversight mechanisms in place to regulate such activities when conducted by internal, external and association lobbyists.[51] Lobbying the political process presents inherent risks and opportunities for the perceived or actual exertion of undue influence, and these risks increase when a company uses third-party lobbyists (through possible conflicts of interest, for example) and call for robust due diligence procedures. It is crucial that companies have robust lobbying guidelines in place to retain control of the process, ensure that lobbyists are behaving ethically, and reduce the risk of inappropriate influence.

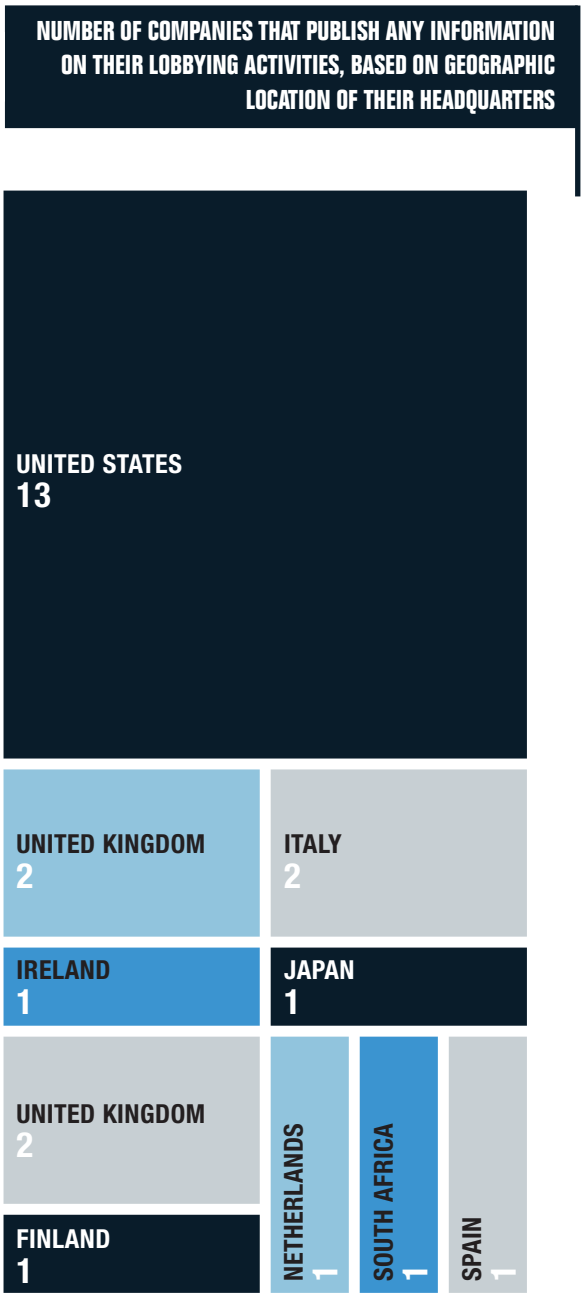
Very few companies publish *any* information on their global lobbying activities and expenditure, beyond high-level and legally required disclosures. Only **6 out of 130** (5%) provide comprehensive information on the aims and topics on which they lobby.[52]

In the United States, only **2 out of 39** of companies publish any information on their lobbying activities beyond the requirements set by US laws,[53] and no company publishes information on their global lobbying expenditure beyond these obligations. Similarly, while many companies in the European Union publish direct links to their mandated disclosures under the EU Transparency Register,[54] only **4 out of 26** companies headquartered in the EU go beyond this to publish information on their lobbying aims and activities on a national or wider international level.

This pattern also extends to lobbying expenditures: only **14%** of companies assessed in the DCI publish any information on the amount they spend on advancing their public policy positions.[55]

Where companies do publish some details of their expenditure, in the majority of cases, this data is limited to a high-level figure or only applies to the jurisdiction in which the company is headquartered.

Responsible companies – especially those engaged in formal and informal lobbying in multiple jurisdictions – should be transparent about their public policy aims and expenditures everywhere they lobby to increase public trust, reassure investors and shareholders, and reduce the risk of corruption or perceived corruption in the sector overall.



[49] OECD, Lobbying in the 21st Century: Transparency, Integrity and Access (OECD: Paris), May 2021, https://www.oecd.org/governance/lobbying-in-the-21st-century-c6d8eff8-en.htm [accessed 21 May 2021].

[50] Data calculated from results on Question 5.2.1

[51] Ibid.

[52] Data calculated from results on Question 5.2.2

[53] Ibid.

[54] European Commission and European Parliament, EU Transparency Register, https://ec.europa.eu/transparencyregister/public/homePage.do [accessed 19 March 2021].

[55] Data calculated from results on Question 5.2.3; Transparency International UK, Open Business, p.45 (cit. 21)

6. Supply Chain Management

Companies in the defence sector must navigate complex supply chains, involving multiple entities with different corporate structures and operating across different geographies and sectors. Corruption in the supply chain can manifest in both supplier selection and contract delivery. Governments around the world are also increasingly intervening in supply chains, requiring the use of domestic suppliers or single-source tenders, in order to create jobs, retain investment, and enhance their domestic defence industry. In many cases, this market intervention takes place in regions of the world where corporate ethics are often lacking and regulation is weak. As tiers of suppliers become more remote from the principal contractor, the opportunities for corruption become greater, with less clarity over issues ranging from conflicts of interest to beneficial ownership and financial transparency.

The most responsible companies will assure themselves of every supplier's beneficial ownership, ensure that each company's anti-bribery and corruption policies are, at minimum, comparable to their own ethical standards, and will assist them in improving their standards where necessary. Good practice means including anti-bribery and corruption clauses in all contracts with significant external suppliers,[56] including clauses specifying audit and termination rights, and encouraging subcontractors further down the chain to adopt equally high standards.

Key findings:

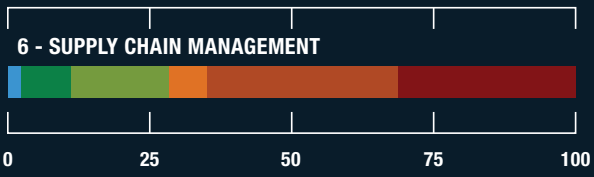
Despite the possible bribery and corruption risks associated with supply chain management, the DCI finds a surprising lack of transparency in this area. Only **28%** of companies score in the top three bands (A-C) for their policies and transparency in relation to supply chain management, with the remaining **72%** falling in the bottom three bands (D-F) across all indicators in this risk category.

Fewer than half (**49%**) of companies publicly indicate that they conduct any level of due diligence on suppliers.[57] Only **8%** of companies publish clear information on their due diligence process for suppliers,[58] specifying that this includes identifying beneficial ownership and provisions to renew such checks throughout the business relationship. Due diligence is a basic element of any risk mitigation system, and is especially pertinent in identifying and addressing any bribery and corruption risks. Given the high-risk nature of the defence sector, transparency around supply chain management – including on due diligence procedures – signals to investors, potential suppliers, government procurement officials, and other stakeholders that the company is a business partner that leads with integrity.

Almost a quarter (**24%**) of companies publicly indicate that they have procedures in place to take active steps to 'flow down' their anti-bribery and corruption standards to subcontractors,[59] yet **53%** show no clear evidence of such initiatives.[60] With supply chains and enforcement actions spanning multiple jurisdictions, the concept of 'flowing down' an adequate level of anti-bribery and corruption standards to sub-contractors has become an important feature of responsible business conduct. The DCI finds that companies adopt a range of different approaches to this in practice, for example by providing tailored anti-corruption training to suppliers, by including contractual clauses, or by making public a set of supplier principles that sets the minimum standards of ethical behaviour expected throughout the supply chain.

Very few companies (**7%**) show any public evidence that they record and publish high-level anonymised data on their internal ethics investigations in relation to suppliers,[61] such as the number of complaints received, number of investigations launched and number of disciplinary actions taken as a result. The vast majority (**93%**) provide no information on this subject. Placing even such basic and high-level information in the public domain acts as an indicator of the proper functioning of the programme, and reassures external stakeholders that the company is willing to take necessary action to tackle ethical violations.

Companies are responsible for promoting good practice within their supply chain. Robust anti-corruption measures throughout the supply chain serve not only to reduce the risk of misconduct and of any potential legal or reputational damage, they also foster productivity and long-term sustainability. Despite this, the DCI finds that many companies do not have appropriate systems in place to manage risks and cascade a culture of anti-corruption throughout their supply chains.



Distribution of results by band for all companies in the area of Supply Chain Management (%)

[56] See, for example: Transparency International UK, '13. Managing Third Parties: Guidance', Global Anti-Bribery Guidance, https://www.antibriberyguidance.org/guidance/13-managing-third-parties/guidance#10 [accessed 7 April 2021]; Transparency International Defence & Security, Out of the Shadows, p.14 (cit. 15)

[57] Data calculated from results on Question 6.2

[58] Ibid.

[59] Data calculated from results on Question 6.4

[60] Ibid.

[61] Data calculated from results on Question 6.5

7. Agents, Intermediaries and Joint Ventures

The use of third parties, intermediaries, and agents in defence procurement is widely recognised as one of the most significant and pervasive bribery and corruption risks in defence. A cross-sectoral OECD study highlighted that three out of four foreign bribery cases examined between 1999 and 2014 involved the improper use of intermediaries. According to the study, the majority of these cases involved the payment of bribes to obtain public procurement contracts. As such, companies that choose to use such third parties despite the risks – especially in the often secretive and opaque defence sector – must implement stringent processes to manage them. Conducting enhanced due diligence on all such business associates is an important step to reduce these risks. At minimum, this should include checks to determine whether the third party (including agents, intermediaries and joint ventures) has any actual or potential conflicts of interest, past involvement in dishonest business practice, or opaque beneficial ownership. Companies should also include formal anti-bribery and corruption clauses in all contracts with third parties, providing the company with audit and termination rights.

Key findings:

Compliance professionals, particularly in the defence sector, consistently identify agents and intermediaries as an area of significant third-party risk. Despite this, almost half (**48%**) of companies assessed by the DCI publish no clear information on their approach to reduce the corruption risks associated with the use of agents.[63]

In addition, only **20%** of companies publicly indicate that they have robust procedures in place to conduct anti-bribery and corruption due diligence on agents and intermediaries.[64] These companies go beyond simply stating that they conduct due diligence on these third parties, by committing to engage only where risks identified in due diligence can be mitigated and to refreshing these checks every two years. A third (**33%**) of companies show some evidence of due diligence procedures,[65] however a larger proportion (**47%**) provide no publicly facing commitment to upholding these standards.[66]

An essential part of any third-party due diligence process involves establishing ultimate beneficial ownership.[67] This is especially relevant for the use of agents in the defence sector, where opaque ownership structures can mask conflicts of interest or links to politically exposed persons (PEPs). However, the DCI finds that only **10%** of companies demonstrate the use of a risk-based beneficial ownership verification policy.[68] A large majority (**75%**) of companies show no clear evidence of procedures to establish the ultimate beneficial ownership of agents,[69] or do not publicly commit to act on the results of such due diligence through review or possible termination of a relationship in cases where risks cannot be mitigated.

What are agents, and why do they pose a risk?

Transparency International Defence and Security defines agents as individuals or entities authorised to act for, or on behalf of, a company to further its business interests, for example in sales or marketing, and in (or with) a foreign country or foreign entity. The terms 'agent', 'advisor' and 'broker' are often used interchangeably, but the authority to act on behalf of the company's interests in the pursuit of contracts distinguishes this type of third party from other intermediaries, such as consultants and lobbyists.

Although agents can play a vital and legitimate role in defence transactions, there is substantial evidence from recent and historic investigations that such actors can facilitate and engage in corrupt activity. In particular, agents pose inherent risks due to their ability to act independently to serve their own interests and due to the close links they often have with decision-makers, which can lead to inappropriate influence on the procurement process.[70]

Through ongoing monitoring of third parties, especially agents and intermediaries, companies develop a better understanding of their risk profile which, in turn, helps them implement appropriate mitigation measures and reduce the risk of adverse reputational or legal consequences. In addition:

> "By disclosing evidence of this due diligence, the company will also gain the trust of stakeholders, including investors, consumers and employees. These stakeholders will feel confident that third party relationships have been thoroughly vetted, and thus will feel more

[62] OECD, OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials, (OECD Publishing: Paris), 2014, p.10, https://read.oecd-ilibrary.org/governance/oecd-foreign-bribery-report_9789264226616-en#page10 [accessed 19 March 2021]

[63] Data calculated from results on Question 7.1.1

[64] Data calculated from results on Question 7.1.2

[65] Ibid.

[66] Ibid.

[67] World Economic Forum, Good Practice Guidelines on Conducting Third-Party Due Diligence (WEF: Geneva), April 2013, p.7, 10-11, https://www.weforum.org/reports/good-practice-guidelines-conducting-third-party-due-diligence [accessed 7 April 2021]; Transparency International UK, Open Business, p.26, 31 (cit. 21)

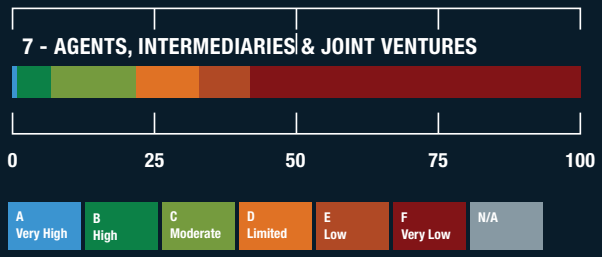
[68] Data calculated from results on Question 7.1.3

[69] Ibid.

[70] Transparency International Defence & Security, License to Bribe? Reducing corruption risks around the use of agents in defence procurement, June 2016, https://ti-defence.org/publications/licence-to-bribe-reducing-corruption-agents-defence-procurement/ [accessed 19 March 2021].

confident that third party risks have been reduced."[71]

While some companies publish information on their policies and procedures to regulate these potential risks, even fewer companies are transparent about the way in which they incentivise agents. Out of 129 relevant global defence firms, only 11 (**9%**) publish comprehensive information on the way in which they pay their agents to promote ethical behaviours and discourage corrupt practices.[72] Mechanisms to reduce risks in this area include implementing a threshold on sales-based commissions to agents, making payments in stages based on clear milestones and only making payments into local bank accounts. Yet the majority (**65%**) of companies show no evidence of these standards in their publicly available materials.[73]



Distribution of results by band for all companies in the area of Customer Engagement (%)

Spotlight on: Joint Ventures

Joint venture partnerships are increasingly common in the defence sector worldwide. In many cases, companies may be minority partners working in new and unfamiliar markets, and may be required to engage with enterprises where the state has a controlling interest. The nature of joint ventures in the defence sector therefore presents a unique set of challenges that companies must address through well-defined anti-bribery and corruption controls. It is essential that companies have comprehensive and transparent systems in place to mitigate corruption risks in joint ventures and to signal to potential partners the standards of behaviour they expect.

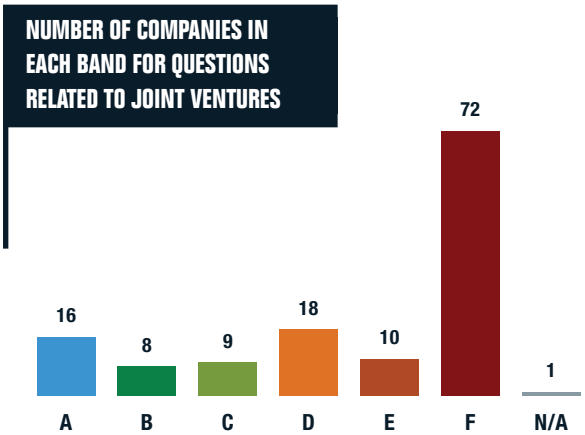
What is a joint venture?

A joint venture is a business entity or project created by two or more companies. A joint venture can be temporary for the purpose of fulfilling a contract or part of a long-term partnership, and certain companies may be involved in multiple joint ventures at any given time.

Over half (**54%**) of companies assessed on the DCI show no evidence of policies or procedures to reduce corruption risks in joint ventures,[74] scoring zero on all indicators in this area.

Only **11%** of companies show evidence of robust procedures in place to conduct anti-bribery and corruption due diligence when entering into joint venture partnerships and on an ongoing basis throughout the contractual relationship.[75] For the majority of companies (**58%**),[76] it is either not clear or there is no evidence that they have systems in place to conduct anti-corruption due diligence on joint ventures.

Similarly, only **25%** of companies publicly commit to incorporating ethical principles into joint venture partnerships and to including anti-bribery and corruption clauses in their contracts with such partners, with explicit audit and termination rights.[77] Anti-corruption clauses in third party contracts reinforce the anti-corruption message, provide important leverage in the event of suspected misconduct, and help to reassure both the contracting company's leadership and outside parties that any corrupt practices will be detected and controlled. Given the level of potential risk associated with joint ventures, it is concerning that the majority (**59%**) of companies show no clear evidence of specific anti-corruption clauses in these contracts.[78]



[71] Transparency International UK, Open Business, p.26 (cit. 21)
[72] Data calculated from results on Question 7.1.5
[73] Ibid.
[74] Data calculated from results on Questions 7.2.1, 7.2.2 and 7.2.3
[75] Data calculated from results on Question 7.2.1
[76] Ibid.
[77] Data calculated from results on Question 7.2.2
[78] Ibid.

8. Offsets

Offsets represent one of the most opaque practices in the defence sector. The frequent lack of transparency and adequate oversight makes them one of the most profound areas of corruption risk for the sector. The opacity of offset contracting is exacerbated by its complexity, where value credits and multipliers negotiated behind closed doors can distort the market value of the transaction.[79] Although offset obligations are often determined by the purchasing government, there are several steps that companies can take to increase transparency and minimise the associated corruption risks. At a minimum, companies should publicly acknowledge the corruption risks associated with offset contracting and indicate that all offset partners or projects are subject to enhanced due diligence procedures. The most responsible companies will be transparent about their involvement in such projects.

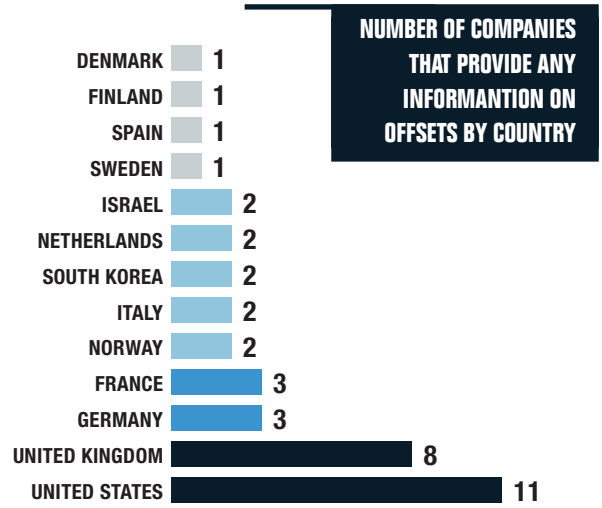
Key findings:

Overall, the world's top defence companies publish almost no information on their involvement in offset contracting. **70%** of companies receive a score of zero for all indicators that relate to offsets,[80] suggesting that they either do not address offsets in their publicly available materials or provide very little information on the subject.

Of the companies that publish some information on their anti-corruption measures to manage the corruption risks associated with offsets, only **5 out of 41** (12%) receive a score of more than 50% of the available points.[81]

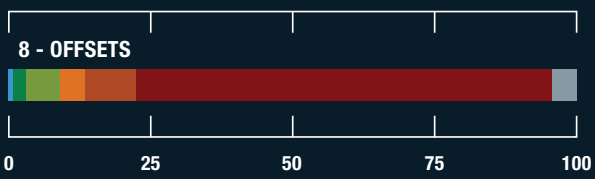
Two companies publicly state that they do not engage in offset contracting in the conduct of business, and show no evidence of engaging in such practice in their publicly available information.[82] Going beyond this, **one** company publishes a statement to indicate that it does not engage in offset contracting as a matter of policy, due to the associated corruption risks.[83]

Almost three quarters (**72%**) of companies assessed by the DCI provide no public commitment to conduct anti-bribery and corruption due diligence on all aspects of an offset obligation. Only a very small proportion (**8%**) of companies publicly acknowledge the corruption risks associated with offsets and indicate that a dedicated team is responsible for their management,[84] while only **6%** provide clear information on their due diligence process for offset obligations.[85] Given the corruption risks associated with offset contracting, companies should strengthen their policies and disclosures in this area, as well as working with government and industry partners to promote transparency in offset contracting.



What is an offset?

Offsets in the defence sector are contractual arrangements in which the purchasing government of the importing country obliges the supplying company of the exporting country to reinvest some proportion of the contract in the importing country. In practice, offset arrangements typically take two forms: 'direct offsets', in which the investment is directly related to the subject of the main purchase, and 'indirect offsets', in which the investment is not related.[86] In the context of the DCI, the term 'offset contracting' refers to both direct and indirect offset agreements – unless otherwise stated – as well as any other equivalent terms to indicate similar arrangements such as industrial cooperation, co-production or counter-trade agreements.



Distribution of results by band for all companies in the area of Offsets (%)

[79] Transparency International Defence & Security, Due diligence and corruption risk in defence industry offsets programmes, (TI-UK: London), 2012, p.9, https://ti-defence.org/publications/due-diligence-and-corruption-risk-in-defence-industry-offsets-programmes/ [accessed 23 March 2021].

[80] Data calculated from results on Questions 8.1, 8.2, 8.3 and 8.4

[81] Ibid.

[82] Data calculated from results on Questions 8.1, 8.2, 8.3 and 8.4

[83] Data calculated from results on Questions 8.1, 8.2, 8.3 and 8.4

[84] Data calculated from results on Question 8.1

[85] Data calculated from results on Question 8.2

[86] Transparency International Defence & Security, Defence offsets: Addressing the risks of corruption & raising transparency (TI-UK: London), April 2010, p.12, https://ti-defence.org/publications/defence-offsets-addressing-the-risks-of-corruption-raising-transparency/ [accessed 7 April 2021].

9. High-Risk Markets

As multinational businesses expand into new markets, their ability to identify and impose controls on the relevant corruption risks will continue to be a crucial part of good practice. In almost all cases, the level of risk in a particular market is determined by the level of transparency and oversight of both the government and the defence industry. Companies operating in countries with very low transparency and oversight inevitably face a much higher risk of corruption. Therefore, the more information that companies proactively put into the public domain, the easier it is for government oversight bodies as well as public scrutiny to function effectively. Measures such as enhanced due diligence and interrogation of beneficial ownership will help. However, in countries where the military effectively runs the government and where the finance ministry may have little to no oversight of defence procurement, greater openness is essential to mitigate the risk of corruption.

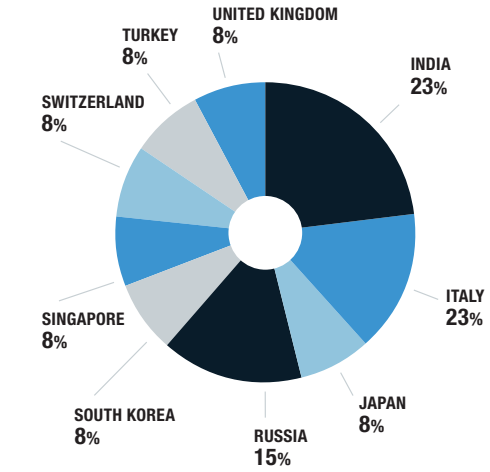
Key findings:

The DCI finds that only **24%** of companies have clear risk management procedures in place to assess the corruption risks of operating in different markets and jurisdictions.[87] In the most responsible companies, these procedures will have a direct impact on business decisions and trigger the implementation of additional controls in cases identified as being at high risk of corruption.

Very few (13%) companies publicly indicate that they have any measures in place to assess the corruption risks of specific markets,[88] while a significant number (**63%**) of companies show little to no evidence of such controls.[89] Several companies publicly indicate that they conduct risk assessments based on geography, but do not provide any further indication that such assessments account for the particular bribery and corruption risks in a given market. It is essential that companies conduct tailored risk assessments prior to entering into new markets to ensure that mitigating measures are commensurate with the level of corruption and bribery risk. Alternatively, companies can choose not to operate in high-risk markets due to the associated corruption risks.

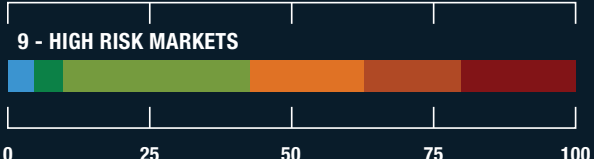
The majority of companies (**75%**) publish information on their significant subsidiaries, however only **10%** publish information on the country of operation of their affiliated entities.[90] The DCI shows some variation in the amount of information that companies publish on their fully and non-consolidated entities – only companies within the 10% disclose information on the percentage ownership, country of incorporation and country of operation for each entity. In addition, the majority companies do not clearly publish details of all their affiliated entities, or fail to demonstrate that they update this list on an annual basis.

GEOGRAPHIC DISTRIBUTION OF COMPANIES THAT PUBLISH COMPREHENSIVE INFORMATION ON THEIR SUBSIDIARIES



Of the companies that publish the most information on this subject, less than half (**46%**) are headquartered in Europe and none are headquartered in the United States; instead the companies that publish comprehensive information are mainly headquartered in Asia Pacific and the Middle East. Although some of these companies are operationally smaller, and therefore affiliated with fewer entities, this is not true in all cases. Moreover, one in four (**25%**) companies do not publish any meaningful information on their subsidiaries, associates and joint ventures in which they have a stake.

Data in the DCI indicates that companies are more likely to publish information on their domestic subsidiaries than any similar entities based abroad. This pattern may reflect differing disclosure practices between regulatory regimes, but given that the majority of companies assessed in the DCI span more than one jurisdiction, the most responsible companies should provide comprehensive information across all of their operations. Making this information available helps to level the playing field and provides a crucial element of transparency to the defence sector worldwide, especially in markets where oversight might be lacking.



Distribution of results by band for all companies in the area of High Risk Markets (%)

[87] Data calculated from results on Question 9.1

[88] Ibid.

[89] Ibid.

[90] Data calculated from results on Question 9.2

Spotlight on: Defence Sales

Only **11%** of companies publish clear information to account for the customers of at least 80% of their defence sales.[91] These companies publish high-level percentages or equivalent figures to indicate the major defence customers that they supply, thereby bringing a crucial element of transparency to the global arms trade. Since the customers of major defence contracts are almost exclusively national governments, "customers" in this context refers to governments.

A further **13%** provide some information on their major customers – either for all sales rather than defence-specific, or for some customers on an ad hoc basis – while the majority (**76%**) of companies publish little to no meaningful information on their major defence customers.[92]

Due to the nature of the arms trade, there are often practical limitations on the amount of information that companies can publicly disclose in relation to domestic and international sales. Such restrictions may be imposed by national governments for reasons of national security, commercial sensitivity or other data protection legislation. However, if 11% of companies are able to publish high-level information on their customers, other companies may be able to learn from peers and improve their disclosures in this area.

[91] Data calculated from results on Question 9.4

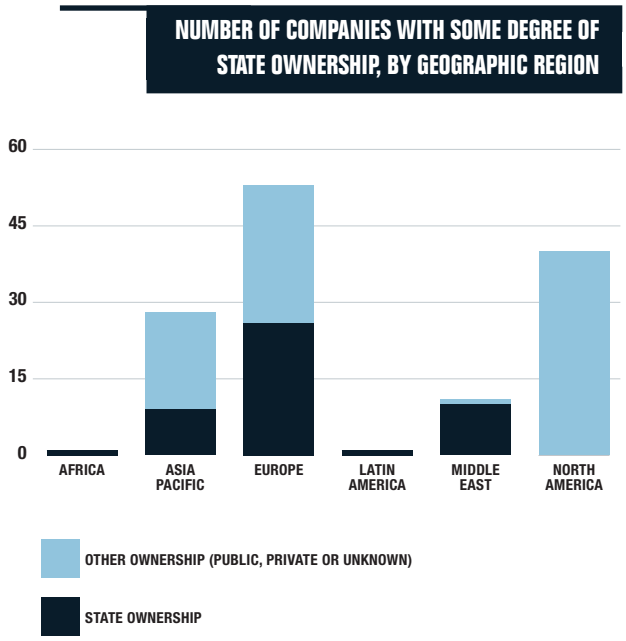
[92] Ibid.

10. State-Owned Enterprises

State-owned enterprises (SOEs) need not pose an inherent corruption risk. However, such companies can encounter particular vulnerabilities that publicly and privately owned companies do not. An intrinsically close relationship with the ownership entity – in this case, the state – can leave SOEs vulnerable to significant political interference. Even where companies are only partially state-owned, the potential for influence and intervention from state actors is very high. The governance structure of SOEs also creates the opportunity for anti-competitive behaviour, especially when public officials hold decision-making roles in the company, and evidence suggests that this can expose a company to higher corruption risks. Adding to this, instances of corruption within SOEs can have devastating consequences on the national government, economy and general population; it can damage citizens' trust in state institutions in a way that private company corruption scandals may not. In addition, the most progressive state-owned defence companies should strive to be transparent about their management and decision-making processes on some of the areas in which they face heightened risks – for example, audit process oversight, asset transactions and executive-level conflicts of interest.

Key findings:

The DCI identifies **47 companies** as having some degree of state ownership. The level of state-ownership in each entity varies across companies, from 100% to 10% with significant minority control.

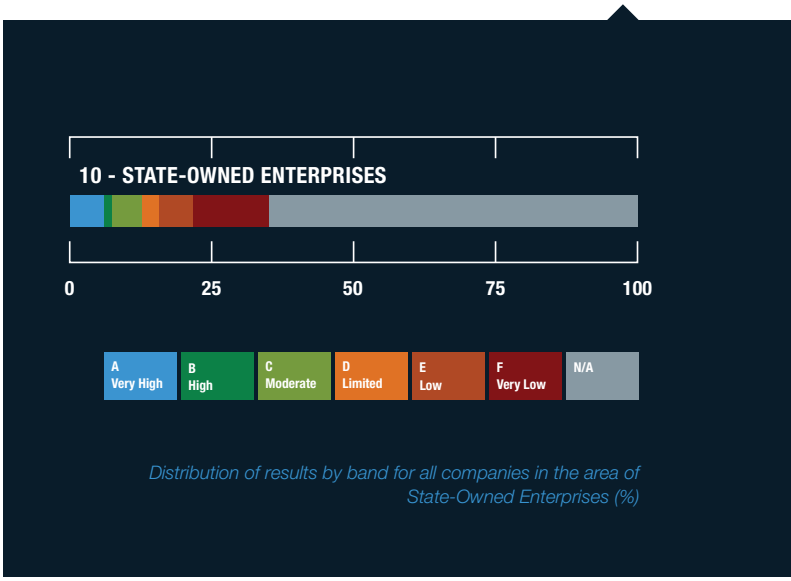


Just over a third (**36%**) of companies with a portion of state ownership score in the top three bands (A-C) for their transparency in this area. However, fully or majority state-owned companies publish notably less information on their management than partially state-owned enterprises. Only **23%** of companies with majority state-ownership score in the top three bands (A-C) and this figure drops even further to **11%** when looking specifically at fully state-owned companies.[93]

Only **23%** of companies with some degree of state ownership publish comprehensive information on the composition of their board of directors and the nomination and appointment process for new members.[94] The remaining **77%** provide either very little detail of their board composition in the public domain or no information on the nomination and appointment process.[95] Placing this information in the public domain is essential to mitigate any instances or perceptions of undue influence or conflicts of interest at the highest levels of the company.

What is a state-owned enterprise?

A state-owned enterprise (SOE) is defined broadly as an entity that is owned or controlled by the state and that carries out activities that are commercial or for public policy objectives, or a combination of these. In practice, a company is considered a state-owned enterprise when the state has direct significant control through full, majority or significant minority ownership of 10% of shares or more.



Distribution of results by band for all companies in the area of State-Owned Enterprises (%)

[93] Data calculated from results on Questions 9.3 and 10.1. Ownership data based on the company's publicly available information; companies with significantly opaque or unclear ownership structures excluded from this calculation.

[94] Data calculated from results on Question 10.3

[95] Ibid.

In addition, the composition of an audit committee in companies with any degree of state ownership is an important indicator of the anti-corruption systems that it has in place. Independent directors provide expertise and technical knowledge, and act as a balancing force should there be any attempts by the state to interfere unduly in the governance of the company. Yet, out of **47** fully or partially state-owned companies in the DCI, only 12 (26%) are transparent about the composition of their audit committee and indicate that it is composed of a majority of independent directors.[96] In two-thirds (**68%**) of fully or partially state-owned enterprises there is no public indication that an audit committee even exists.[97]

Only a small minority (**9%**) of companies with a degree of state ownership show evidence of clear procedures in place to manage asset transactions, which include activities such as mergers, acquisitions, divestments, refinancing and write-offs.[98] Just over a quarter (**28%**) of companies provide some information on this subject but the majority (**64%**) publish no evidence of their systems to manage asset transactions in the public domain. Asset transactions can expose partially or fully state-owned enterprises to a range of corruption risks, for example through the manipulation of asset values by public officials, anti-competitive behaviour and the use of assets or resources as benefits to influence certain individuals.[99] It is crucial that companies with any portion of state ownership implement procedures to ensure that asset transactions align with market value and that they are transparent about this process.

[96] Data calculated from results on Question 10.4

[97] Ibid.

[98] Transparency International, 10 Anti-Corruption Principles for State-Owned Enterprises (TI: Berlin) 2017, p.23, https://www.transparency.org/en/publications/10-anti-corruption-principles-for-state-owned-enterprises [accessed 19 March 2021].

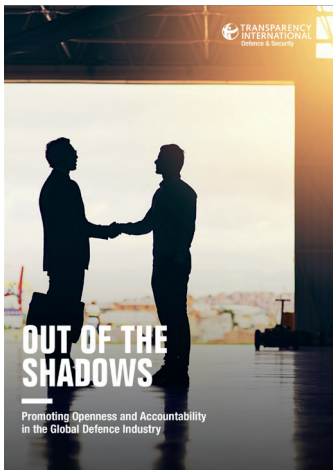
[99] Ibid.

Annex I: Additional Resources

The Defence Companies Index on Anti-Corruption and Corporate Transparency 2020 website contains a number of materials that explain the rationale, structure and assessment criteria of the index. These include:

The **DCI Questionnaire & Model Answers** document, which outlines the 56 questions that make up the index, grouped into 10 key categories where stronger controls and greater transparency within defence companies can reduce corruption risk.

The **DCI Methods Paper** outlines the key methodological features of the index, providing further insight into the assessment process, scoring and implications.



The TI-DS report, **Out of the Shadows: Promoting Openness and Accountability in the Global Defence Industry**, published in September 2018, which outlines the rationale behind what we assess and propose as good practice in the 10 key risk categories.

DCI
Defence Companies Index
on Anti-Corruption & Corporate Transparency

The DCI Website and full data can be accessed via **www.ti-defence.org/dci**

Annex II: The Question Set

The full Questionnaire and Model Answer document, with specific scoring criteria for each question, can be found at **https://ti-defence.org/dci/the-dci-indicators/**

1. Leadership and Organisational Culture	
1.1	Does the company have a publicly stated anti-bribery and corruption commitment, which is authorised by its leadership?
1.2	Does the company have a comprehensive anti-bribery and corruption policy that explicitly applies to both of the following categories: a) All employees, including staff and leadership of subsidiaries and other controlled entities; b) All board members, including non-executive directors.
1.3	Does the board or a dedicated board committee provide oversight of the company's anti-bribery and corruption programme?
1.4	Is responsibility for implementing and managing the company's anti-bribery and corruption programme ultimately assigned to a senior executive, and does he or she have a direct reporting line to the board or board committee providing oversight of the company's programme?
2. Internal Controls	
2.1	Is the design and implementation of the anti-bribery and corruption programme tailored to the company based on an assessment of the corruption and bribery risks it faces?
2.2	Does the company review its anti-bribery and corruption risk assessment and update it when gaps and issues are identified?
2.3	Is the company's anti-bribery and corruption programme subject to regular internal or external audit, and are policies and procedures updated according to audit recommendations?
2.4	Does the company have a system for tracking, investigating and responding to bribery and corruption allegations or incidents, including those reported through whistleblowing channels?
2.5	Does the company have appropriate arrangements in place to ensure the quality of investigations?
2.6	Does the company's investigative procedure include a commitment to report material findings of bribery and corruption to the board and any criminal conduct to the relevant authorities?
2.7	Does the company publish high-level results from incident investigations and disciplinary actions against its employees?
3. Support to Employees	
3.1	Does the company provide training on its anti-bribery and corruption programme to all employees across all divisions and geographies, and in all appropriate languages?
3.2	Does the company provide tailored training on its anti-bribery and corruption programme for at least the following categories of employees: a) Employees in high risk positions, b) Middle management, c) Board members.
3.3	Does the company measure and review the effectiveness of its anti-bribery and corruption communications and training programme?
3.4	Does the company ensure that its employee incentive schemes are designed in such a way that they promote ethical behaviour and discourage corrupt practices?

3.5	Does the company commit to and assure itself that it will support and protect employees who refuse to act unethically, even when it might result in a loss of business?
3.6	Does the company have a clear policy of non-retaliation against whistleblowers and employees who report bribery and corruption incidents?
3.7	Does the company provide multiple whistleblowing and advice channels for use by all (e.g. employees and external parties), and do they allow for confidential and, wherever possible, anonymous reporting?
4. Conflict of Interest	
4.1	Does the company have a policy defining conflicts of interest – actual, potential and perceived – that applies to all employees and board members?
4.2	Are there procedures in place to identify, declare and manage conflicts of interest, which are overseen by a body or individual ultimately accountable for the appropriate management and handling of conflict of interest cases?
4.3	Does the company have a policy and procedure regulating the appointment of directors, employees or consultants from the public sector?
4.4	Does the company report details of the contracted services of serving politicians to the company?
5. Customer Engagement	
5.1.1	Does the company have a clearly defined policy and/or procedure covering political contributions?
5.1.2	Does the company publish details of all political contributions made by the company and its subsidiaries, or a statement that it has made no such contribution?
5.1.3	Does the company have a clearly defined policy and/or procedure covering charitable donations and sponsorships, whether made directly or indirectly, and does it publish details of all such donations made by the company and its subsidiaries?
5.2.1	Does the company have a policy and/or procedure covering responsible lobbying?
5.2.2	Does the company publish details of the aims and topics of its public policy development and lobbying activities it carries out?
5.2.3	Does the company publish full details of its global lobbying expenditure?
5.3.1	Does the company have a policy and/or procedure on gifts and hospitality to ensure they are bona fide to prevent undue influence or other corruption?
6. Supply Chain Management	
6.1	Does the company require the involvement of its procurement department in the establishment of new supplier relationships and in the oversight of its supplier base?
6.2	Does the company conduct risk-based anti-bribery and corruption due diligence when engaging or re-engaging with its suppliers?
6.3	Does the company require all of its suppliers to have adequate standards of anti-bribery and corruption policies and procedures in place?
6.4	Does the company ensure that its suppliers require all their sub-contractors to have anti-corruption programmes in place that at a minimum adhere to the standards established by the main contractor?
6.5	Does the company publish high-level results from ethical incident investigations and disciplinary actions against suppliers?
7. Agents, Intermediaries and Joint Ventures	

7.1.1	Does the company have a clear policy on the use of agents?
7.1.2	Does the company conduct risk-based anti-bribery and corruption due diligence when engaging or re-engaging its agents and intermediaries?
7.1.3	Does the company aim to establish the ultimate beneficial ownership of its agents and intermediaries?
7.1.4	Does the company's anti-bribery and corruption policy apply to all agents and intermediaries acting for or on behalf of the company, and does it require anti-bribery and corruption clauses in its contracts with these entities?
7.1.5	Does the company ensure that its incentive schemes for agents are designed in such a way that they promote ethical behaviour and discourage corrupt practices?
7.1.6	Does the company publish details of all agents currently contracted to act with and on behalf of the company?
7.1.7	Does the company publish high-level results from incident investigations and sanctions applied against agents?
7.2.1	Does the company conduct risk-based anti-bribery and corruption due diligence when entering into and operating as part of joint ventures?
7.2.2	Does the company commit to incorporating anti-bribery and corruption policies and procedures in all of its joint venture relationships, and does it require anti-bribery and corruption clauses in its contracts with joint venture partners?
7.2.3	Does the company commit to take an active role in preventing bribery and corruption in all of its joint ventures?
8. Offsets	
8.1	Does the company explicitly address the corruption risks associated with offset contracting, and is a dedicated body, department or team responsible for oversight of the company's offset activities?
8.2	Does the company conduct risk-based anti-bribery and corruption due diligence on all aspects of its offset obligations, which includes an assessment of the legitimate business rationale for the investment?
8.3	Does the company publish details of all offset agents and brokers currently contracted to act with and/or on behalf of the company?
8.4	Does the company publish details about the beneficiaries of its indirect offset projects?
9. High Risk Markets	
9.1	Does the company have enhanced risk management procedures in place for the supply of goods or services to markets or customers in countries identified as at a high risk of corruption?
9.2	Does the company disclose details of all of its fully consolidated subsidiaries and non-fully consolidated holdings (associates, joint ventures and other related entities)?
9.3	Does the company disclose its beneficial ownership and control structure?
9.4	Does the company publish a percentage breakdown of its defence sales by customer?
10. State-Owned Enterprises	
10.1	Does the state-owned enterprise publish a breakdown of its shareholder voting rights?
10.2	Are the state-owned enterprise's commercial and public policy objectives publicly available?
10.3	Is the state-owned enterprise open and transparent about the composition of its board and its nomination and appointment process?
10.4	Is the company's audit committee composed of a majority of independent directors?
10.5	Does the state-owned enterprise have a system in place to assure itself that asset transactions follow a transparent process to ensure they accord to market value?

Transparency International Defence & Security

10 Queen Street Place,
London,
EC4R 1BE

ti-defence.org
twitter.com/@TI_Defence

Transparency International UK

Registered charity number 1112842

Company number 2903386