

# **DEFENCE COMPANIES INDEX ON ANTI-CORRUPTION AND CORPORATE TRANSPARENCY 2020**



**Methods Paper**

**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.**

© 2020 Transparency International. All rights reserved. Reproduction in whole or in parts is permitted, providing that full credit is given to Transparency International and provided that any such reproduction, in whole or in parts, is not sold or incorporated in works that are sold. Written permission must be sought from Transparency International if any such reproduction would adapt or modify the original content.

Published February 2021.

Transparency International UK's registered charity number is 1112842.

# DEFENCE COMPANIES INDEX ON ANTI-CORRUPTION AND CORPORATE TRANSPARENCY 2020

Methods Paper



# CONTENTS

<b>1. Summary...</b>	<b>...1</b>
<b>2. What is the DCI?...</b>	<b>...1</b>
What is the purpose of the DCI?...	...1
What the DCI does not measure...	...2
<b>3. Content of the index...</b>	<b>...3</b>
Underlying themes...	...3
Guidance notes...	...3
Scoring criteria...	...4
Key definitions...	...4
<b>4. Sources of company information...</b>	<b>...5</b>
<b>5. The assessment process...</b>	<b>...6</b>
<b>6. Company selection...</b>	<b>...7</b>
<b>7. Index outputs...</b>	<b>...7</b>
The results...	...7
Comparability...	...8
<b>8. Potential sources of error...</b>	<b>...9</b>
<b>9. Selected references...</b>	<b>...11</b>
<b>Annex I: DCI risk areas...</b>	<b>...12</b>
<b>Annex II: Questionnaire and Model Answers (QMA) 2020...</b>	<b>...15</b>
<b>Annex III: The Assessment Process (in depth)...</b>	<b>...19</b>
<b>Annex IV: Companies selected for assessment in 2020...</b>	<b>...21</b>
<b>Annex V: Full list of definitions...</b>	<b>...25</b>

# 1. SUMMARY

The Defence Companies Index on Anti-Corruption and Corporate Transparency (DCI) seeks to assess the levels of commitment to anti-corruption and transparency in the corporate policies and procedures of 134 defence companies worldwide.

Produced by Transparency International's Defence and Security (TI-DS) team, the DCI 2020 follows two previous corporate indices published in 2012 and then again in 2015. Due to significant changes in the aim, focus, methodology and question set of the 2020 index, any comparison with previous indices is not possible or appropriate.

The purpose of the DCI is to use publicly available information to assess the quality, extent and availability of anti-bribery and corruption policies and procedures in the areas that present the highest corruption risks to defence companies. The results of this project will be presented in bands to reflect companies' overall commitment to anti-corruption and corporate transparency, as well as through a set of scores relating to each key risk area that structures the questionnaire.

This document outlines the key methodological features of the DCI 2020, to provide further insight into the assessment process, scoring and implications of the index. The new formulation of the DCI 2020 reflects the substantial feedback received from a range of stakeholders as part of a comprehensive public consultation, which covered both the question set and the methodology itself. The DCI 2020 represents TI-DS' commitment to promoting greater openness and transparency in the defence sector to help reduce corruption, build public trust, reassure investors, and build constructive relationships between companies and their employees and customers.

# 2. WHAT IS THE DCI?

The Defence Companies Index on Anti-Corruption and Corporate Transparency (DCI) 2020 sets the standards for transparency, accountability and anti-corruption standards in corporate policies and procedures for defence sector companies worldwide. The DCI is produced by Transparency International's Defence and Security team, as a new and updated formulation of the Companies Index first published in 2012 and then again in 2015. Due to significant changes in the aim, focus, methodology and question set of the 2020 index, any comparison with previous indices is not possible or appropriate. For more information on this, see the 'Comparability' section of this paper.

The DCI 2020 assesses 134 of the world's leading defence companies across 38 countries using a question set covering the most significant corruption risks facing the sector. The DCI is used worldwide by governments, investors, civil society, academics and companies themselves, in order to gain a better understanding of anti-corruption and transparency standards and procedures within the defence sector.

## What is the purpose of the DCI?

The DCI 2020 provides a unique insight into the level of commitment to transparency and anti-corruption standards in the world's largest defence companies. By analysing what companies are publicly committing to in terms of their policies and procedures, the DCI seeks to drive reform in the defence sector, thereby reducing corruption and its impact.

**Set good practice standards for openness in the defence sector.** The DCI provides a framework of good practice that promotes standards of anti-corruption and transparency of policies and procedures, which in turn help to increase accountability and reduce the risk of corruption in the defence sector. The index recognises that, despite advances of internal compliance policies and procedures, there remains a need to increase transparency in a sector characterised by opacity and secrecy. Greater transparency and disclosure is the key to creating a common benchmark and enabling meaningful oversight to reduce the risk of corruption in the sector, especially given the close links between government and industry.

In the highest risk markets, where oversight and transparency is weakest, public disclosures are the only way to effectively address and reduce the opportunities for corruption. Transparency is also good for business; responsible companies are more likely to thrive in the market, benefit from open competition and reassure investors. The standards of good practice outlined in

the DCI stem from Transparency International Defence and Security's work on understanding the way in which corruption occurs in the defence sector and from a recognition that internal compliance programmes alone are insufficient to increase accountability sector-wide.

**Promote dialogue and engagement with companies on transparency in the defence sector.** The DCI provides a tool for Transparency International Defence and Security to engage with defence companies to initiate a dialogue on issues relating to anti-corruption and corporate transparency, with the ultimate aim of driving reform and promoting openness in the sector. In addition to an open consultation on the updated Questionnaire and Model Answer (QMA) document, TI-DS provided companies with several opportunities to engage in the data collection phase of the assessment process. For more information on this, see the section entitled 'The Assessment Process'. This engagement with companies provides a platform for positive change in the sector, as well as helping to ensure the validity and credibility of the DCI assessments. Moreover, the DCI also facilitates the development and sharing of good practice standards between companies, particularly those working in partnerships or those working in similar markets.

**A tool for evidence-based advocacy.** The DCI provides a tool for governments, defence companies, investors, civil society, media and other stakeholders to promote an understanding of defence corruption issues, raise standards, and reduce the risk of corruption sector-wide. The index highlights and addresses key standards of anti-corruption and transparency in 10 distinct risk areas; each assessment can therefore be used to identify topics or control mechanisms where transparency is lacking, and provide a roadmap for change. Transparency International Defence and Security uses the DCI as the basis for evidence-based advocacy and engagement with a broad range of stakeholders, as well as to inform future research to better understand the impact of corporate opacity on corruption in the arms trade.

## What the DCI does not measure

### The DCI is not a measurement of corruption.

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. All companies operating in the defence sector face some degree of corruption risk. 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 in turn helps to reduce the risk of corruption in the sector overall.

### The DCI is not a substitute for internal audit.

The topics covered on the DCI represent key aspects of corporate anti-corruption policies, procedure and operations which would benefit from increased transparency, based on Transparency International Defence and Security's research and experience of working with the sector. The question set highlights the most important or commonly overlooked risk areas that companies should address in a transparent way to foster accountability and benefit the sector. As such, it does not attempt to provide a comprehensive overview of all components of a defence company's internal compliance programme.

Moreover, the index focuses solely on information that companies make available in the public domain. In other words, each assessment is based solely on information from documents and webpages available on a company's publicly available website. The DCI therefore analyses the presence, quality and transparency of a company's policies, procedures and disclosures but cannot measure implementation in practice – beyond information made publicly available. Unlike the 2015 Companies Index, the DCI 2020 does not include any internal information provided by companies. For more information on this, see the section entitled 'Sources of Company Information'.

## 3. CONTENT OF THE INDEX

Based on in-depth discussions with anti-corruption and defence experts, Transparency International Defence and Security has identified 10 key areas where stronger controls and greater transparency within defence companies can reduce corruption risk. These risk areas form the main structure of the Questionnaire and Model Answer (QMA) document. These areas are:

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

The 2020 QMA is composed of 56 indicators in the form of questions, each with detailed guidance and scoring criteria. Dividing the questions into risk-specific sections reflects the DCI's focus on transparency of the core corruption risks facing defence companies and their employees on a daily basis.

Each of the 10 key areas contain a different number of questions, to ensure that the weighting of the questionnaire accurately reflects the level of corruption risk associated with a lack of transparency in each of these areas. A high-level summary of the 2020 QMA is available in Annex II of this document. The full QMA is available online at [www.ti-defence.org/dci](http://www.ti-defence.org/dci).

### Underlying themes

The 2020 Questionnaire and Model Answer (QMA) document is underpinned by two key themes: policies and processes, and transparency and public disclosure. The majority of the questions on the DCI fall into one of those two categories, with three questions that touch on both topics.

**Policies and Processes.** These are indicators that relate specifically to the standard and amount of publicly available information on certain policies and procedures relevant to reduce the risk of corruption within defence companies worldwide. Robust policies and controls play a vital role in safeguarding companies against corruption risks. They represent the backbone of an organisation's internal controls, the first recourse for employees and a key pillar in establishing a culture of transparency and anti-

corruption within an organisation. The 2020 QMA contains 37 questions that fall into this category.

**Transparency and Public Disclosure.** These are indicators that relate specifically to transparency and public disclosure of data or information that would benefit and reduce corruption risk in the sector overall. Robust policies and controls must be coupled with broader transparency to reassure stakeholders that the systems are indeed functioning as they should be, and to promote accountability in the sector. These questions are based on the recognition that corporate compliance programmes have advanced significantly in recent years as a result of increased enforcement and legal mechanisms, global initiatives and a growing international consensus against corruption in favour of responsible business conduct. Ultimately, greater transparency and disclosure is the key to meaningful oversight and reducing corruption risk. The 2020 QMA contains 16 questions that fall into this category.

### Guidance Notes

In a change from previous indices, the 2020 DCI QMA contains specific guidance for each question. The guidance exists to provide some essential insight and clarification into the questions and topics raised on the DCI, in a way that is useful to all stakeholders. It outlines good practice standards, addresses the way in which companies may present this data in a practical manner, and provides detail on the type of company information that may be relevant. Where appropriate, the guidance also clarifies the risk that the question is trying to address and the importance of increasing transparency and public disclosure on the subject.

Transparency International Defence and Security developed this guidance in response to feedback from previous indices conducted in 2015 and 2012, as well as to provide companies, assessors and external observers with a greater understanding of international good practice standards in these areas. The additional level of detail provided by the guidance also helps to ensure consistency among assessments.

Further information about the rationale for the key corruption risk areas identified and addressed in the DCI 2020 can be found in our report, 'Out of the Shadows: Promoting Openness and Accountability in the Global Defence Industry'.<sup>1</sup>

<sup>1</sup> This report is available online at <http://ti-defence.org/publications/out-of-the-shadows/>.



## Scoring Criteria

For each question, a company may receive 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. Companies may also be eligible for a score of ‘N/A’ on certain questions, as described below. The 2020 QMA contains a total of 56 questions; with a maximum overall score of 112 for the full assessment.

The general principles underlying the scoring criteria are reflected in the table below:

2	Full points; i.e. the company’s publicly available information meets the expectation of the question fully and there is evidence to substantiate this expectation.
1	Half points; i.e. the company’s publicly available information meets some of the expected standards, but the evidence to support this is either lacking or falls short of the good practice expectation outlined in score ‘2’.
0	No points; i.e. the company’s does not provide publicly available information to demonstrate that it meets the required standards of the question, or the evidence provided is sufficiently unclear that it cannot meet the expectation of score ‘1’.
N/A	Not applicable; i.e. the company is exempt from scoring on this question because the subject is not relevant or applicable to its nature or context.

The purpose of the scoring criteria is to outline the standards of good practice and to indicate the extent to which a given company may meet these standards through its public disclosures. To score full points on any question, companies are not expected to use the exact wording of the scoring criteria. Companies can still score full marks using equivalent language that conveys the underlying commitment or intent of the question, providing the assessor cannot find any evidence to the contrary.

As part of the 2020 QMA, there are two questions where companies may only receive a score of ‘2’, ‘0’ or ‘N/A’; question 5.1.1 on political contributions policies and 5.1.2 on political contributions disclosures. The option to score ‘1’ was removed after extensive consultation internally, externally and across the TI movement which highlighted the complexity of defining political expenditures across different jurisdictions. For example, the term ‘political contributions’ could include direct political expenditures (both at local and national level), membership of trade associations, contributions to certain think tanks, and more. In the United States, corporate contributions to Political Action Committees (PACs) add another dimension to this subject. TI-DS therefore took the decision to remove the option to score ‘1’ from the scoring criteria, until further research enables the identification of clear standards in this field.

Likewise, there may be cases where certain questions simply do not apply. This exemption applies to selected questions in cases where TI-DS research has identified that a subject may not apply to a company based on

the nature of its business, its operations or its corporate structure. Where this occurs, the assessor can mark the question as ‘N/A’ and it will be exempt from the company’s overall score. Receiving ‘N/A’ on a question will therefore not have a negative effect on a company’s performance in the DCI. There is no limit to the number of times that an assessor can mark a question as ‘N/A’, though it can only be applied when stipulated as part of the criteria; this classification can be used wherever appropriate for each company. A total of 20 questions are eligible to be marked as non-applicable on the DCI 2020.

## Key Definitions

Any specific definitions that might be relevant to the scoring of a particular question are outlined in the QMA either at the start of the section or as part of the question guidance. A full list of definitions available in Annex V. However, there are a few overarching definitions that have implications throughout the DCI.

### Anti-bribery and corruption programmes

Companies use a variety of terms to describe their corporate systems for promoting integrity and reducing corruption risk. Terminology that covers these initiatives may include ‘business ethics’, ‘business conduct’, ‘ethics programmes or policies’, or ‘compliance programmes’. In addition, each company may house their policies and programmes to promote ethical values and tackle corruption in separate documents. For example, some companies may organise their values and integrity-building efforts under a Business Ethics or Human Resource Department. Other companies may organise their anti-corruption and other compliance efforts under a Legal or Risk Department. Given the wide variety of terms and organisational structures that cover integrity building and anti-corruption efforts, TI-DS uses the phrase ‘anti-bribery and corruption programmes’ to describe a company’s approach to promoting its integrity at all levels of its operations and to reducing corruption risk. Companies that organise their efforts under a different name will not be disadvantaged for using equivalent wording, so long as it

is clear to the assessor that the company addresses each corruption risk in a clear and transparent way.

## Corruption

Transparency International defines corruption as “the abuse of entrusted power for private gain”. TI-DS research identified specific corruption risks in the defence and security sector, which is presented in relation to defence companies in the form of the contents of the Questionnaire and Model Answer (QMA) document.

## Corruption risk

Corruption risk refers to the probability that defence and security corruption might occur, along with a reflection of the potential cost associated with that corruption. It thus reflects the potential that such loss, whether monetary, social or political can arise; and reflects the severity of such cost when it occurs. Increased risk means a higher potential for corruption or a higher cost associated with the risk, or both. Companies have the ability to influence levels of corruption risk in the sector as ‘supply side’ actors, while the ‘demand side’ actors are assessed on TI-DS’ sister index: the Government Defence Integrity Index (GDI).<sup>2</sup> The 2020 DCI assesses companies’ commitment to transparency and anti-corruption standards, which helps to reduce the risk of corruption both in the company and in the sector overall.

## Transparency

Transparency refers to being open in the clear disclosure of information, rules, plans, processes and actions. For the purpose of this assessment, transparency is used in combination with public disclosure to describe the level of detail and information provided by companies on their internal processes and operations. In some cases this simply refers to a clear description of a specific policy or procedure, while in other cases it refers to the publication of specific information that may help to mitigate a specific corruption risk or increase accountability in the sector.

# 4. SOURCES OF COMPANY INFORMATION

The DCI 2020 assesses the standards of anti-corruption measures and levels of transparency in the operations of 134 major defence companies worldwide. The assessment of a company’s commitment to anti-corruption and transparency is **based entirely on publicly available information**.

The decision to exclude internal information from the company assessments represents the most significant change compared to the previous Companies Index in 2015 and 2012. This reflects TI-DS’ commitment to greater transparency, which increases customer and investor confidence in the company, ensures the details of these programmes are open to public scrutiny, enables companies to share and understand good practice and improves the reputation of companies and the industry as a whole.

In particular, a group of researchers working with Transparency International Defence and Security retrieved publicly available information through a review of the company’s website, including any available reports, for evidence of a strong commitment to transparency and anti-corruption, as well as any functioning hyperlinks to other relevant online materials. Only official company information and documents was taken into consideration as evidence; any references to the company or its processes on third party websites – such as industry association pages or news reports, for example – did not contribute towards the scoring. Typical documents include annual reports, social responsibility reports, ethics and compliance sections of the website, and individual policy documents where available.

In each instance, companies were assessed on the latest available version of the documentation at the time of the assessment. Where a company’s website and/or published reports are not available in English, a translator with the relevant language expertise was assigned to conduct the assessment in close cooperation with the lead assessor.

TI-DS did not undertake to verify whether information disclosed on websites or in reports was complete or correct. The increased focus of the 2020 DCI on transparency of policies and disclosure of information can be seen as a proxy for this, with companies encouraged to make information publicly available to show that stated policies are being followed and reported on in practice.

<sup>2</sup> Government Defence Integrity Index (GDI), Transparency International Defence & Security, 2020, [www.ti-defence.org/gdi](http://www.ti-defence.org/gdi)

# 5. THE ASSESSMENT PROCESS

The assessment process for the DCI 2020 consisted of multiple stages, with ongoing feedback and quality control throughout. Five independent assessors were recruited to undertake the assessments,<sup>3</sup> alongside Transparency International Defence and Security team members .

Figure 1 shows the assessment process in detail. After an assessor undertook an initial review of the publicly available information on a company’s website, a TI-DS team member conducted an internal review of the document in order to produce a draft assessment.

Each draft assessment was then sent for company review, where relevant points of contact were given four weeks to review the evidence,<sup>4</sup> provide feedback and make changes to their publicly available evidence where appropriate. Further information about the company

review process is available in Annex III.

In cases where a company did provide feedback, the assessor reviewed and incorporated any relevant information to produce a second assessment, which was then subject to another internal review by TI-DS. If a company chose not to provide feedback, the assessment proceeded to the final quality control stage. At the final review stage, TI-DS checked each assessment to ensure consistent application of the scoring criteria and assigned a final score to the company.

The assessment process for the DCI 2020 took place over a 16 month period. All companies received a full copy of their final assessment and overall scores two weeks prior to publication by TI-DS. Companies were given the opportunity to provide a response to be published

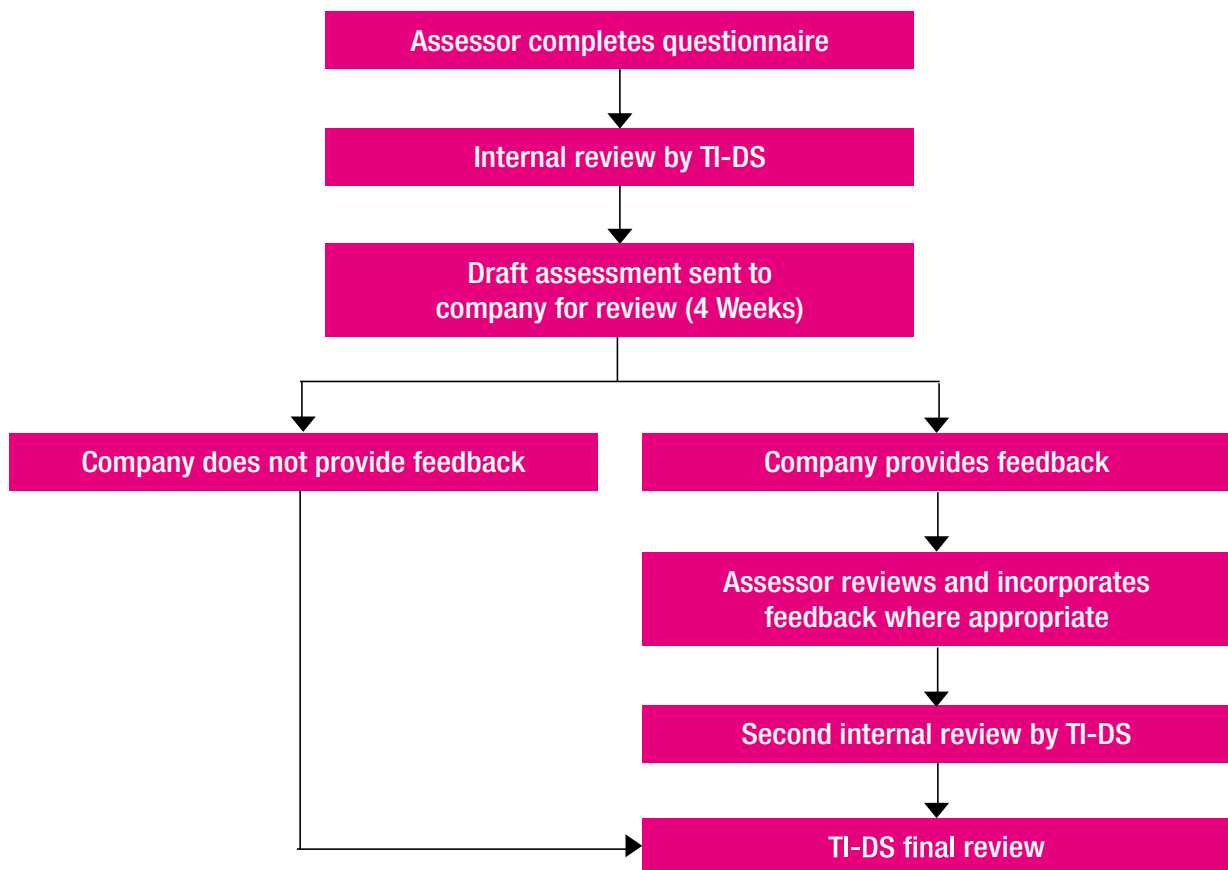


Figure 1: A flowchart of the assessment process, with arrows to show feedback and review at each stage.

<sup>3</sup> Assessors were required to declare any actual, potential or perceived conflicts or interests in the recruitment phase. Assessors remain anonymous; company assessments will not be attributed to a specific assessor.

<sup>4</sup> Due to the COVID-19 pandemic, some companies requested extended deadlines in order to make substantial changes to their publicly available materials. Any extensions were mutually agreed with TI-DS and generally granted (provided the dates remained within the overall assessment period).

alongside their final results on the website.

## 6. COMPANY SELECTION

The companies subject to assessment on the 2020 DCI were selected based on the following criteria:

- The company features in the 2016 edition of Stockholm International Peace Research Institute (SIPRI) Top 100 Arms-Producing and Military Services companies;<sup>5</sup> and/or

Band	Lower Range	Upper Range	Commitment to anti-corruption and transparency
A	83.3	100	Very High
B	66.7	83.2	High
C	50.0	66.6	Moderate
D	33.3	49.9	Limited
E	16.7	33.2	Low
F	0	16.6	Very Low

- The company features in the 2017 edition of the Defense News Top 100 defence companies;<sup>6</sup> and/or
- The company is the largest national defence company (by revenue and exports) headquartered in a country that would otherwise be unrepresented on the DCI 2020 but that has arms exports in excess of at least £10 million, as identified by SIPRI.

In total, these sources resulted in an assessment list of 134 of the world's largest defence companies. Although the companies differ widely in their characteristics, products and/or services, ownership structures and countries of operation, each receives a substantial proportion of their revenue from sales to various militaries or ministries of defence across the world.

TI-DS did not attempt to verify this information or make changes to companies or subsidiaries based on additional research; the companies were taken directly from these lists. The full methodologies of both lists can be found via the respective SIPRI and Defense News websites.

The 134 companies derived from the above calculations were correct at the launch of the project in October 2018. Minor adjustments to the list were made over the course of the project to account for any mergers, acquisitions or dissolutions. In line with the DCI's approach of evaluating companies based on publicly available information only,

<sup>5</sup> Due to reporting cycles, the 2016 SIPRI list was the most current list available when the company selection exercise was carried out in May 2018. The list can be accessed at <https://www.sipri.org/publications/2017/sipri-fact-sheets/sipri-top-100-arms-producing-and-military-services-companies-2016>.

<sup>6</sup> The Defense News 2017 list was the most current list available when the company selection exercise was carried out in May 2018. This list can be accessed at <https://people.defensenews.com/top-100/>. In August 2018, Defense News published its top 100 for 2018, containing four new companies: Russian Helicopters, Toshiba Infrastructure Systems, Hyundai Rotem Company, STM Savunma Teknolojileri Muhendislik ve Ticaret A.S., Oki Electric Industry. These companies were added to the assessment list; no companies were removed.

these situations were determined by the company's online presence. Where a relevant merger or acquisition was announced during the assessment phase, the companies continued to be assessed as separate entities until the change was reflected online (i.e. until the websites were incorporated or one ceased to exist).

The full list of companies selected for assessment in 2020 is available in Annex IV. A total of six mergers and/or acquisitions known to TI-DS affected the company assessment list throughout the research phase. These changes are described and referenced in the footnotes of Annex IV.

## 7. INDEX OUTPUTS

### The Results

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 will correspond to an overall band, which is mapped out using the below classifications:

Since the assessment is based on the quality and availability of a company's publicly available information, a low score on the DCI indicates a weak commitment to transparency and accountability and, therefore, a higher risk of contributing to corruption in the defence sector. Conversely, a high score on the DCI reflects a strong commitment to corporate transparency and accountability and therefore a lower – though not entirely absent – risk of contributing to corruption in the defence sector worldwide.

Each company also receives a score and corresponding band for each of the 10 key risk areas in the 2020 QMA: leadership and organisational culture; internal controls; support to employees; conflict of interest; customer engagement; supply chain management; agents, intermediaries and joint ventures; offsets; high risk markets; and state-owned enterprises.

All companies received a full copy of their final assessment and overall scores two weeks prior to publication by TI-DS. At this stage, companies were given the opportunity to provide a response to be published alongside their final results on the website.

Beyond the DCI process, data from the assessments will also be used to produce high-level qualitative results; for example, divided by risk area, country and/or geographical region. Presentation of the core results, after extensive analysis, will be presented in hard copy and webtext. Ultimate ownership and responsibility for the outputs rests with TI-DS.

## Comparability

The aim, focus and question set for the DCI 2020 is fundamentally different from that of the previous indices published in 2015 and 2012. In the design of the 2020 question set, all previous indicators were reviewed, revised and/or removed and several new risk areas were added based on extensive sectoral research and the shift in approach towards transparency and public disclosure. No questions or scoring criteria from the 2015 CI remain the same on the 2020 DCI.

Therefore, in the analysis and presentation of scores for the 2020 assessment, TI-DS will not make any direct comparisons of overall company scores with data from 2015 or 2012. Some parallels may be drawn between scores on specific questions that have not changed substantially since the 2015 index, but this will not be reflected in the overall results.

In order to reflect these significant changes, Transparency International Defence and Security took the decision to change the name of the index from the Defence Companies Anti-Corruption Index (CI) to the **Defence Companies Index on Anti-Corruption and Corporate Transparency (DCI)**. This name change reflects the increased focus on transparency and public disclosure as key initiatives to reduce corruption risk in the defence sector overall, as well as serving to highlight the significant extent of changes compared to the previous indices.

Many of the changes to the Questionnaire and Model Answer (QMA) document for 2020 were designed to incorporate feedback received as part of a public consultation. This consultation saw a range of stakeholders – including academics, industry representatives, compliance experts and investors – review a draft version of the question set and provide feedback on the content and specific scoring criteria. At the core of TI-DS' approach remains the belief that there is an inherent value in this information being available in the public domain as it contributes to setting common standards, encourages the sharing of best practice, and deters corrupt activity where formal oversight mechanisms are absent or failing.

Following the public consultation, Transparency International Defence and Security edited and refined the question set to ensure that the level of transparency and anti-corruption standards needed for the highest score reflects the importance of the issue and the level of corruption risk it is designed to address. These changes can be seen throughout the revised QMA. As an example, questions rarely ask for the disclosure of full policy documents, but instead look for evidence that such a policy exists, through a company statement or otherwise, and language was revised accordingly. Where certain practical and/or legal considerations could not be mitigated at this stage, TI-DS removed several questions,

in the hope that the sector can work towards greater standards of transparency over time.

Greater openness and transparency will not only help reduce corruption in the sector, it will build public trust, reassure investors, and build constructive relationships with employees and customers. Ultimately, the most responsible companies in the sector will benefit from adopting this approach and the clean business practices it promotes.

## 8. POTENTIAL SOURCES OF ERROR

In the design and conduct of the assessment process, TI-DS considered, and sought to address, the following potential sources of error:

### 1. Inaccuracy

**a. Due to an incomplete set of publicly available resources,** meaning that TI-DS was unable to review all information on a company's ethics and anti-corruption programme. Prior to the start of the assessment process, TI-DS endeavoured to contact at least one person within each company so that they could update or make any changes to their publicly available information in line with the new QMA if they wished. An internal TI-DS team reviewed all assessments to check the relevance and applicability of evidence and scoring criteria used on a question-by-question, company-by-company basis. In addition, all companies were given the opportunity to review a draft version of their assessment and provide feedback to guide assessors towards additional new or relevant publicly available information, should it exist. TI-DS reviewed and discussed internally the impact of any additional documents on any given company's score. At the end of the assessment phase, companies were also given the opportunity to provide a formal response to be published alongside their final results on the DCI website.

**b. Due to TI-DS misinterpreting a publicly available resource.** All companies were given at least one opportunity to comment on a draft version of their assessment and to clarify any misinterpretations. TI-DS also implemented multiple internal quality and consistency checks to reduce the risk of misinterpretation of evidence and ensure consistency among scoring application.

**c. Due to the information that was or was not in the public domain.** The DCI 2020 assesses companies based only on the information that they make publicly available. This decision reflects TI-DS' commitment to fostering greater transparency and accountability in the defence sector, which we believe will help to reduce corruption, build public trust, reassure investors, build constructive relationships with customers and improve the reputation of companies and the industry as a whole. When formulating the assessments, TI-DS did not solicit or take into consideration any internal documents or information provided by the companies during the feedback process. Companies were given the opportunity to provide a formal response to be published alongside their final results on the DCI website, in which they could clarify or provide

additional information not previously available in the public domain.

**d. Due to changes in companies' publicly available information over the course of the assessment.** The DCI 2020 assessment phase ran for a period of 16 months, meaning that regularly published company materials such as Annual Reports, Corporate Social Responsibility and other reporting documents became available throughout the course of the assessment process. Given the number of companies assessed across multiple jurisdictions, the reporting periods covered in these documents may differ. TI-DS took steps to ensure that all draft/first assessments were conducted based on the most recently published company information where available, and invited companies to provide feedback and highlight any newly published information in the four-week company review period. Following this, companies were given the opportunity to provide additional feedback in May 2020 to account for evidence in newly published annual reporting documents from the previous year.

**e. Due to information not in the public domain as a result of confidentiality and commercial sensitivity concerns.**

In developing the revised DCI question set, TI-DS consulted a range of legal experts who provided advice on competition law, anti-trust law and commercial sensitivity issues. TI-DS also considered the impact of the European Union's General Data Protection Regulations (GDPR, 2018) on the question set. No significant legal barriers to publishing this information were identified during these discussions.

## 2. Imprecision

In designing the DCI 2020, TI-DS consulted a broad range of stakeholders including defence companies and associations, defence ethics organisations, academics, research experts and civil society. The aim of this process was to ensure that the criteria outlined in the Questionnaire & Model Answer (QMA) document reflected technical measures and processes relevant to the defence and security industry. TI-DS thoroughly tested and discussed the question set with industry ethics and compliance practitioners prior to the launch of the assessment phase. The results of the index are presented in bands, rather than as a numerical ranking, in order to minimise the issue of error ranges in individual scores.

## 3. Inconsistency

Research for the DCI 2020 was conducted independently from evidence gathered in previous iterations of the project in 2015 and 2012. TI-DS built consistency checks into each stage of the research process. All draft assessments were reviewed internally by TI-DS, all companies were given the opportunity to review their draft assessment and, another round of checks were conducted by TI-DS after

company feedback (if provided) was incorporated. TI-DS took steps to ensure that each assessment was reviewed by a different individual at each stage of the process to reduce the risk of inconsistencies, misinterpretations or clear inaccuracy in the application of the scoring criteria.

## 4. Bias

The foundations of the Questionnaire & Model Answer (QMA) document for the DCI 2020 was developed in collaboration with a broad range of industry stakeholders, defence ethics organisations, academics and experts. The company selection criteria were clearly defined at the start of the project and the assessment questionnaire is based on technical measures and processes, rather than perceptions. TI-DS developed a comprehensive QMA with guidance notes, as well as a technical codebook for assessors to reduce the risk of variability. The QMA was shared with all selected companies prior to the launch of the assessment phase, and companies were able to ask questions and provide additional information from their website during the company feedback period. Internal review by a group of TI-DS team members featured at multiple stages throughout the research process to mitigate individual bias in the assessments, while also reducing the risk of chronological bias.

## 5. Possible conflicts of interest

The assessments were completed by TI-DS staff and a team of five assessors. TI-DS was thus alert to possible conflicts of interest with internal staff, and incorporated conflict of interest considerations into the recruitment process when hiring the assessors. No conflicts of interest were identified during this process.

Transparency International UK works with Meggitt plc as part of its Business Integrity Forum. Throughout the assessment process, TI-DS ensured that no individuals who engage with Meggitt plc through the TI-UK Business Integrity Programme were involved in the DCI assessment process.

Transparency International Defence and Security (TI-DS) does not benefit in any way from financial or in-kind support received by other chapters in the Transparency International movement.

## 9. SELECTED REFERENCES

*Defence Companies Anti-Corruption Index 2015 Report*, Transparency International Defence & Security, 2015, <http://companies.defenceindex.org/docs/2015%20Defence%20Companies%20Anti-Corruption%20Index.pdf>

Dixon, Katharine, Charlotte Linney, Mia Paukovic, and Andrew Watson, 2018, *Out of the Shadows: Promoting Openness and Accountability in the Global Defence Industry*. London: Transparency International, Defence & Security. <https://ti-defence.org/publications/out-of-the-shadows/>

International Forum on Business Ethical Conduct (IFBEC), 'Offsets in the Aerospace and Defence Industry', 2015, <http://www.global-kinetics.com/wp-content/uploads/2016/02/IFBEC-Offsets-Report.pdf>

'License to Bribe? Reducing corruption risks around the use of agents in defence procurement', Transparency International Defence & Security, June 2016, <http://ti-defence.org/publications/licence-to-bribe-reducing-corruptionagents-defence-procurement/>

OECD, 'Combatting corruption and promoting business integrity in state-owned enterprises: Issues and trends in national practices', 2016, <https://www.oecd.org/daf/ca/2016-SOEs-issues-paper-anti%20corruption-and-business-integrity.pdf>

OECD, 'OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Officials', 2014, [https://www.oecd-ilibrary.org/governance/oecd-foreign-bribery-report\\_9789264226616-en](https://www.oecd-ilibrary.org/governance/oecd-foreign-bribery-report_9789264226616-en)

OECD, 'Typologies on the Role of Intermediaries in International Business Transactions', 2009, <https://www.oecd.org/daf/anti-bribery/antibriberyconvention/43879503.pdf>

U.S. Department of Justice, 'Evaluation of Corporate Compliance Programmes', June 2020, <https://www.justice.gov/criminal-fraud/page/file/937501/download>



# ANNEX I: DCI RISK AREAS

Based on in-depth discussions with anti-corruption and defence experts, Transparency International Defence and Security (TI-DS) identified 10 key areas where greater commitment to transparency and anti-corruption standards within defence companies can reduce corruption risk. These risk areas form the basis of the 2020 Questionnaire and Model Answer (QMA) document's 56 indicators.

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

## Leadership and Organisational Culture

Company leadership comes under significant scrutiny in corruption cases, and 'tone from the top' is a key feature anti-bribery legislation such as the U.S. Foreign Corrupt Practices Act (FCPA) and the U.K. Bribery Act. A 2014 OECD analysis of 427 foreign bribery cases over the previous 15 years discovered that at least half were conducted with the involvement of management.

**Specific issues covered under this risk area include commitment from top-level company leadership; anti-corruption policy; board-level oversight; and day-to-day management of anti-bribery and corruption activities. This section contains 4 questions (max. 8 points).**

## Internal Controls

Anti-bribery and compliance programmes play a vital role in safeguarding companies against corruption; they represent the backbone of an organisation's internal controls. Such internal controls are the first recourse for employees and a key pillar in establishing a culture of transparency and anti-corruption within an organisation.

**Specific issues covered under this risk area include risk assessments; internal audit; procedure and quality of internal investigations; and high-level data on employee allegations and ethical investigations. This section contains 6 questions (max. 12 points).**

## Support to Employees

In addition to robust internal controls, companies also need to tailor their systems and procedures to all employees, across all divisions and areas of operation. Training forms a central part of this support system promoting an understanding of bribery and improper business conduct in order to develop employees' capacity to identify, avoid and resist corrupt approaches.

Moreover, it is essential that companies provide a range of effective and confidential whistleblowing channels to allow employees to raise concerns across the management chain. Several of the most recent investigations into defence corruption are a result of reports from whistleblowers, thereby highlighting the importance of these systems.

**Specific issues covered under this risk area include anti-bribery and corruption training; ethical incentives; supporting employees to raise concerns; non-retaliation against those who report unethical behaviour; and whistleblowing provisions. This section includes 7 questions (max. 14 points).**

## Conflicts of Interest

Conflicts of interest are a major risk in the defence industry, where a small number of companies compete for high value, opaque and relatively infrequent contracts with a small number of customers. These risks are further exacerbated by the fact that governments comprise the majority of customers for defence companies. Conflicts can therefore arise through personal relationships, relationships with government officials, financial interests and other employment or engagement.

**Specific issues covered under this risk area include conflict of interest policy and management procedure; appointment of directors, employees or consultants from the public sector; and reporting of services of any contracted politicians. This section contains 4 questions (max. 8 points).**

## Customer Engagement

Closed-door meetings between procurement officials and defence companies can be legitimate and necessary, but they also create opportunities for bribery, influence-peddling and the development of relationships which could lead to potential or actual conflicts of interest. Lobbying, political contributions, charitable donations and gifts and hospitality can all be used as vehicles for bribery,

corruption and inappropriate influence if not appropriately controlled. Robust internal policies and public disclosure of any contributions made or received are essential to reduce risks and increase accountability.

**Specific issues covered under this risk area include political contributions; charitable donations and sponsorships; responsible lobbying policy; aims and topics of lobbying activities; lobbying expenditure; and gifts and hospitality. This section contains 7 questions (max. 14 points).**

### Supply Chain Management

Complex supply chains, involving multiple entities and operating across different geographies and sectors, are a regular feature in the defence industry. As tiers of suppliers become more remote from the principal contractor, the potential risks and opportunities for corruption become greater with less clarity over everything from conflicts of interest to beneficial ownership and financial transparency.

**Specific issues covered under this risk area include involvement of the procurement department; supplier due diligence; anti-bribery and corruption standards for suppliers; cascading standards throughout the supply chain; and high-level data on supplier allegations and ethical investigations. This section includes 5 questions (max. 10 points).**

### 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 sources of bribery and corruption risks in the sector. Despite extensive research and recognition of these risks, the use of agents and intermediaries in the defence sector remains opaque and often inappropriately regulated. In addition, compliance professionals are now consistently identifying joint ventures as an area of significant third party risk. The nature of joint ventures in the defence sector mean that companies can be minority partners working in unfamiliar or new markets, and may be required to engage with state-owned enterprises where the state may have a controlling interest.

**Specific issues covered under this risk area include policy on the use of agents; due diligence on agents and intermediaries, including beneficial ownership; ethical incentives for agents; transparency of contracted agents; high-level data on agent allegations and ethical investigations; due diligence on joint ventures; and anti-bribery and corruption standards in joint ventures. This section contains 10 questions (max. 20 points).**

### Offsets

Offsets represent one of the most opaque practices in the defence industry. Although offsets can fulfil an entirely legitimate purpose, the frequent lack of transparency and oversight makes them one of the most profound areas of corruption risk for the sector. In the EU, offsets are illegal in all sectors except for defence; yet a 2015 study indicates that at least 80 countries worldwide require offset arrangements when purchasing defence equipment, systems or services. In this light, a significant risk stems from those companies that publish little to no information on this practice.

**Specific issues covered under this risk area include policy on offsets; due diligence on offset projects and beneficiaries; transparency of contracted offset brokers; and transparency of beneficiaries of indirect offset projects. This section contains 4 questions (max. 8 points).**

### High Risk Markets

As multinational companies develop and expand into new and emerging markets, the ability of businesses to identify and impose controls on the relevant corruption risks will continue to be a crucial part of good practice. Between 2013 and 2017, nine of the top ten global importers were rated as being at high or very high risk of defence sector corruption. In almost all cases, the level of risk in a particular market is determined by the depth 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.

**Specific issues covered under this risk area include risk management in countries identified as at high risk of corruption; public disclosure of subsidiaries and other holdings; public disclosure of beneficial ownership; and breakdown of defence sales by customers. This section contains 4 questions (max. 8 points).**

### State-Owned Enterprises

State-owned enterprises (SOEs) may not pose an inherent corruption risk. But such companies can encounter particular vulnerabilities that privately-owned companies may 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.

**Specific issues covered under this risk area include public disclosure of shareholder voting rights; commercial**

**and public policy objectives; nomination, appointment and composition of the board; composition of the audit committee; and management of asset transactions. This section contains 5 questions (max. 10 points).**

Further information about these corruption risk areas can be found in our report, 'Out of the Shadows: Promoting Openness and Accountability in the Global Defence Industry'.

# ANNEX II: QUESTIONNAIRE AND MODEL ANSWERS (QMA) 2020

The full Questionnaire and Model Answer document, with specific scoring criteria for each question, can be found on the DCI website, available at: [www.ti-defence.org/dci](http://www.ti-defence.org/dci).

## 1. Leadership & Organisational Culture

- 1.1 Does the company have a publicly stated anti-bribery and corruption commitment, which is authorised and endorsed 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 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?
- 2.3 Does the company have a system for tracking, investigating and responding to bribery and corruption allegations or incidents, including those reported through whistleblowing channels?
- 2.4 Does the company have appropriate arrangements in place to ensure the quality of investigations?
- 2.5 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?
- 2.6 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 and that covers the following categories of possible conflict:
- a) Employee relationships;
  - b) Government relationships;
  - c) Financial interests; and
  - d) Other employment.
- 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 and Intermediaries

- 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?

## ANNEX III: THE ASSESSMENT PROCESS (IN DEPTH)

The 2020 DCI assessment process consists of seven distinct stages, with ongoing feedback and review. A team of five independent assessors was recruited to undertake the assessments,<sup>7</sup> with support and internal reviews by Transparency International Defence and Security team members. All five assessors attended a three-day in-person training led by TI-DS, in which each question was discussed in detail to ensure a comprehensive understanding of the concepts, materials and practical applications of the Questionnaire and Model Answer (QMA) document. Assessors were also required to conduct a test assessment prior to formally beginning the assessment phase, to identify and provide further clarity on any outstanding issues. All of these factors contributed to strengthening the consistency and credibility of (and between) assessments.

TI-DS divided the research process into seven stages, which included:

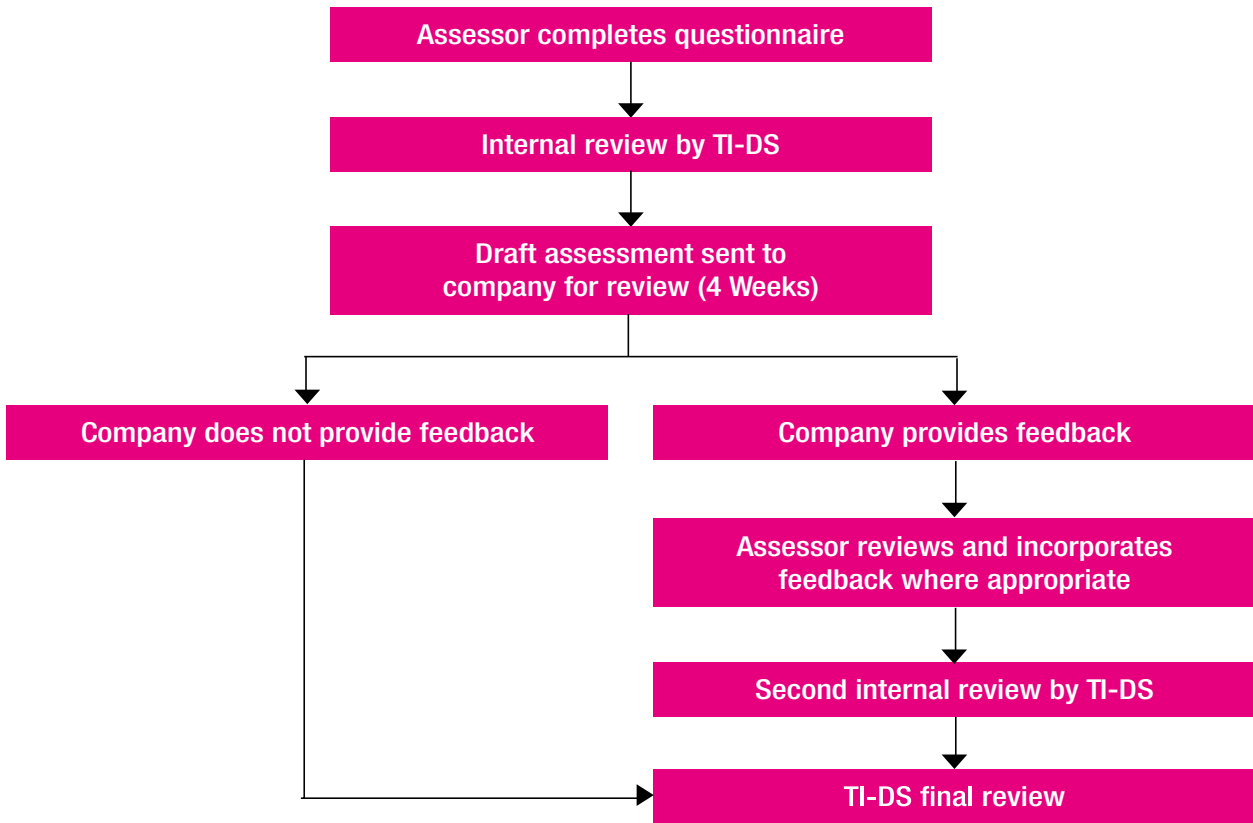
- An assessor conducted a review of all publicly available information on a company's website, copying the relevant evidence into the assessment template and assigning a score based on the QMA criteria.
- TI-DS then conducted an internal review on the draft assessment, to ensure alignment and consistency between the evidence provided and the score assigned, as well as to check that all evidence is properly cited. Assessors made and incorporated changes identified by TI-DS where relevant, to ensure the quality of assessments.
- Once the first assessment was approved internally, the draft assessment was sent to the company, where points of contact then had four weeks to review the evidence, provide feedback and make changes to their publicly available evidence where appropriate. Further information on the company review is available below.
- In the event that a company did not provide feedback, the assessment proceeded to the final review and standardisation phase.
- In the event that a company did provide feedback on its first assessment and/or decided to make changes to its publicly available materials on this basis, the document returned to an assessor for a second assessment. The assessor was responsible for reviewing the assessment alongside the company feedback and for making changes to the evidence and scoring where necessary, ultimately producing a second draft. Assessors were also tasked with verifying that information provided by companies was available in the public domain; if not, this information was not taken into account as evidence.
- The second assessment, complete with any new evidence or changes to scoring as a result of company feedback, was then subject to a second internal review by TI-DS. In this instance, the internal review focused on ensuring that any changes to scoring were appropriately reflected in the evidence (and vice-versa), and to ensure that any changes were implemented consistently throughout the assessment.
- Finally, all assessments were subject to a final review. This process involved a review of the specific evidence and score assigned to each question and between assessments, to ensure consistent application and interpretation of the QMA criteria. The overall score assigned to the company following this process was taken as the final result.

The full duration of this process for one company varied significantly depending on the volume and complexity of the publicly available information, as well as the amount of changes identified by TI-DS in the review process. Overall, the assessment process for the DCI 2020 took place over a 16 month period.

All companies received a full copy of their final assessment and overall scores two weeks prior to publication by TI-DS. Companies were given the opportunity to provide a response to be published alongside their final results on the website.

<sup>7</sup> Assessors were required to declare any actual, potential or perceived conflicts or interests in the recruitment phase. Assessors remain anonymous; company assessments will not be attributed to a specific assessor.





## COMPANY REVIEW AND FEEDBACK

TI-DS made a concerted effort to contact all companies at the initial launch of the project, to identify a point of contact (POC) for each company. Letters were sent to individual CEOs in good time before the public consultation period, and emails were also sent to any POCs identified through desk research. Company representatives were also invited to submit their contact details through an online form so that, once verified by the TI-DS team, they could be added to the mailing list. TI-DS took active steps to ensure that these contact details were updated as necessary throughout the duration of the project.

As described in the section above, the assessment process provided companies with the formal opportunity to respond and provide feedback on a draft version of their assessment prior to final review. Each company was automatically given a period of four weeks from receipt of the assessment to provide feedback, using a standardised template provided by TI-DS. In some cases, companies requested extended deadlines in order to make substantial changes to their publicly available materials; which were mutually agreed with TI-DS. Where no company POCs could be identified – through desk research, online submission and letters to CEOs – the assessment was fast-tracked directly to final review.<sup>8</sup>

The company review and feedback period served the

following purposes:

- To increase the validity and credibility of the data, by allowing companies the opportunity to highlight any misinterpretations or omissions of relevant public information;
- To provide an initial platform for engagement with companies, many of whom decided to make alterations or additions to their publicly available information on the basis of the QMA criterion;
- To enhance understanding of the DCI and the concepts that it encompasses to raise awareness of risk areas, mitigations and the importance of transparency with defence companies.

Assessors reviewed all information provided by companies in their feedback and considered new details alongside the assessment to determine any necessary and appropriate changes to the evidence and/or scoring. It is important to note that assessors were only able to make changes to the draft assessment if prompted and sign-posted by the company in the feedback template. Assessors did not undertake a full re-assessment of the company's publicly available materials as a result of the feedback, due to the high volume of publicly available evidence per company.

<sup>8</sup> There were three companies where no point of contact could be identified. These included: Komatsu Ltd, PT. Dirgantara Indonesia (Persero), and Toshiba Infrastructure Systems. In each case, hard copies of the announcement letter and final assessment were posted to the company's corporate headquarters as listed on its website.

# ANNEX IV: COMPANIES SELECTED FOR ASSESSMENT IN 2020

The companies subject to assessment on the 2020 DCI were selected based on two external ranking sources – one produced by the Stockholm International Peace Research Institute (SIPRI) and one produced by Defense News – as well as an assessment of large national defence companies from countries not represented on these lists, to ensure a geographic spread. Further information on this process can be found in the ‘Company Selection’ section of this paper.

The 2020 DCI covers 134 of the world’s largest defence companies across 38 countries. The below list was compiled at the launch of the project, with some minor changes based on mergers and acquisitions throughout the process highlighted in the footnotes.

Company	Country (HQ)
AAR Corporation	United States
Abu Dhabi Shipbuilding	United Arab Emirates
Accenture PLC	Ireland
AECOM	United States
Aerojet Rocketdyne <sup>9</sup>	United States
Airbus SE	Netherlands
Almaz-Antey	Russia
Arab Organisation for Industrialisation (AOI)	Egypt
Arsenal JSCo.	Bulgaria
Aselsan A.S.	Turkey
Austal	Australia
Aviation Industry Corporation of China (AVIC)	China
Babcock International Group PLC	United Kingdom
BAE Systems PLC	United Kingdom
Ball Aerospace & Technologies Corporation	United States
Battelle Memorial Institute	United States
Bechtel Corporation	United States
BelTechExport Company JSC	Belarus
Bharat Dynamics	India
Bharat Electronics	India
Boeing	United States
Booz Allen Hamilton Inc.	United States
CACI International Inc.	United States
CAE Inc.	Canada
CEA Technologies	Australia
Chemring Group PLC	United Kingdom
China North Industries Group Corporation (NORINCO)	China
China Shipbuilding Industry Corporation (CSIC)	China

<sup>9</sup> Formerly GenCorp.

Cobham Ltd	United Kingdom
Cubic Corporation	United States
Curtiss-Wright Corporation	United States
Daewoo Shipbuilding & Marine Engineering	South Korea
Damen Schelde Naval Shipbuilding	Netherlands
Dassault Aviation	France
Day & Zimmerman	United States
Denel SOC	South Africa
Diehl Stiftung & Co. KG	Germany
DynCorp International	United States
Elbit Systems	Israel
Embraer S.A	Brazil
Excalibur Army	Czech Republic
Fincantieri S.p.A	Italy
Fluor Corporation	United States
Fujitsu Ltd.	Japan
General Atomics	United States
General Dynamics Corporation <sup>10</sup>	United States
General Electric Aviation	United States
GKN Aerospace	United Kingdom
Glock	Austria
Hanwha Aerospace	South Korea
Harris Corporation	United States
Hewlett-Packard Enterprise Company	United States
High Precision Systems	Russia
Hindustan Aeronautics Ltd.	India
Honeywell International	United States
Huntington Ingalls Industries Inc.	United States
Hyundai Rotem Company	South Korea
IHI Corporation	Japan
IMI Systems Ltd. <sup>11</sup>	Israel
Indian Ordnance Factories	India
Indra Sistemas S.A.	Spain
Israel Aerospace Industries Ltd.	Israel
Japan Marine United Corporation	Japan
Kawasaki Heavy Industries Ltd.	Japan
KBR Inc.	United States
King Abdullah II Design and Development Bureau	Jordan
Komatsu Ltd.	Japan

<sup>10</sup> General Dynamics Corporation acquired CSRA in April 2018, and as such CSRA was removed from the assessment.

<sup>11</sup> Formerly Israel Military Industries. IMI Systems was formally acquired by Elbit Systems in November 2018; however, since the two companies maintain individual websites with distinct policies and procedures, the two companies are assessed as two separate entities. See: Elbit Systems, 'Elbit Systems Completes the Acquisition of IMI Systems', 25 November 2018, <https://elbitsystems.com/pr-new/elbit-systems-completes-the-acquisition-of-imi-systems/>.

## 23 Defence Companies Index (DCI) 2020: Methods Paper

Kongsberg Gruppen ASA	Norway
Korea Aerospace Industries	South Korea
Krauss-Maffei Wegmann GmbH & Co.	Germany
L3 Harris Technologies <sup>12</sup>	United States
Leidos Inc.	United States
Leonardo S.p.A	Italy
LiG Nex1 Co., Ltd.	South Korea
Lockheed Martin Corporation	United States
ManTech International Corporation	United States
MBDA Missile Systems	France
Meggitt PLC	United Kingdom
Massachusetts Institute of Technology (MIT)	United States
Mitre Corporation	United States
Mitsubishi Electric Corporation	Japan
Mitsubishi Heavy Industries Ltd.	Japan
Moog Inc.	United States
Nammo AS	Norway
Naval Group <sup>13</sup>	France
Navantia S.A	Spain
NEC Corporation	Japan
Nexter Group	France
Northrop Grumman Corporation <sup>14</sup>	United States
OGMA – Indústria Aeronáutica de Portugal SA	Portugal
Oki Electric Industry	Japan
Oshkosh Corporation	United States
Patria Oyj	Finland
Perspecta <sup>15</sup>	United States
Polish Defence Holdings	Poland
Poongsan Corporation	South Korea
PT Dirgantara Indonesia (Persero)	Indonesia
QinetiQ Group	United Kingdom
Rafael Advanced Defense Systems Ltd.	Israel
Raytheon Company <sup>16</sup>	United States
Rheinmetall A.G	Germany

<sup>12</sup> L3 Harris Technologies is the result of an equal merger between L3-Technologies and Harris Corporation, which was finalised in June 2019. The merger was finalised prior to assessment of either company, so the company was assessed as the new entity, L3 Harris Technologies.

<sup>13</sup> Formerly DCNS.

<sup>14</sup> Northrop Grumman formally completed its acquisition of Orbital ATK in June 2018, resulting in the latter entity being removed from the assessment list. See: Northrop Grumman, 'Northrop Grumman Completes Orbital ATK Acquisition', 6 June 2018, <https://news.northropgrumman.com/news/releases/northrop-grumman-completes-orbital-atk-acquisition-blake-larson-elected-to-lead-new-innovation-systems-sector>.

<sup>15</sup> Formerly Vencore.

<sup>16</sup> United Technologies Corporation (UTC) and Raytheon Company completed an equal merger resulting in the creation of Raytheon Technologies Corporation in April 2020. A full assessment of Raytheon, including company feedback and a resulting second assessment, had been completed at the time of the merger finalisation; whereas a first assessment of UTC had been conducted but without company review. As a result, it was mutually agreed between TI-DS and the company that the original assessment of Raytheon would remain unchanged and UTC would be removed from the index due to inability to respond or make changes; noting that many of these legacy anti-corruption and compliance procedures remain in place for the foreseeable future. See: Raytheon Technologies, 'United Technologies and Raytheon Complete Merger of Equals Transaction', 3 April 2020, <https://investors.rtx.com/static-files/1d0010bd-9a41-4be8-b797-0048967463ae>. It should also be noted that Rockwell Collins was removed from the assessment list after it was acquired by UTC in 2017; the company is now part of the Raytheon Technologies group.

Roketsan	Turkey
Rolls Royce PLC	United Kingdom
Rostec (Concern Radioelectronic Technologies, JSC)	Russia
RTI Systems	Russia
RUAG Holding Ltd.	Switzerland
Russian Helicopters	Russia
Saab AB	Sweden
Safran S.A	France
Science Applications International Corporation (SAIC)	United States
Serco Group PLC	United Kingdom
ST Engineering	Singapore
STM Savunma Teknolojileri Muhendislik ve Ticaret A.S.	Turkey
Tactical Missiles Corporation, JSC	Russia
Turkish Aerospace Industries	Turkey
Tashkent Mechanical Plant	Uzbekistan
Tatra Trucks A.S.	Czech Republic
Telephonics Corporation	United States
Terma A.S.	Denmark
Textron	United States
Thales Group	France
The Aerospace Corporation	United States
ThyssenKrupp AG	Germany
Toshiba Infrastructure Systems	Japan
Triumph Group Inc.	United States
Ukroboronprom	Ukraine
Ultra Electronics Holdings PLC	United Kingdom
United Aircraft Corporation	Russia
United Engine Corporation	Russia
United Instrument Manufacturing Corporation	Russia
United Shipbuilding Corporation	Russia
Uralvagonzavod	Russia
Vectrus <sup>17</sup>	United States
ViaSat Inc.	United States
Zastava Arms	Serbia

---

<sup>17</sup> Formerly Exelis.

# ANNEX V: FULL LIST OF DEFINITIONS

**Accountability** is the concept that individuals, agencies and organisations (public, private and civil society) are held responsible for reporting their activities and for executing their powers properly. It also includes the responsibility for money or other entrusted property.

**Agents** are defined 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. Agents pose distinct risks compared to other types of intermediaries, because they are authorised to act on the company's behalf, often with a high level of discretion and minimal oversight, and their activities usually involve close interaction with public officials. The terms agent and broker are often used interchangeably.

An **anti-bribery and corruption programme** is defined here as the company's anti-bribery efforts including values, code of conduct, detailed policies and procedures, risk management, internal and external communication, training and guidance, internal controls, oversight, monitoring and assurance.

An **audit** is defined as an internal or external examination of an organisation's accounts, processes, functions and performance to produce an independent and credible assessment of their compliance with applicable laws and regulations.

A **beneficial owner** is the real person who ultimately owns, controls or benefits from a company or trust fund and the income it generates.

The **board of directors** is the corporate body charged with the functions of governing the enterprise. Directors can be executive or non-executive, dependent on whether that person engages in the day-to-day management of the company, and independent or non-independent, dependent on whether that person holds shares or other interests in the company.

**Bona fide** refers to an act made in good faith without an intention to engage in undue action. The term can be included in policies regarding gifts, hospitality or expenses.

**Bribery** is defined as the offering, promising, giving, accepting or soliciting of an advantage as an inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of money, gifts, loans, fees, rewards or other advantages (taxes, services, donations, favours etc.).

A **code of conduct** is a statement of principles and values that establishes a set of expectations and standards for how an organisation, government body, company, affiliated

group or individual will behave, including minimal levels of compliance and disciplinary actions for the organisation, its staff and volunteers.

**Compliance** refers to the procedures, systems or departments within public agencies or companies that ensure all legal, operational and financial activities are in conformity with current laws, rules, norms, regulations, standards and public expectations.

**Conflict of interest** (CoI) is defined here as a situation where an individual or the entity for which they work, whether a government, business, media outlet or civil society organisation, is confronted with choosing between the duties and demands of their position and their own private interests.

A **cooling-off period** is a time-limited restriction on the ability of former politicians or public officials to accept appointments to positions in the private sector.

**Corruption** is defined as the abuse of entrusted power for private gain. Corruption can be classified as grand, petty and political, depending on the amounts of money lost and the sector where it occurs.

**Due diligence** refers to an investigation or audit of a potential business, investment, or individual prior to entering into a business transaction or appointment of individuals.

**Facilitation payments** are defined here as a small bribe, also called a 'facilitating', 'speed' or 'grease' payment; made to secure or expedite the performance of a routine or necessary action to which the payer has legal or other entitlement.

A **gift** is defined as money, goods, services or loans given ostensibly as a mark of friendship or appreciation. A gift is professedly given without expectation of consideration or value in return. A gift may be used to express a common purpose and the hope of future business success and prosperity. It may be given in appreciation of a favour done or a favour to be carried out in the future.

**Hospitality** refers to entertainment given or received to initiate, develop or strengthen relationships, including meals, receptions, tickets to entertainment, social or sports events, and participation in sporting events. The distinction between hospitality and gifts can blur, especially where the giver of the hospitality does not attend and act as a host.

**Incentives** are defined as "payments to employees that are linked to the achievement of set targets designed to motivate people to achieve higher levels of performance". Typically such targets are quantified and measured in

terms of outputs, such as production and sales, and profits. Increasingly, targets also include other factors such as safety and quality.

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.

**Lobbying** is defined as any activity carried out to influence a government or institution's policies and decisions in favour of a specific cause or outcome. Even when allowed by law, these acts can become distortive if disproportionate levels of influence exist – by companies, associations, organisations and individuals.

**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. This can be done through both direct offsets, i.e. defence-related projects such as sub-contracting, or through indirect offsets, i.e. defence-unrelated enterprises such as purchases of goods or services. In this index, the term 'offset contracting' refers to both direct and indirect offset agreements, or any other terms to indicate such arrangements (e.g. counter-trade agreements).

**Offset beneficiaries**, for the purpose of this assessment, include the customer with whom the offset contract is negotiated; as well as any business partnerships formed in pursuance of the offset contract such as joint ventures.

**Offset brokers**, for the purpose of this assessment, are defined as dedicated third parties who are contracted to negotiate, arrange and provide advice on offset arrangements for or on the company's behalf. These brokers can include agents, intermediaries, marketing or consultancy firms and expert individuals.

**Oversight** is the process of independently monitoring and investigating – internally or externally – the operations and activities of a government agency, company or civil society organisation to ensure accountability and efficient use of resources.

**Political engagement** refers to the ways in which an enterprise contributes to or participates in the political process. This can include but is not limited to activities such as making political contributions, indirect political expenditure, advocacy and lobbying, lobbying through trade associations and other membership bodies, training of public sector officials and political activities related to the workplace.

A **politician** refers to a member of the legislature; an individual who is actively engaged in conducting the business of a government.

A **public official** refers to any person holding a legislative,

executive, administrative or judicial office, whether appointed or elected; and any person exercising a public function, including for a public agency or public enterprise.

A **risk assessment** is a systematic and continuing process for identifying and analysing inherent risks to enable an assessment of their likelihood and impact on the enterprise's ability to achieve its commitments and objectives. Within the framework of the risk approach of the enterprise, the results of anti-corruption risk assessments are used to identify and prioritise risks and to design controls for the anti-corruption programme to be implemented to mitigate the risks.

A **state-owned enterprise (SOE)** is defined broadly as an entity that is owned or controlled by the state that carries out activities that are commercial or for public policy objectives, or a combination of these. For the purposes of a TI-DS methodology, an SOE will be defined as an enterprise where the state has significant control through full, majority or significant minority ownership (OECD 2015).

A **subsidiary** is a company that is owned or controlled by another company, which is usually referred to as the parent company or holding company. **Fully consolidated subsidiaries** are entities which are fully or majority-owned by the parent company. Their financial statements are fully accounted for in the group consolidated financial statements. **Non-fully consolidated holdings** are entities of which the parent company owns (controls) between 20% and 50% and they are consolidated by the equity method.

A **supplier**, for the purpose of this assessment, refers to any company that has a direct business relationship and/or interaction with the main company (sometimes known as tier one or first generation suppliers). A company's **supply chain** refers more broadly to all contracted suppliers, contractors, sub-contractors and vendors.

A **third party**, for anti-corruption purposes, is a prospective or contracted business associate, including agents, distributors, lobbyists, brokers, consultants and other intermediaries, joint venture and consortia partners, contractors, vendors and suppliers.

**Transparency** means being open in the clear disclosure of information, rules, plans, processes and actions. As a principle, public officials, civil servants, the managers and directors of companies and organisations, and board trustees have a duty to act visibly, predictably and understandably to promote participation and accountability and to allow third parties to easily perceive what actions are being performed.

**Whistleblowing** involves a disclosure 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, government body or company (or one of its business partners) that threaten public interest, its integrity and reputation.

