DEFENCE AND SECURITY SECTOR POLICY

cdp

CONTENTS

1. INTRODUCTION AND PURPOSES OF THE DOCUMENT

The CDP Group promotes the country's growth, both in its capacity as a permanent shareholder in strategic infrastructure and assets, and by implementing special purpose actions aimed at business growth and international expansion in key sectors.

The progressive expansion of the role and operations of Cassa Depositi e Prestiti S.p.A. (hereinafter "CDP"), reflected in the 2021 amendment to its Articles of Association[1], makes it necessary to adopt precise guidelines, as defined in the Strategic Plan. These guidelines provide for the systematic integration of environmental, social and governance aspects throughout the Financing and Investment process, as these are considered essential factors for ensuring sustainable development and the generation of greater value for both the companies in which it invests and for the community as a whole.

Therefore, CDP deems it appropriate to adopt specific strategies in certain sectors that are important for the Italian economy and that require specific guidelines for the allocation of resources.

In particular, the Defence and Security Sector is a strategic sector in terms of ensuring the security of countries but is also one of the most debated sectors in terms of compatibility with the sustainability criteria.

The relationship between banks and the businesses involved in the production and trade of defence materials has long been the focus of attention of investors, customers, non-governmental organisations and society at large. With the ultimate aim of contributing to peace processes, these stakeholders seek to prevent financiers and companies from being involved in operations concerning so-called "controversial" weapons, or involving countries subject to international sanctions or responsible for serious human rights violations, and to ensure that terrorism financing and the illegal arms trade are avoided. Moreover, given the limited transparency of governmental weapons procurement processes, for obvious security reasons, even more attention needs to be paid to the prevention of corruption.

In recent years, alongside initiatives undertaken by international institutions to promote disarmament, non-proliferation of weapons and the establishment of arms trade control systems, there has been a growing debate on the need to strengthen support for the defence sector, as a result of recent geopolitical and international developments, in order to safeguard economic security and the resilience of the national system.

Recent geopolitical and international developments have also highlighted the urgency of ensuring greater protection of both physical and virtual resources. The increasing exposure of companies, citizens and public institutions to cyber threats has made it essential to strengthen, in a coordinated manner, the capacities for prevention, resilience and protection of strategic resources, both physical and digital, ensuring effective security for citizens, businesses and public institutions.

Defence and security essentially refers to a set of systems designed to protect the integrity of a State's territory and safeguard its citizens and public institutions. Accordingly, strategies and production choices are defined by the State concerned, which, for companies operating in Italy, is the Italian government.

In light of this context, and mindful of its role within the country, in 2022 CDP adopted a sector policy governing its approach to the Defence and Security Sector, with the aim of ensuring support for a sector that is strategic for the country, while at the same time safeguarding its economic and financial, sustainability and reputational objectives.

This Policy, consistent with CDP's General Responsible Lending and Investment Policies, therefore aims to guide CDP's operations in the Defence and Security Sector by establishing the related treatment, limitation and exclusion criteria.

[1] Introduction of the principle of sustainable development: "The company's corporate purpose, in pursuing long-term economic, social and environmental sustainability to the benefit of shareholders and taking account of the interests of other stakeholders relevant to the company, is..."

This document describes:

- the reference context (chapter 2);
- the scope of application (chapter 3);
- the CDP's position in the Defence and Security Sector (chapter 4);
- the roles and responsibilities of the parties involved (chapter 5);
- how transparency and accountability are ensured (chapter 6).

This document is subject to periodic review, also in order to reflect, by way of example and without limitation, regulatory and legislative developments, changes in the relevant context and/or the adoption of a new strategic plan. In any case, the review shall take place every three years.

This Policy, where appropriate, should be read in conjunction with other policies, in particular with the General Responsible Lending and Investment Policies and the relevant company and/or Group regulatory framework.

2. REFERENCE CONTEXT

2.1 External regulatory and legislative context

At the time of the update of this Policy, the main international regulatory framework includes the following Treaties, Conventions and Regulations:

- Geneva Protocol (1925), prohibiting the use of asphyxiating, poisonous, or other gases, and bacteriological methods in warfare;
- Partial Test Ban Treaty (1963), prohibiting nuclear tests where such explosions cause radioactive debris outside the permitted limits;
- Treaty on the Non-Proliferation of Nuclear Weapons (1970), an international treaty whose objective is to prevent the spread of nuclear weapons and to further the goal of achieving nuclear disarmament;
- Biological Weapons Convention (1975), prohibiting the development, production and retention of bacteriological (biological) and toxin (viruses, bacteria, microorganisms, spores, toxins) weapons, with the requirement to destroy existing stock.
- ENMOD Convention (1978), prohibiting military or any other hostile use of environmental modification techniques;
- Convention on prohibitions or restrictions on the use of certain conventional weapons (Convention on Certain Conventional Weapons, 1980) which may be deemed to be excessively injurious or to have indiscriminate effects;
- Wassenaar Arrangement (1996), promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. With the updates introduced in 2013 and 2015, these safeguards were also extended to software and cyber tools, including those intended for cyber-espionage and cyber-attacks;
- Comprehensive Nuclear-Test-Ban Treaty (1996), banning all nuclear tests in all environments, both for military or peaceful purposes;
- Anti-Personnel Mine Ban Treaty (Ottawa Convention, 1997), a convention on the use, stockpiling, production and transfer of anti-personnel mines and on their destruction, including the requirement to provide assistance to mine victims;
- Chemical Weapons Convention (CWC, 1997), the first instrument of international law on disarmament, prohibiting the development, production, acquisition, retention, stockpiling, transfer and use of chemical weapons and any associated material;
- United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons (2001);
- Hague Code of Conduct against ballistic missile proliferation (HCOC, 2002), regulating ballistic missiles capable of delivering weapons of mass destruction, which aims to act as a transparency and confidence building instrument concerning the spread of ballistic missiles. The subscribing States voluntarily commit to provide pre-launch notifications on ballistic missile and space-launch vehicle launches and test flights;
- Budapest Convention (ETS No. 185) of 2004, the first international treaty against cybercrime, which establishes common standards and promotes cooperation among States to combat digital offences. In 2023, a Second Additional Protocol was adopted to enhance international cooperation, introducing expedited procedures for the sharing of electronic evidence and for direct cooperation with service providers;

- Convention of Cluster Munition (Oslo Convention, 2008), prohibiting the use, stockpiling, production and transfer of cluster munitions, with the requirement to destroy existing stock;
- Council Common Position 2008/944/CFSP of the European Union of 8 December 2008 (as subsequently amended), which defines common rules governing the control of exports of military technology and equipment;
- Arms Trade Treaty (2014), setting out the criteria for authorising (or prohibiting) the transfer of conventional arms;
- Treaty on the Prohibition of Nuclear Weapons (2017), which includes undertakings not to develop, test, produce, acquire, possess, stockpile, use or threaten to use nuclear weapons;
- United Nations Global Treaty on Cybercrime (adopted in 2024, with entry into force expected after 2026), a binding international agreement that strengthens the 2001 Budapest Convention and encourages international cooperation in the prevention of cybercrime, addressing offences such as terrorism, human trafficking, drug trafficking and online financial crimes;
- European Council Regulation (EC) No. 1236/2005 concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment;
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 (Cybersecurity Act), which strengthens the mandate of ENISA, by establishing it as the European Union Agency for Cybersecurity with permanent coordination and support tasks for the Member States, and establishes a European cybersecurity certification framework for ICT products, services and processes, aimed at ensuring common standards, reducing regulatory fragmentation and increasing trust in the European digital market;
- Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items;
- European Directive 2022/2555, known as the Network and Information Security Directive (hereinafter "NIS2"), which establishes a unified legal framework to ensure a high level of cybersecurity within the EU, extending its scope to 18 critical sectors, introducing strict obligations on risk management and incident notification, and strengthening the accountability of corporate business units;
- Regulation (EU) 2025/38, known as the Cyber Solidarity Act (CSoA), in force from 2025, complements the NIS2 Directive and introduces measures to strengthen the EU's capacity to address cyber threats, including a network of European cyber hubs and cyber incident response mechanisms.

The UN's 2030 Agenda also aims to make a contribution to setting up sound and transparent national arms control systems. In fact, the achievement of many of the goals of the Agenda are dependent on reducing armed violence and improving international security.

At national level, the main regulatory reference in the field of armaments is Law No. 185/90, as amended (and its implementing regulations), which governs the control of the export, import and transit of armaments materials and provides for administrative financial penalties in the event of breaches of the obligations set out therein.

The national framework is supplemented by the following provisions:

- Italian Law No. 220 of 9 December 2021, which introduces, on the one hand, a prohibition on the financing, in any form, of companies involved in the construction, production, development, assembly, repair, preservation, use, storage, stockpiling, retention, promotion, sale, distribution, export, transfer or transportation of anti-personnel mines, cluster munitions and submunitions and any part thereof, and on the other hand, a prohibition on carrying out (or providing support in carrying out) any technological research or activity that involves the manufacture, sale and transfer, on any basis, export, import and holding of cluster munitions and submunitions or any part thereof;
- Instructions issued by the Bank of Italy, COVIP, IVASS and the Ministry of Economy and Finance (MEF) to counter the financing of companies producing anti-personnel mines, cluster munitions and submunitions, in implementation of Article 3, paragraph 1, of Law No. 220 of 9 December 2021;
- Italian Law No. 110 of 18 April 1975, which regulates the control of weapons, munitions and explosives and provides a definition for both military weapons and conventional firearms.

Similarly, with specific reference to data security, the Government has supported the efforts of the main national and international institutions in promoting cybersecurity measures, by adapting the regulatory framework through the following measures:

- Decree-Law No. 105 of 21 September 2019, converted with amendments into Law No. 133 of 18 November 2019, which establishes the National Cybersecurity Perimeter (PSNC), defining the scope, entities and procedures for the protection of networks, information systems and IT services of national interest, as well as the coordination and supervisory tasks assigned to the Presidency of the Council of Ministers and the Department of Information for Security (DIS);
- Legislative Decree No. 123 of 3 August 2022, which regulates the national certification framework and updates Italian legislation in line with Title III of the Cybersecurity Act (Regulation (EU) 2019/881), defining the parties involved, the procedures for the issuance and control of cybersecurity certifications, as well as the responsibilities of the National Cybersecurity Agency as the competent authority;
- Law No. 90 of 21 June 2024, which further strengthens the national cybersecurity system by introducing measures for the coordinated implementation of digital security policies, enhancing the operational functions of the National Cybersecurity Agency and promoting public–private cooperation in the protection of critical infrastructure, with subsequent implementing decrees (e.g. Prime Minister's Decree of 30 April 2025) defining its operational organisation and inter-institutional coordination arrangements;
- Legislative Decree No. 138 of 18 September 2024, which transposes EU Directive 2022/2555 (NIS2), strengthening the cybersecurity of critical networks and information systems, as well as of public and private entities operating in essential sectors (e.g. energy, healthcare, transport, etc.), and assigning to the National Cybersecurity Agency tasks of coordination, supervision and support for the implementation of security measures.

2.2 Main related internal regulations

The internal corporate regulatory sources, in addition to this document, by which CDP upholds and acknowledges the principles of sustainability as fundamental values, include, but are not limited to:

- Articles of Association;
- Code of Ethics;
- Organisation, Management and Control Model pursuant to Legislative Decree no. 231/2001;
- Sustainability Framework;
- General Responsible Lending Policy
- General Responsible Investment Policy
- Energy Sector Policy;
- Transport Sector Policy;
- Agrifood, Wood and Paper Industries Sector Policy;
- General Stakeholder Engagement Policy;
- General Stakeholder Grievance Mechanism Policy;
- General Diversity, Equity and Inclusion Policy;
- General Risk Policy;
- Credit Risk Policy.

This document should be read in conjunction with the general policies, in particular those on Responsible Financing and Investment.

The regulatory and legislative framework is also supported by further internal regulatory provisions that set out the principles, methods and operational arrangements through which sustainability is implemented within the organisation and in relation to Defence and Security Sector operations, including, for example, the Group Operational Instruction on "Regulatory and Operational Requirements for the Defence and Security Sector".

3. SCOPE OF APPLICATION

3.1 Scope by type of operation

The scope of application of this document relates to CDP's operations in the Defence and Security Sector, with reference to transactions originated after the approval of this document[2], both in terms of Investment (on a direct basis and, where possible, on an indirect basis) and Financing (on a direct basis only[3]), as well as the renewal of such transactions. This Policy does not apply to transactions[4] relating to equity investments already held in the portfolio, nor to amendments to Financing agreements. With regard to investments in the portfolio, in line with the provisions of the General Responsible Investment Policy, to which reference should be made, CDP conducts ongoing monitoring and engages with the company management to discuss possible guidelines with regard to development plans and to conduct specific analyses on ad hoc issues. These regular engagement activities also make it possible to identify any problems that arise in the investment management phase and jointly agree what actions need to be implemented, to be successively verified through appropriate monitoring.

It is specified that, within the scope of its institutional mission, CDP is also required, by virtue of specific legislative provisions and/or dedicated mandates, to manage third-party funds (e.g. resources from Ministries). Activities in this area are carried out in compliance with the applicable regulatory requirements and the guidelines of the relevant institutions.

In addition, in order to tighten the criteria for transactions in the sector, real estate transactions involving the lease and/or transfer of real estate to Counterparties operating in the Defence and Security Sector are also included, in accordance with the provisions of paragraph 4.3 "Counterparty criteria".

It is further specified that the exclusion criteria relating to Counterparties apply to all transactions, irrespective of the sector.
A transaction is deemed to fall within the Defence and Security Sector in the following cases:

i. A Financing/Investment transaction with a general purpose, where the Counterparties have generated at least 20% of their turnover from the Defence and Security Sector over the past three financial years;
ii. A Financing/Investment transaction with a specific purpose, where the main subject matter consists of goods attributable to the Defence and Security Sector.

Considering that CDP pays particular attention to the reputational aspects of export transactions in the Defence and Security Sector, resolutions concerning such transactions shall be passed exclusively by the Board of Directors of CDP, upon proposal of the Chief Executive Officer, subject to the non-binding mandatory opinion of the Risk and Sustainability Committee.

CDP's Board of Directors may also approve exceptions or derogations from this document, in accordance with applicable internal regulations, always on a case-by-case basis, and on the basis of evaluations conducted by the relevant departments, and particularly with the General Responsible Lending Policy and the General Responsible Investment Policy.

3.2 Scope of the Company

This Policy applies, with the above specifications, to transactions carried out by CDP S.p.A. in the Defence and Security Sector.
CDP is committed to ensuring that the Companies subject to management and coordination[5] that have adopted a policy in the Defence and Security Sector consistent with CDP's Policy[6] implement the updates periodically made to this Policy, in line with the principle of proportionality and having regard to the decision-making autonomy of the Corporate Bodies of the Group Companies, especially the Regulated Entities[7], as well as the specific sector regulations applicable to them.

[2] The amendments introduced with this update shall apply to transactions originated from the date of approval of this Policy
[3] All forms of indirect financing are therefore excluded.
It is specified that the safeguards provided for under Law No. 220/2021 and the related Implementing Instructions apply to all transactions, including indirect transactions and/or those involving third-party funds, falling within the scope of application of that law as detailed in specific internal regulations, and in any event in compliance with the external regulations applicable to the relevant operations.
[4] This includes equity and similar transactions such as acquisitions, demergers, mergers, share conversions, corporate restructurings, shareholder financing or capital injections, subscriptions to hybrid instruments and convertibles, and capital increases, except where such increases relate to the acquisition of a company operating in the sector.
[5] Pursuant to Articles 2497 et seq. of the Italian Civil Code.
[6] SIMEST S.p.A., CDP Equity S.p.A.
[7] Companies subjected to a system of authorisations, regulations, inspections and information provision by sectoral Regulators (e.g. Bank of Italy and IVASS).

4. CDP'S ROLE IN THE DEFENSE AND SECURITY SECTOR

In compliance with the applicable regulatory and statutory framework, CDP directs its strategic and operational approach by allocating resources towards the priority areas identified in the Strategic Plan. With specific reference to the sector addressed by this document, CDP's 2025–2027 Plan has identified Economic Security and Strategic Autonomy as one of the macro strategic objectives, defining Security and Defence as an additional area of intervention for CDP's activities, supplementing the ten already set out in the 2022–2024 Plan. CDP intends to operate in the Defence and Security Sector with the aim of: (i) strengthening the country's production capacity in strategic areas by reducing dependence on production factors and critical inputs; (ii) contributing to the development and protection of critical infrastructure, particularly in the energy and digital sectors; (iii) enhancing the country's international standing by consolidating balanced economic relations from a strategic perspective and strengthening its commitment to international cooperation; and (iv) responding to the defence and security needs of States, including by contributing to the safeguarding of peace processes.

At the same time, CDP considers it to be of paramount importance that the Counterparties and the nations involved in the transactions have adequate control measures in place to ensure that the assets covered by the Policy are only used with due respect for human rights and in accordance with the principles established in the international treaties. Accordingly, CDP assesses the ability of the Counterparties and of the countries concerned to ensure that such goods are not used for purposes other than those set out in this Policy, including, but not limited to, use by terrorist organisations or other armed groups, use against the civilian population in violation of human rights, as well as the use of technological tools for unlawful purposes that may result in misuse, unauthorised access or digital compromise of the assets and the related information.

CDP's activities in the Defence and Security Sector are carried out in full compliance with the main international conventions and treaties on weapons and cybersecurity, with the regulations adopted at European level, and with Italian legislation. With specific reference to the latter, CDP ensures compliance with the provisions and information obligations set out in Law No. 185/1990, Legislative Decree No. 109/2007[8] (also referred to in Legislative Decree No. 231/2007), and Law No. 220/2021 and the related Implementing Instructions. Therefore, the provisions set out in this document are to be understood to supplement and not replace the provisions of those regulations.

In light of the foregoing principles, CDP has defined a number of criteria to guide its activities in the Defence and Security Sector. These criteria, as detailed in the paragraphs below, refer to:

- the type of defence and security assets covered by the transaction;
- the final recipient of the transaction;
- the Counterparty in the transaction;
- the country of destination of the assets covered by the transaction.

It is specified that, in the context of CDP's activities in the field of international cooperation, in addition to the exclusion criteria set out in the following paragraphs, the exclusions arising from CDP's participation in the European Development Finance Institutions (EDFI) also apply[9].

For transactions in the Defence and Security Sector, in addition to identifying cases of excluded transactions CDP has also defined a specific transaction assessment model with reference to the Counterparties and the countries of destination of the assets covered by the transaction. If the analysis conducted reveals issues of concern, the outcome of the assessments will contain a proposal to proceed with restrictions depending of the level of the concerns raised.

[8] Legislative Decree 109/2007 defines the financing of the proliferation of weapons of mass destruction as: "The provision or collection of funds and economic resources, in any manner carried out and instrumental, directly or indirectly, to support or facilitate all activities linked to the design or implementation of programmes aimed at developing weapons of a nuclear, chemical or biological nature." In accordance with its Anti-Money Laundering and International Financial Sanctions Policies, CDP applies specific enhanced controls to thoroughly assess the risk that a customer or transaction may be connected to proliferation, and to examine factors such as ownership structure transparency, transaction purpose, the involvement of high-risk countries, the economic rationale of the transaction, and the acquisition of sensitive goods or technologies.

[9] Harmonized EDFI Exclusion List: https://edfi.eu/wp-content/uploads/2024/10/EDFI-Exclusion-List_-September-2011.pdf

For the purposes of applying this Policy, CDP obtains from the Counterparty, in accordance with the procedures set out in the General Responsible Financing and Investment Policies and as detailed in the relevant internal regulations, the documentation required to carry out the assessments[10].

In certain specific circumstances, if deemed necessary, CDP may make use of an advisory contribution from independent experts to assist in the assessment of compliance to Policy requirements.

4.1 Criteria with regard to the nature of the transaction

CDP does not intend to support in any way whatsoever assets that have indiscriminate effects and may cause undue harm or serious injury, including but not limited to controversial weapons and/or instruments of torture.

Therefore, in the case of Financing/Investment transactions with a specific purpose, CDP does not participate, in any form, in transactions involving:

- controversial weapons[11] and/or their key components[12] such as:
  - nuclear weapons;
  - chemical weapons;
  - biological weapons;
  - depleted uranium weapons;
  - anti-personnel mines;
  - anti-tank mines;
  - cluster munitions and submunitions / bombs;
- conventional firearms, small arms and light weapons unless the transaction: (i) involves items to be used exclusively by the armed forces and/or the police[13] or (ii) refers to weapons that are manufactured and marketed for sporting purposes only or (iii) refers to weapons marketed in the EU member states;
- goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment[14];
- the following cyber weapons: digital tools or malicious software (e.g. malware, ransomware)[15] specifically designed to be used or intended to cause damage, destruction or compromise to IT systems, critical infrastructure, networks or data, unless such assets (i) are intended exclusively for the armed forces, police forces and/or governments[16], or (ii) are aimed at improving the resilience of corporate and/or public utility systems.

Transactions referring to the permitted defence materials and dual-use items are subject to verification of compliance with the additional criteria listed below.

4.2 Criteria with regard to end-users

CDP operates in the sector with the objective of meeting the defence and security needs of countries and therefore excludes transactions whose final recipients are private individuals or other organisations that may use the goods covered by this Policy for other purposes, such as terrorism or the unlawful use of acquired information and data, including through cyber-attacks or breaches of digital systems.

Accordingly, for Financing/Investment transactions with a specific purpose, CDP considers admissible only those transactions whose sole final recipient is a government or a company authorised by it, and which comply with the provisions of Law No. 185/1990.

[10] In carrying out its assessment activities, and in line with the provisions of the Group Policy on International Financial Sanctions, CDP complies with the measures set out therein.
[11] For a comprehensive definition of controversial weapons and the related legislation, please refer to the glossary.
[12] A critical component that is necessary for the operation of the controversial weapon and specifically designed for that purpose.
[13] The country of reference is assessed in accordance with paragraph 4.4, "Criteria for recipient countries", which sets out the related exclusion and assessment criteria.
[14] The goods set out in Regulation (EU) 2019/125.
[15] For a comprehensive definition of the main types of malicious software designed for cyber-attacks, please refer to the glossary.
[16] The country of reference is assessed in accordance with paragraph 4.4, "Criteria concerning recipient countries", which sets out the applicable exclusion and evaluation criteria.

4.3 Criteria with regard to Counterparties[17]

CDP intends to establish relations only with Counterparties that comply with the legislation in force, the international restrictions on weapons and the international treaties ratified in Italy.

In addition to compliance with the regulatory requirements, CDP intends to define further criteria to be met by the Counterparties.

CDP will therefore refrain from participating in any capacity in transactions that have as the Counterparty a company that:

- directly or indirectly[18] through subsidiary/associate companies or parent companies, carries out an activity that involves the production, trade, stockpiling, sale, transfer, import or export of controversial weapons[19] and/or their key components[20], or provides any service associated with such weapons, including technological research;
- manufactures and/or sells conventional firearms, small arms and light weapons, unless the transaction: (i) is intended exclusively for the armed forces and/or law enforcement, or (ii) is solely for research and development and for improving the environmental and/or social impact of corporate processes, or (iii) relates to weapons produced and/or sold exclusively for sporting purposes, or (iv) relates to weapons sold within EU Member States;
- manufactures and/or sells goods which have no use other than for the purposes of capital punishment, torture or other cruel, inhuman or degrading treatment or punishment[21];
- is subject to the prohibition under Italian Law 220/2021[22];
- produces and/or sells cyber weapons: digital tools or malicious software (e.g. malware, ransomware)[23] specifically designed to be used or intended to cause damage, destruction or compromise to IT systems, critical infrastructure, networks or data, unless such assets (i) have as their sole final recipients governments, the armed forces and/or police forces, or (ii) are intended to improve the resilience of corporate and/or public utility systems.

Without prejudice to the exclusion criteria set out above, CDP assesses Counterparties operating in the Defence and Security Sector on the basis of their approach to managing material sustainability issues for the sector, their governance, including the procedures adopted for operating in countries that violate human rights and/or have a high level of corruption in line with this Policy, their management of the risk of corruption in business activities, and their involvement in ESG disputes.

If the assessments and checks conducted reveal shortcomings, CDP engages with the Counterparty in order to identify possible corrective measures or actions to mitigate the issues of concern and integrates the outcome of the discussions into its own assessment process. If the overall analyses identify significant unresolved issues of concern, CDP may decide to proceed with the transaction with an increasing level of restrictions.

In the case of Financing/Investment transactions having a specific purpose, these assessments of the Counterparty, together with the assessments of the recipient countries, contribute to the overall evaluation of the transaction.

[17] With reference to export transactions, assessments will be carried out with regard to the exporters and, where applicable and permitted, the other companies involved in the transaction.
[18] To be understood as being indirectly involved are: a) subsidiary/associate companies pursuant to art. 2359 of the Italian Civil Code or companies or entities involved in the production, trade, stockpiling or any other activity or service associated with "controversial weapons" or the key components of a system utilised in those weapons, even where such companies do not operate in the weapons sector; b) direct parent companies of companies or entities involved in the production, trade, stockpiling or any other activity or service associated with the abovementioned "controversial weapons" or the key components of a system utilised in those weapons, even where such companies do not operate in the weapons sector.
Such assessments are carried out on the basis of the best information available.
[19] Nuclear weapons (except in cases permitted by the existing international Treaties ratified in Italy and in compliance with responsibilities stemming from NATO membership), chemical weapons, biological weapons, depleted uranium weapons, anti-personnel mines, anti-tank mines, cluster munitions and submunitions/bombs.
[20] A critical component that is necessary for the operation of the controversial weapon and specifically designed for that purpose.
[21] The goods set out in Regulation (EU) 2019/125..
[22] It is specified that the safeguards set out under Law No. 220/2021 and the related Implementing Instructions apply to all transactions, including indirect transactions and/or those involving third-party resources, falling within the scope of application of that law as detailed in the relevant internal regulations and, in any event, in compliance with the external regulations applicable to the specific operations.
For transactions falling within the scope of Law No. 220/2021, and for the purposes of the prohibitions set out therein, the term "Financing" shall be understood in its broadest sense and shall therefore include any form of financial support provided, including through subsidiaries based in Italy or abroad, including, by way of example and without limitation, the granting of credit in any form, the issuance of financial guarantees, the acquisition of equity investments, and the purchase or subscription of financial instruments.
[23] For a comprehensive definition, please refer to the glossary.

4.4 Criteria with regard to the countries of destination

With regard to transactions carried out in the Defence and Security Sector, CDP intends to avoid any form of complicity with human rights violations during armed conflicts and to limit the risk of exporting to countries where an armed conflict is taking place if the countries concerned fail to provide adequate guarantees regarding the actual use and final destination of weapons, or are exposed to a high risk of corruption.

For this purpose, for Financing/Investment transactions with a specific purpose, CDP[24] refrains, in any capacity, from participating in transactions involving countries that:

- are subject to a European Union, NATO or OSCE embargo on war supplies; and/or
- are in a state of armed conflict, identifying these countries also on the basis of the guidelines issued by Italian and international bodies.

For countries not falling under the above categories, CDP assesses:

- the level of corruption;
- respect for human rights;
- the existence of disputes concerning the sector;
- the ratification of the main international treaties on weapons.

The country assessments based on the above parameters are combined with the Counterparty assessments described in paragraph 4.3 above (including the analysis of the policies adopted to assess the risk of human rights violations in the countries they operate in and to prevent the risk of corruption) to determine the overall assessment outcome for the transaction in question. In the case of transactions in a flagged country where the counterparty's policies are considered to be not entirely satisfactory, CDP applies an increasing level of restrictions to its participation in the transaction, depending on the severity of the issues of concern raised.

5. ROLES AND RESPONSIBILITIES

In the light of the context outlined, the roles and responsibilities of the various parties involved – in compliance with the regulatory and organisational system and with company powers and internal delegations – are defined below:

Board of Directors

- approves this document, as well as any non-formal revision and the possible repeal thereof, on an exclusive and non-delegable basis;
- resolves, with exclusive powers, on all export transactions relating to the Defence and Security Sector, upon proposal of the Chief Executive Officer and subject to the non-binding mandatory opinion of the Risk and Sustainability Committee.
- assesses whether it is also appropriate to intervene in Financing/Investment operations in the areas excluded from this document, approving any exceptions or interventions by way of derogation, as indicated in chapter 3, "Scope of Application".

Risk and Sustainability Committee

- issues an opinion to the Board of Directors on this document and on any revisions;
- issues a non-binding mandatory opinion on transactions relating to the Defence and Security Sector, within the scope of its remit;
- issues specific opinions on any derogations.

[24] In line with the provisions of the Group Policy on International Financial Sanctions, CDP complies with the objective restrictive measures identified therein, as summarised in the individual Country Sheets attached to the Group Policy on International Financial Sanctions.

Chief Executive Officer

- proposes to the Board of Directors the approval of this Policy, as well as any changes;
- continuously supervises, receiving information flows for this purpose, the application of this Policy, thus ensuring an organisational structure appropriate for the objective.

Administration, Finance, Control and Sustainability Department

- ensures that proposals for updating this document are developed in accordance with the Strategic Guidelines defined from time to time, also taking into account the relevant issues identified, in coordination with the other competent structures and in line with the Group Operational Instruction on "Regulatory and Operational Requirements for the Defence and Security Sector", while providing continuous advisory support on its interpretation;
- ensures, in conjunction with the structures involved, the proper implementation of this Policy, assessing the consistency of the various CDP areas of intervention with the principles defined therein, contributing, jointly with the structures concerned, to the necessary additions to the contractual framework;
- conducts the analyses necessary to comply with the criteria set out in this Policy, with a view to forming a final summary opinion on the eligibility of the transaction;
- oversees the dialogue with the ESG rating agencies in order to acquire information and content aimed at contributing to the improvement of this document.

Public Administration Department

- contributes, in coordination with the Administration, Finance, Control and Sustainability Department, to the updating of this Policy with regard to cybersecurity;
- ensures, in cooperation with the relevant structures, the correct implementation of this Policy with regard to cybersecurity matters.

Sector Strategy and Impact Department

- ensures the definition and the proposals for updating the Strategic Guidelines that address the intervention priorities aimed at bridging the market/socio-economic gaps;
- ensures, as part of the ex-ante sustainability and impact assessment, the identification of the relevant sustainability issues connected with the sectors covered by this Policy, within the sustainability impact assessment of the transaction in support of the competent functions.
- ensures the ex-post evaluation of the aggregate impact actually generated by the initiatives put in place by CDP is carried out.

Business Department

- ensures, with the support of the Administration, Finance, Control and Sustainability Department and/or the Public Administration Department, that the principles set out in this document are applied in Financing transactions, also by directing origination activities towards transactions consistent with this Policy and CDP's General Responsible Lending Policy;
- submits to the Board of Directors for approval all export transactions relating to the Defence and Security Sector and those transactions for which the derogation cases apply, in accordance with this Policy.

Investment Management, People, Transformation, and External Relations Department

- ensures, with the necessary support of the Administration, Finance, Control and Sustainability Department and/or the Public Administration, that the principles set out in this document are complied with in Investment transactions, including by guiding origination activities towards transactions consistent with this Policy and CDP's General Responsible Investment Policy;
- submits to the Board of Directors for approval all investment transactions relating to the Defence and Security Sector and those transactions for which the derogation cases apply, in accordance with this Policy;

- contributes to identifying relevant issues useful for defining the strategic priorities, through constant dialogue with the relevant stakeholders;
- oversees, in unison with the other competent Business Units, the dialogue with civil society in order to acquire, monitor and guide policy on issues relevant to the definition of the contents of this document;
- ensures appropriate awareness-raising and training initiatives with regard to this document.

Risk Department

- ensures second-level monitoring of risks (of competence), in compliance with the principles of the General Risk Policy, the Group Assessment of Reputational Risk Policy, the Anti-Money Laundering Policy and the Anti-Money Laundering Anomaly Indicators Regulation;
- ensures that ESG risks are properly assessed.

Internal Audit Department

- ensures third-level monitoring, based on the Regulations approved by the Board of Directors and according to a risk-based approach, assessing the completeness, adequacy, functionality (in terms of effectiveness and efficiency) and reliability of the internal control system as applicable to business processes;
- promptly reports critical issues identified during audits to the relevant company structures and periodically monitors the correct implementation of the resulting mitigation actions.

6. TRANSPARENCY AND ACCOUNTABILITY

CDP, recognising the value of transparency and continuous dialogue with its customers, investors, rating agencies and civil society organisations, in order to understand their legitimate expectations, undertakes to ensure continuous and transparent reporting.

For this purpose, CDP publishes its sustainability report annually on its website, in accordance with the European Sustainability Reporting Standards, as required by the Corporate Sustainability Reporting Directive.

This document is available on CDP's website.

7. ANNEXES

7.1 Glossary

- **UN 2030 Agenda[25]:** plan of action for people, the planet and prosperity signed in September 2015 by the governments of the 193 UN Member Countries. It incorporates 17 Sustainable Development Goals (SDGs) in a major agenda for action with a total of 169 targets.
- **Cyber weapons:** means of cyber warfare[26] designed, used, or intended to be used to cause injury or death to persons, or damage or destruction to objects; in other words, they produce effects that qualify a cyber operation as an attack[27].

[25] https://unric.org/it/agenda-2030/

[26] The set of military operations conducted in and through cyberspace to inflict damage on an adversary, whether state or non-state, consisting, inter alia, in preventing the effective use of systems, weapons and IT tools, or, more generally, of the infrastructure and processes under its control. It also includes defensive and "enabling" activities (aimed at ensuring access to and use of cyberspace) – source: National Cybersecurity Agency.

[27] Source: Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Rule 103, par.2, p. 452. The Tallinn Manual was drafted on the initiative of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), a NATO centre of excellence headquartered in Tallinn, Estonia.
For more information, see the CCDCOE official page dedicated to the Tallinn Manual: https://ccdcoe.org/research/tallinn-manual/

- **Conventional firearms:** the weapons set out in art. 2 of Italian Law 110/75, including rifles and carbines which, though being suitable for use as war weapon, have specific characteristics for use in hunting and sporting activities, having limited firing capacity and designed for use with non-military ammunition. Conventional firearms include: rifles and semi-automatic rifles with one or more smoothbore barrels; rifles with two rifled barrels, with successive loading by manual action; combination rifles with two or three barrels (both smoothbore and rifle), with successive loading by manual action; rifles, carbines and muskets with one rifled barrel, even if designed for semi-automatic operation; rifles and carbines that use rimfire ammunition, only of the non-automatic type; revolvers; semi-automatic pistols. This category also includes ammunitions and explosives for small arms and lights weapons.
- **Controversial weapons:** weapons which have indiscriminate effects and cause undue damage and injury. This category may be extended over time to reflect future technological developments. At the date of publication of this Policy and for the purposes therein, the following are classified as controversial weapons:
  - **Nuclear weapons** - any device which is capable of releasing nuclear energy in an uncontrolled manner and which has a group of characteristics that are appropriate for use for warlike purposes (definition taken from the 1967 Treaty for the Prohibition of Nuclear Weapons in Latin America and the Caribbean).
  - **Chemical weapons** - meaning:
    a. weapons used in combat, which use the toxic properties of certain chemicals to cause death or harm or to incapacitate the enemy;
    b. munitions and devices or systems specifically designed to cause death or other harm through the toxic properties of chemicals;
    c. any equipment specifically designed for use directly in connection with the employment of the munitions and devices specified.

    These weapons are regulated by the Chemical Weapons Convention (CWC, 1993), which prohibits any activity that aims to develop, produce, otherwise acquire, stockpile or retain or transfer chemical weapons.
  - **Biological weapons** - meaning:
    a. microbial or other biological agents, or the resulting toxins, used to cause harm or produced in quantities that have no justification for prophylactic, protective or other peaceful purposes;
    b. weapons, equipment or means of delivery designed to use such agents and toxins for hostile purposes. The biological agents used to develop biological weapons can be broken down into the following categories: viral (e.g. yellow fever), bacteriological (e.g. plague) and biological with indirect effects.

    Biological weapons are regulated by the 1972 Biological and Toxin Weapon Convention (BTWC);
  - **depleted uranium weapons** - depleted uranium is obtained as a by-product of the production of enriched uranium. It is used to make anti-tank munitions due to its armour-piercing qualities. It is not regulated by any international treaty but CDP has opted to include it as a material to be excluded from transactions, to the same extent as controversial weapons;
  - **anti-personnel mines** - a mine designed to be exploded by the presence, proximity or contact of a person and that will incapacitate, injure or kill one or more persons (Article 2, paragraphs 1 and 2, of the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, signed in Ottawa on 3 December 1997, ratified by Italian Law No. 106 of 26 March 1999. The same definition is utilised in Italian Law 220/2021 containing "Measures to counter the financing of manufacturers of anti-personnel mines, cluster munitions and submunitions"). Mines designed to be detonated by the presence, proximity or contact of a vehicle as opposed to a person, that are equipped with anti-handling devices, are not considered anti-personnel mines as a result of being so equipped;
  - **anti-tank mines** - mines designed to destroy or damage tanks and other vehicles;
  - **cluster munitions and submunitions / bombs** - a conventional munition that is designed to disperse or release explosive submunitions each weighing less than 20 kilograms, with the specific exclusions indicated under a), b) and c), point 2, of Article 2 of the Oslo Convention prohibiting cluster munitions, signed in Dublin of 30 May 2008, as referenced in Italian Law No. 95 of 14 June 2011. This definition is also utilised in Italian Law 220/2021 containing "Measures to counter the financing of manufacturers of anti-personnel mines, cluster munitions and submunitions").
- **Small arms:** weapons intended for use by an individual, such as self-loading revolvers and pistols, rifles and carbines, assault rifles and light machine guns. This definition is also intended to include ammunition and explosives for small-calibre weapons.
- **Light weapons:** generally defined as weapons designed for use by two or three persons, serving as a crew, although some may be carried and used by one person, including for example: heavy machine guns, portable anti-tank missile launchers, rocket launchers and portable anti-aircraft missile launchers. This definition is also intended to include ammunition and explosives for light weapons.

- **Cybersecurity:** measures to preserve the confidentiality, integrity and availability of information in the Cyberspace, the latter to be understood to mean the complex environment resulting from the interaction of users, software and services on the Internet, through technological devices and Internet-connected networks[28].
- **Counterparty:** the Beneficiary Company receiving the Financing or the Investment. In the case of (i) export transactions, the Counterparty shall be understood to be the promoting company/exporter of the transaction; (ii) project finance transactions, the Counterparties shall be understood to include both the borrower/SPV and its equity investments, individually or jointly, a shareholding of at least 51% of the share capital.
- **Environmental, Social and Governance (ESG):** the environmental, social and governance factors which qualify a financial activity as sustainable.
- **Financing/Lending:** without prejudice to other applicable internal and/or Group regulations, for the purposes of this document the term refers to the use of funds for general or specific purposes, carried out through any technical form permitted by law and by CDP's Articles of Association, using both own resources and third-party funds, at domestic and international level, including bond issues, revolving credit facilities, the acquisition of corporate receivables and the provision of guarantees[29].
- **CDP Group:** Cassa Depositi e Prestiti S.p.A. and Companies subject to management and coordination by CDP S.p.A. pursuant to Articles 2497 and following of the Italian Civil Code.
- **Investment:** without prejudice to the other related internal and/or Group regulations, for the purposes of this document this term refers to investment activity carried out both through direct investments (investments in shares, units and/or securities representing the risk capital of companies, participating financial instruments in companies, and other instruments, including hybrid instruments, similar in economic substance to the above, both domestically and internationally, as well as real estate investments) and through indirect investments (investments in units of debt and equity investment funds or fund-of-funds managed by Asset Management Companies (SGR), and holdings in other UCITS (Collective Investment Undertakings) or other investment vehicles, both domestically and internationally), using both own funds and third-party funds[30].
- **Malware:** an abbreviated form of malicious software. A program inserted into an IT system, generally in an unauthorised and concealed manner, with the intention of compromising the confidentiality, integrity or availability of the target's data, applications or operating systems[31].
- **Defence materials:** materials which, due to their technical-constructive or design requirements or characteristics, are such as to be considered built primarily for military use or for use by the armed forces or police, as defined by Art. 2 of Italian Law 185/90, as amended, and classified in the following categories:
  - Nuclear, biological, chemical and electric weapons
  - Automatic firearms and the related ammunition
  - Mid and large calibre weapons and armaments and the related ammunition
  - Bombs, torpedoes, mines, rockets and missiles
  - Tanks and vehicles specifically designed for military use
  - Vessels and the related equipment, specifically designed for military use
  - Aircraft and helicopters and the related equipment, specifically designed for military use
  - Powders, explosives, propellants
  - Electronic, electro-optical and photographic systems or equipment, specifically designed for military use
  - Special armoured materials specifically designed for military use
  - Specific material for military training
  - Machinery, apparatus and equipment designed for the purpose of manufacturing, testing and controlling weapons and munitions
  - Special equipment specifically designed for military use.
- **Goods which have no practical use other than for the purposes of capital punishment, torture and other cruel, inhuman or degrading treatment or punishment:** the goods identified in Regulation (EU) 2019/125, specifically, equipment whose main purpose is for use in capital punishment, torture or other cruel, inhuman or degrading treatment or punishment, such as goods designed for the execution of human beings or to restrain human beings.

[28] Source: ISO 27001
[29] For information on the Financing Transactions to which this Policy applies, please refer to paragraph 3.1, "Scope by Type of Transaction".
[30] For information on the Investment Transactions to which this Policy applies, please refer to paragraph 3.1, "Scope by Type of Transaction".
[31] Source: Glossary of the National Cybersecurity Agency.

- **Sustainable Development Goals (SDGs):** 17 goals agreed by the United Nations that aim to achieve a total of 169 targets relating to economic and social development, including poverty, hunger, health, education, climate change, gender equality, water, sanitation, energy, urbanisation, the environment and social equality.
- **Dual-use items:** items, including software and technology, which can be used for both civil and military purposes, and include items that can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices (Article 2 of Regulation (EU) 2021/821, as set out in Annex I to Regulation (EU) 2021/821.
- **Strategic Plan:** the CDP Group Strategic Plan 2025–2027, approved by CDP's Board of Directors at its meeting of 19 December 2024, including any subsequent updates.
- **Ransomware:** a type of malware that encrypts the victim's computer files and demands a ransom payment in exchange for decryption. In most cases, ransomware takes the form of trojans distributed through malicious or compromised websites, or via email[32]. These appear as seemingly harmless attachments (such as PDF files, for example) originating from legitimate senders (institutional or private entities). This factor prompts unsuspecting users to open the attachment, which is usually labelled with subject lines relating to invoices, utility bills, payment notices or similar matters.
- **Defence and Security Sector:** sector related to the production and trade of weapons, defence materials, dual-use goods used in the sector, including Cybersecurity products or services.

The first issued Policy was approved by the Board of Directors on 14 December 2022, while this update was approved by the Board of Directors on 20 November 2025

[32] Source: Glossary National Cybersecurity Agency