CEB

COUNCIL OF EUROPE DEVELOPMENT BANK
BANQUE DE DEVELOPPEMENT DU CONSEIL DE L'EUROPE

Integrity and Compliance Report 2021



Integrity and Compliance Report 2021

by the Office of the Chief Compliance Officer (OCCO)

Contents

Message from the Governor 3

1. Compliance function 4

2. Compliance activities in 2021 6

2.1 EU Pillar Assessment 6

2.2 Compliance policy making and maintenance 6

2.3 Project integrity 7

2.4 Compliance of procurement 9

2.5 Ethics and integrity 10

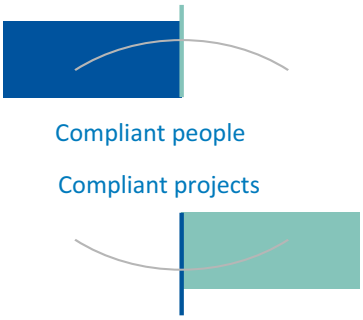
2.6 Training and awareness raising 11

3. Personal data protection 13

4. Information security 14

5. International relations 16

Abbreviations 17



Message from the Governor



I am pleased to present the 2021 Annual Report of the Office of the Chief Compliance Officer (OCCO), on OCCO's core activities in integrity, ethics and information security standard-setting and checking. This report provides an overview of how, in 2021, OCCO played a vital support function for the Bank in the realisation of its mandate, not only in continuing to strengthen the integrity due diligence process in order to enhance alignment with the highest integrity standards, but also in its response to the challenge of increased lending volumes (notably COVID-19 loans) as well as one-off Bank-level projects.

By promoting the highest ethical standards, good governance and cybersecurity, OCCO continues to make a crucial contribution to the CEB's risk management, with its mandate encompassing management of the financial and non-financial risks of money laundering, financing of terrorism (AML-CFT), tax evasion and avoidance, misconduct, mis-procurement, data breaches and cyberattacks. OCCO is also the principal investigative office and has responsibility for CEB compliance training.

While OCCO's achievements throughout the year were many and varied, some are especially noteworthy. One particular success in which OCCO played a leading role as co-ordinator in several areas of the work was the conclusion of the EU Pillar Assessment exercise in 2022.

On the compliance policy creation and maintenance front, OCCO revamped and modernised all three of the CEB's codes of conduct and obtained the approval of the Administrative Council and the Governing Board for the Bank's Anti-Corruption Charter. The new codes align with ESG best practices and promote the CEB's values, while the revamped Anti-Corruption Charter reaffirms the CEB's zero tolerance to fraud and corruption. A compulsory e-learning module on the updated code of conduct was launched in 2021, thereby contributing to higher institutional awareness of and commitment to the principles set out in the codes.

In terms of IT security, cybersecurity and personal data protection, OCCO continued to deliver high-quality solutions and successfully tackled all cybersecurity risks and crises. In its capacity as information security safeguard, OCCO developed and delivered the Information Security Strategic Plan and the Personal Data Protection Action Plan.

With respect to the Bank's participation in international fora, OCCO maintains a proactive presence in MONEYVAL, GRECO and OECD Global Forum meetings, MDB Investigations Meeting (CII), MDB Personal Data Protection Meeting, and in the meetings of European Chief Compliance Officers (ECCO) and of the Ethics Network of Multilateral Organisations (ENMO), with a particular focus on environmental, social and governance (ESG) factors in its core functions.

OCCO's wide-ranging and cross-cutting role is essential for us all to have confidence that the CEB is doing the right thing for its counterparties, shareholders and other stakeholders. It ensures that, as a vital instrument of European solidarity, the CEB is protected from harm and can continue to deliver on its important social mandate.

Carlo Monticelli
CEB Governor

1. Compliance function

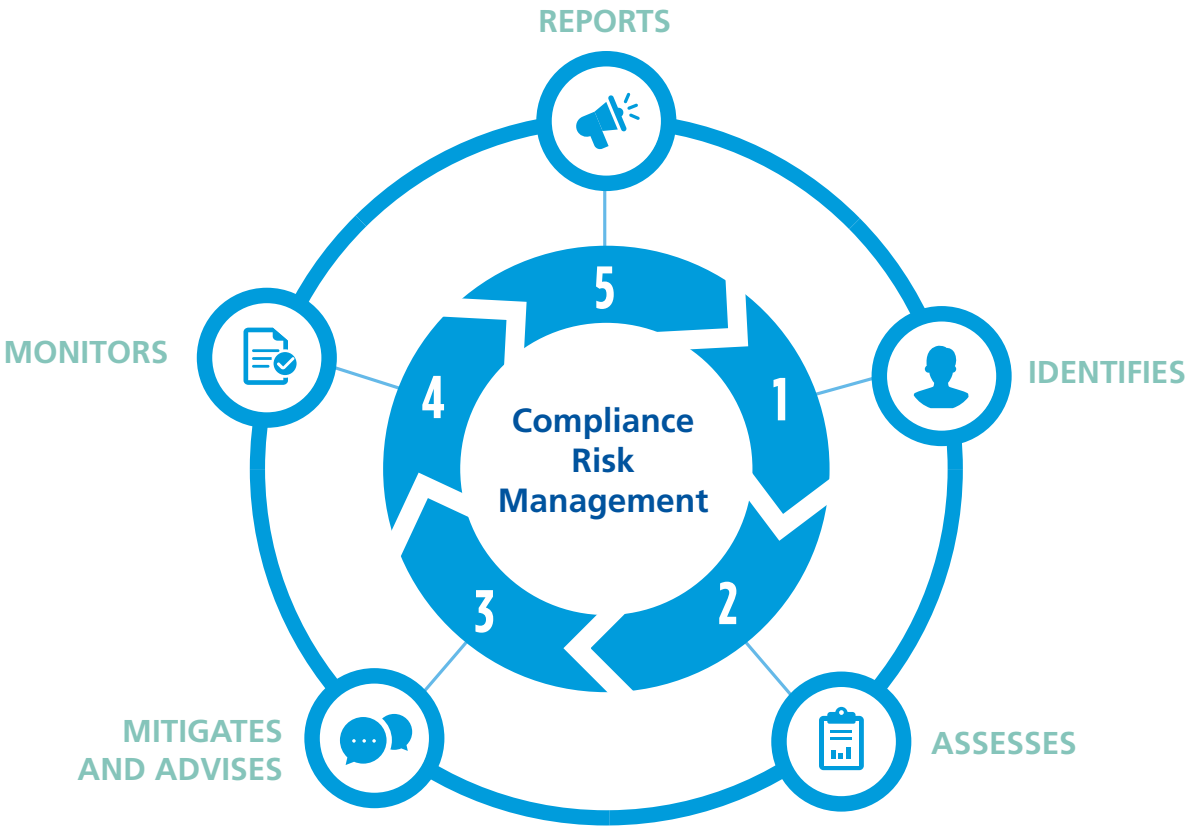
The Office of Chief Compliance Officer plays an important internal compliance risk management role, providing advice and assistance to the CEB's top management, directorates and divisions; it continuously evaluates compliance risks for projects, grants, treasury operations and the Bank's transactions, and safeguards the CEB's financial and non-financial risk of non-compliance.

In keeping with OCCO's independence from all operational divisions, OCCO is headed by the Chief Compliance Officer (CCO) who reports directly to the Governor and has direct access to the Auditing Board, the Collegial Organs, i.e. Administrative Council and Governing Board, as well as to the CEB's External Auditors.

The CCO also plays a specific role in the case of allegations of misconduct against the Governor, a member of the Collegial Organs, including their Chairpersons, or a member of the Auditing Board. In such cases the CCO will report to a compliance committee set up within the Governing Board, who will decide on possible further proceedings in the compliance investigation.

OCCO maintains a long-standing commitment to the highest standards of integrity and governance within the CEB, as well as with counterparties and projects under the CEB's compliance policies [Compliance policies | CEB (coebank.org)](#).

OCCO takes a holistic approach based on "**prevention and advice**" and "**control and investigation**".



The OCCO's mission is defined as:

"to ensure that the Bank conducts its activities in compliance with its own rules, current legislation, the Code of Conduct as well as with good practices and standards, in order to avoid any risk of irregularity in the functioning of the Institution, of its Organs or of its Staff".

With the purpose:

"to enable the CEB to limit its exposure to the risk of legal, administrative or regulatory sanctions, financial loss or loss of reputation incurred in the event of non-compliance. This is of the greatest importance for a development bank, and particularly one with a social vocation placed 'under the supreme authority of the Council of Europe'".

In particular, OCCO is tasked with the responsibility to identify, assess, mitigate and report compliance risks with a number of policies, procedures and good practices regarding:

- anti-money laundering / combatting the financing of terrorism
- non-compliant / uncooperative jurisdictions and tax good governance
- fraud and corruption
- reputational risk of sanctioned or debarred counterparties
- violations or breaches of the codes of conduct
- market abuse (insider trading, market manipulation, etc)
- conflict of interest
- environmental, social and governance (ESG) criteria
- whistleblowing
- dignity at work and respectful workplace.

With its unique mandate, the CEB is committed to fostering both social and environmental sustainability in its project financing (e.g. Environmental and Social Safeguards Policy) and in its internal operations (e.g. CEB Environmental Statement). This is reflected, for instance, both through the CEB dedication to annual sustainability reporting since 2009 and its commitment to exclude the financing of certain activities and sectors. The exclusion list is available in the Handbook for the Preparation and Implementation of Projects (Chapter 3) and the Loan and Project Financing Policy (Chapter 2.3).

The new codes of conduct also now include a reference to ESG (Environmental, Social and Governance) good practices, whose application should be proactively pursued. Furthermore, the Bank's materiality assessment conducted in 2019 has highlighted the importance of governance and ethics concerns for its stakeholders (e.g. non-discrimination, anti-corruption, reporting and transparency, gender equality), hence the key role played by OCCO in ensuring that the CEB continues to comply with these requirements.

OCCO is also tasked with information security, incorporating the Chief Information Security Officer (CISO) function, as well as with the protection of personal data at the CEB (the CCO acting as chair).

To find out more about OCCO's different functions: Integrity and compliance | CEB (coebank.org).

2. Compliance activities in 2021

2.1 EU Pillar Assessment

The aim of the EU Pillar Assessment is to certify capacity for the management of funds from the EU budget in line with the EU Financial Regulation which was updated in 2018.

In January 2022, the European Commission informed the CEB that it had successfully completed the Pillar Assessment with unconditional acceptance and no supervisory measures envisaged.

Since the start of the Pillar Assessment exercise in 2018, OCCO has co-ordinated 3 out of 5 pillars that were subject to assessment: Pillar 7 – Exclusions from access to funding, Pillar 8 – Publication of information on the recipients and Pillar 9 – Personal data protection. In addition to these, in 2021, OCCO provided substantial input regarding Pillar 6 – Financial instruments – specifically sections of Pillar 6b regarding tax avoidance, and the CEB's internal setup to demonstrate that it is compliant with EU requirements. As a result of the exercise, the CEB has updated its Policy on Non-Compliant and Uncooperative Jurisdictions, and has introduced the Guidelines for additional Tax Due Diligence for projects financed by the CEB.

Furthermore, regarding Pillar 7 – Exclusion from access to funding – the CEB's Procurement Division has developed two procedures to ensure integrity due diligence for corporate procurement and for procurement by borrowers, thereby strengthening overall prevention with ex-ante checks.

2.2 Compliance policy making and maintenance

Reform of the CEB's codes of conduct

OCCO has updated and published new codes of conduct since the adoption of the previous codes in 2009. The reform was approved by the Administrative Council and the Governing Board on 11 June 2021, and the new Codes of conduct apply respectively to:

- the Governor, Vice-Governors, staff members and contractual collaborators
- the Chairpersons and members of the Collegial Organs (Governing Board and Administrative Council)
- the members of the Auditing Board.

For the adoption of the new codes of conduct, OCCO conducted benchmarking and comparative analysis exercises with peer group financial institutions, and included proposed changes to the existing provisions. The reform presented aims to reflect the latest international best practices; the codes are now updated to include the following: references to the CEB values i.e. professionalism, co-operation, commitment, transparency, creativity; environmental, social and governance (ESG) aspects; articles on the appropriate use of social media and respectful workplace; an upgraded article on confidentiality, upgrade as new European standards were launched since 2018 (GDPR and Convention 108+); a revised article on pre-employment, post-employment and cooling-off period; an upgraded article on external activities and incompatibilities and a definition of close relatives; an upgraded article on gifts, sundry advantages favours and benefits now including active corruption and facilitating payment - a point raised by ESG rating agencies - ; and finally, various modifications to wording and terminology.

CEB Anti-Corruption Charter

The CEB's Anti-Corruption Charter was revised and presented to the Administrative Council in March 2021. The proposed changes refer to:

- the official introduction of the CEB's commitment to "zero tolerance to corruption"
- a revamp of the definitions regarding "obstructive practices" – aligning the CEB with its peer group
- the CEB's latest Loan and Project Financing Policy
- the CEB's commitment to the continuous enhancement of the compliance, monitoring and assessment function since 2008
- the inclusion of the "*Bank's commitment to corporate social responsibility and, more broadly, sustainability of its operations and project financing*"
- terminology alignments and adherence to the best international practices and standards as well as the work of the relevant international reference bodies.

NCJ policy amendment

On 24 September 2021, the Administrative Council approved an amendment of the CEB non-compliant/uncooperative jurisdictions (NCJ) Policy which has been the outcome of the EU Pillar Assessment exercise.

More specifically, the amendment of the existing CEB NCJ Policy refers to the prohibition of projects with links to jurisdictions that are non-cooperative for tax purposes, and classified as such by the European Commission. This update ensured that the CEB's internal rules and processes regarding financial instruments are assessed as adequate and at the same level as required by the EU Pillar Assessment.

In order to strengthen the internal framework to detect and prevent potential tax avoidance related to the CEB projects, the OCCO has produced internal Guidelines for additional tax due diligence for projects financed by the CEB. These guidelines confirm the CEB's commitment to prohibit tax evasion and tax avoidance, and that it will not support activities that support tax avoidance strategies.

2.3 Project integrity

AML/CFT and tax compliance risk assessments

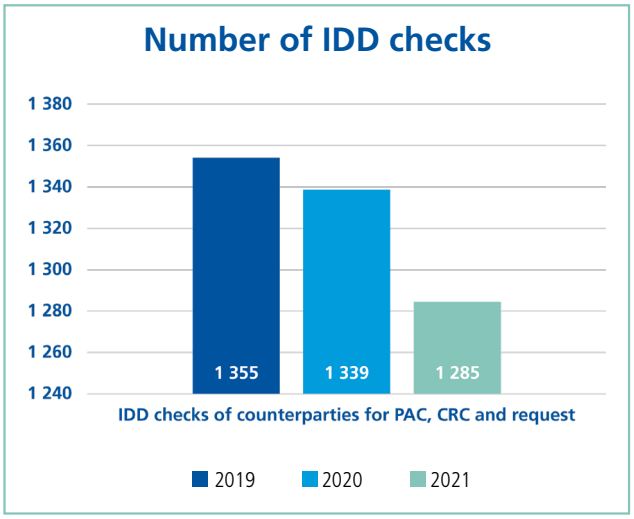
Policies

The CEB is fully committed via its Anti-corruption Charter, Compliance Framework Policy (defining the Anti-money Laundering (AML) and Counterterrorist Financing (CFT) priorities objectives) and Non-compliant/uncooperative jurisdictions (NCJ) policy to the highest standards of integrity for its projects and activities. In particular, the NCJ policy includes a commitment to prohibit the financing of projects used for certain "*Targeted Activities*" defined by the CEB as including "*(i) criminal activities such as money laundering (ML), financing of terrorism (TF), tax crimes (i.e. tax fraud and tax evasion) and (ii) tax avoidance practices*".

Procedures

OCCO has a comprehensive integrity due diligence and tax guidelines and procedures in place, and conducts AML/ CTF, tax compliance risk assessments on a second line of defence basis. These individual risk assessments are backed by the policies developed by OCCO as part of its compliance policy framework. OCCO performs a yearly internal AML/CFT and tax compliance risk assessment exercise at portfolio level, and ongoing individual compliance risk assessments for current and new counterparties in order to identify, assess and understand related risks and vulnerabilities and to design mitigation measures, if needed. The methodology is based on a risk-weighted based approach and self-assessment.

Through the preventive work described above, OCCO aims to ensure that CEB projects meet the Bank's compliance and high integrity standards. This ex-ante work performed in OCCO entails a variety of tasks, ranging from mapping out the risks, to mitigating risks and to establishing appropriate procedures and controls. The integrity due diligence procedures and controls are reviewed regularly in order to maintain any residual risks at a level that is acceptable to the CEB, and to meet market expectations created by a continuously changing regulatory landscape.



An additional critical element of OCCO's work is ensuring that counterparties are subject to scrutiny in terms of business integrity and reputation, and are aligned with the principles and norms established in the CEB's Compliance Framework Policy.

The CCO actively participates as a permanent member of the Project Appraisal Committee (PAC), Credit Risk Committee (CRC) and Development Project Committee (DPC), essential parts of the CEB's project cycle. This process guarantees permanent monitoring of CEB project activities and ensure effective scrutiny over aspects that may pose a risk to the CEB's reputation.

CEB Whistleblowing Policy

The CEB's Whistleblowing Policy is available on the CEB website and falls under OCCO's responsibility. It aims to:

i) protect the organisation from any kind of financial or reputational loss or misconduct

ii) complete the framework which requires the reporting of actions and behaviours that can be detrimental to the CEB's assets, integrity, reputation and staff

iii) support the values of transparency and co-operation.

OCCO also monitors the relevant public e-mail address (OCCO-whistleblowing@coebank.org) to which speak-up related elements or suspicion of non-compliance incidents can be submitted by internal or external whistleblowers.

In 2021, no incidents were reported either by internal or external whistleblowers.

Complaints

Complaints are brought to the attention of OCCO. In 2021, OCCO launched a project to design a Complaints Policy and related Complaints Procedures that, together, will set the framework for the CEB's accountability mechanism.

In 2021, a total of six complaints were registered with OCCO: a) four complaints related to potential fraud, corruption, collusion, coercion, bribery and/or procurement complaints and b) two complaints related to ESG matters brought forward by stakeholders of CEB-financed projects. Out of the four complaints related to potential fraud, corruption, collusion, coercion, bribery and/or procurement, three are closed and one is ongoing as of December 2021. Regarding the two complaints on ESG matters, one was closed, with detailed response to the complainant. Handling of the second complaint is ongoing.

Complaints or suspicion of fraud or corruption, can be submitted to OCCO directly within the compliance section of the CEB website or through its public e-mail address: compliance@coebank.org.

2.4 Compliance of procurement

The CEB's internal procurement procedures, which are aligned with CEB Guidelines for Procurement, were revised in December 2017 in order to enhance controls and create more timely access to relevant information in the procurement process.

As part of the ongoing effort to comply with internal procurement guidelines, rules and internal procurement procedures, to tackle procurement risks and to safeguard integrity and fair behaviour towards suppliers and third parties, OCCO participates in the whole CEB procurement business cycle:

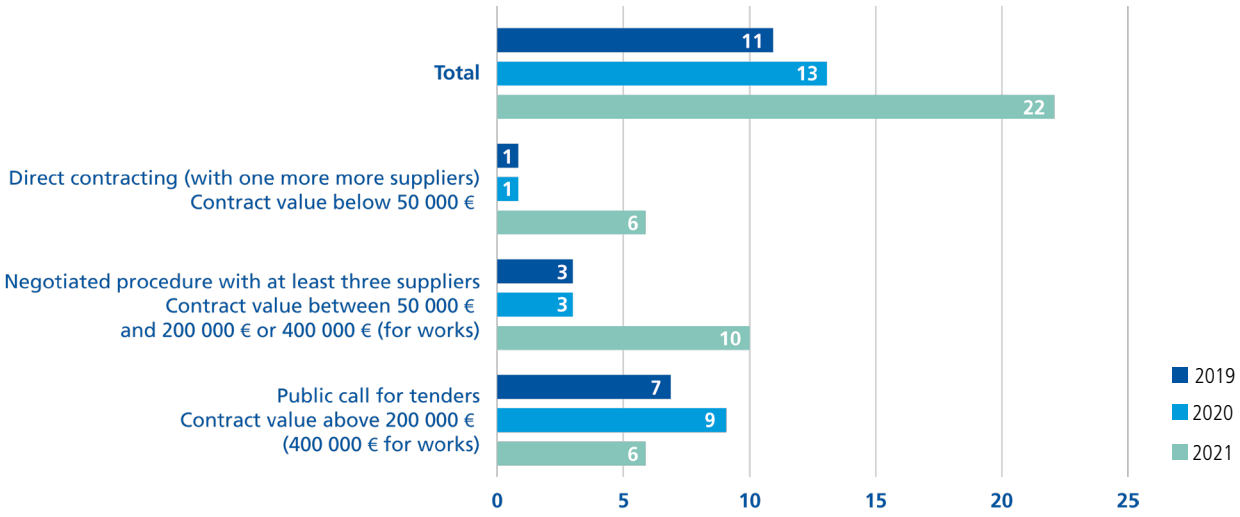
a) as an ex-ante validation point

b) as an observer in openings of tenders at Evaluation Committee meetings for internal procurement purposes whenever necessary

c) as an extension/exception control and validation point

d) as a complaint handling response point.

Validation of the choice of selection procedure



For all procurement contracts above the threshold of€ 50 000, OCCO verifies that the choice of the selection procedure proposed by the administrative unit concerned complies with the relevant procedures. OCCO also checks that there are valid grounds for any specific case that might be requested (notably concerning the thresholds for opening to competitive bidding). In some cases, the requests require prior consultation (pre-screening) with the initiating directorate or need to be reformulated by taking OCCO's comments into account.

2.5 Ethics and integrity

In June 2021, the CEB approved a new set of codes of conduct for staff, elected officials, Collegial Organs and Auditing Board. The new codes of conduct include a reference to ESG good practices, social media use and CEB values.

Oversight on these ethics issues is undertaken by OCCO. This is pursued in several ways, including through the regulation of conflicts of interests, gifts and sundries advantages, favours and benefits, the revision of the CEB's codes of conduct to prohibit passive/active corruption and facilitation payments, the deployment of a mandatory code of conduct training course for all CEB staff and the carrying out of investigations where allegations are made regarding code of conduct breaches.

The purpose of the codes of conduct is to set out the ethical rules that govern the conduct of those working for the CEB and help them to abide by these rules, as well as to inform their colleagues, the CEB's organs and the general public of the standard of conduct they are entitled to expect.

OCCO is audited every year by CEB external auditors and CEB independent Auditing Board and every two years by CEB Internal Audit.

To find out more about the new CEB codes of conduct, please follow the link:
Codes of conduct | CEB (coebank.org).



Investigations

OCCO is responsible for investigating allegations of fraud and corruption in the CEB's projects as well as for investigating allegations of non-observance of the CEB policies, guidelines, rules, procedures and standards of ethical behaviour and integrity on the part of CEB staff members. The investigation procedures are currently being drafted within OCCO.

Consequently, OCCO conducts two (2) types of investigation: a) investigations in relation to CEB-financed activities, and b) investigations of allegations of CEB staff members' misconduct under the relevant CEB Code of Conduct, the Rule for the Protection of Dignity at Work and the CEB Staff Regulations.

OCCO follows the international financial institutions community joint commitment to investigation principles and best practices.

No investigations were carried out in 2021.

2.6 Training and awareness raising

OCCO focuses on promoting the CEB's strong commitment to compliance culture by providing adequate awareness raising, training and communication. The high awareness and accountability of staff and management is maintained via consistent tone from the top, mandatory induction training for newcomers, thematic workshops for all staff and regular communication.

The changing digital working environment has accelerated the introduction of an e-learning solution for the topics of compliance, information security and data protection. Consequently, OCCO has contracted with e-learning providers to deliver on topics within its remit.

Tone from the top

The CCO holds regular monthly meetings with the Governor to keep him abreast of the latest compliance trends or upgrades in the regulations in force. Moreover, the CCO regularly informs the General Management Committee, Credit Risk Committee and Development Project Committee on the latest compliance developments. Strong "tone from the top" messages were conveyed by the Governor on the introductory page of the OCCO intranet site, in a targeted message from the Governor in the code of conduct e-learning module, and in a direct address to the staff as an introduction to the live session on ethical leadership.

Compliance induction course

Since 2016, in line with OCCO's proactive modus operandi and in close cooperation with the Chief Information Security Officer (CISO), OCCO has been organising an annual compulsory induction course for newly recruited CEB staff in order to:

i) promote compliance learning

ii) raise compliance awareness among staff members

iii) anticipate appropriate reactions regarding potential compliance issues

iv) advise on Information security risks.

E-learning

OCCO conducts regular e-learning courses when new regulations, policies or practices are adopted in order to ensure and enhance the CEB's dedication to its principles and values of commitment, co-operation, creativity, transparency and professionalism.

Featured recurrent topics of the training are:

- External compliance risks, i.e. fight against corruption and money laundering, harmful tax practices
- Cooperation with peer group and linkages with other IFIs on compliance issues
- Integrity due diligence internal procedures
- Compliance mission, goals and basic concepts
- Internal compliance risks, i.e. key aspects of the integrity control systems of banks
- Ethics, deontology, integrity, confidentiality

Codes of conduct

Following the introduction of the new codes of conduct, in 2021 OCCO launched a code of conduct training course, which was mandatory for all CEB staff members. It included a revisit of the basic principles embedded in the CEB's code of conduct and corporate values through video presentations, interactive quizzes and links to relevant documentation. The topics covered a general presentation of our codes of conduct, which focus on: Conflict of interests, gifts and sundry advantages, bribery and corruption, the notion of respect for others, harassment, discrimination, and whistleblowing. Such e-learning reinforces commitment to the CEB values and plays a crucial role in preventing and combating non-compliance and misconduct.

Data protection and confidentiality

CCO held its first non-mandatory e-learning session on data protection and confidentiality with the help of the Chief Information Security Officer. It focused on the impact of General Data Protection Regulation (GDPR) on CEB digital activities and included a presentation of the CEB environment with the application of 'Convention 108' on the principles of data protection and data subject rights, and, of course, the protection of data in the context of work. This first online course contributed to familiarise CEB staff with the relevant CEB regulation, aligned with the EU directive.

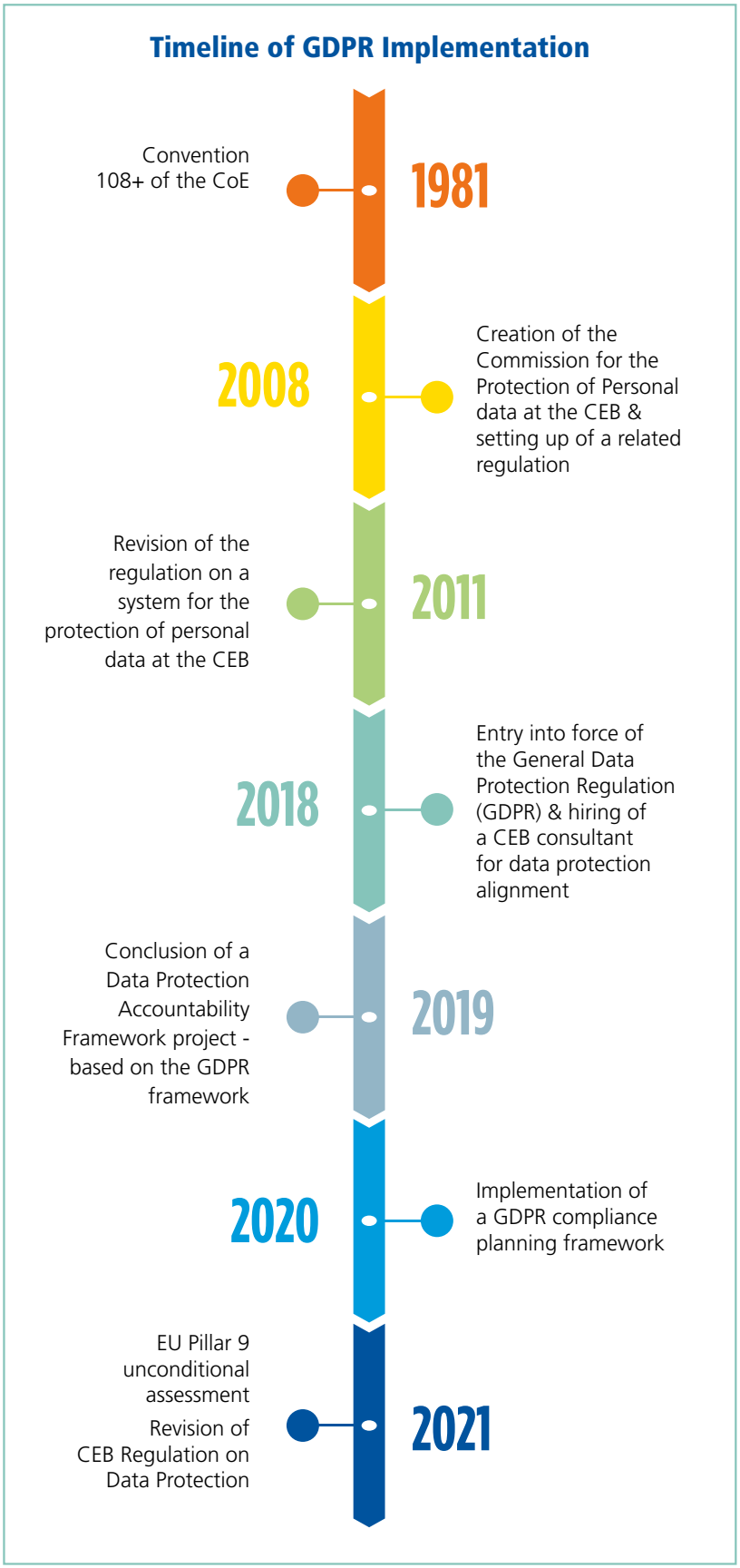
3. Personal data protection

Following the entry into force of the EU's General Data Protection Regulation and the amendment of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Modernised Convention 108+), OCCO launched a "Personal Data Accountability Framework" project, with the assistance of an external consultant, in order to identify all personal data processed by the CEB, assess the risks related to its disclosure, and propose an action plan to improve security.

The first phase of the project involved the presentation of a risk register to the General Management Committee and a proposal for an action plan to mitigate the risks identified, and was concluded in July 2019. The second phase of the project involves the implementation of the action plan.

Furthermore, OCCO continued its work with internal directorates and its consultant on data protection as regards the elaboration of their Data Protection Impact Assessment in various projects.

Contact: dataprotection@coebank.org



4. Information security

The Chief Information Security Officer (CISO) is a member of the OCCO team, responsible for managing information security at the CEB. Supervised by the CCO, the CISO also assumes the role of Data Protection Officer (DPO), in order to ensure the appropriate management of personal data handled within the Bank.

Chief Information Security Officer's activities in 2021

Regular security checks

Monthly checks were carried out on the Bank's various security tools (24 tools, such as for example the firewalls, the anti-malware platform or the privileged access management (PAM) platform) to review whether anomalies could be found. During all these checks, no particular anomalies were detected or raised.

Swift CSP and NIST CSF assessment

Swift has set up a customer security program (Swift CSP), comprising 31 controls covering the main aspects of cybersecurity, such as vulnerability management, access management or security awareness, etc. Several recommendations were implemented by IT to strengthen the security level of CEB's Swift platform. As a consequence, our Swift CSP attestation was submitted, with all mandatory controls compliant except one (however, alternative measures are in place that allow us to have this risk actually covered).

In order to assess the level of maturity of the Bank towards cybersecurity, an overall assessment was conducted during the last quarter of 2021 using the NIST Cyber Security Framework (NIST CSF) methodology. This methodology, used widely within the industry, allows us to evaluate the levels of controls we have in place on all domains of cybersecurity.

Data classification and archival policy

With data being more and more present in the world we are living in, it has become key to have some rules to govern the management of these data, and be able to identify which ones are the most important for the Bank. This is why the formalisation of a data classification and archival policy was initiated in 2020 and finalised in 2021, together with its associated procedure providing specific details for its proper application. Essentially, this policy introduces the concept of classification levels for each data and defines a set of protection rules to be applied, depending on their level of classification. This policy was approved in January 2022.

The evaluation is split into 5 main categories, with 108 points of controls assessed:

IDENTIFY

How the organisation is able to identify the risks and has a good knowledge of its environment?

PROTECT

What the organisation has in place to prevent attacks from happening?

DETECT

What the organisation has in place to detect when something wrong is happening?

RESPOND

How the organisation is organised to efficiently handle anomalies or alerts when they arise?

RECOVER

How the organisation is prepared to build something back in the event a major issue has hit us?

Security awareness

Reaching an appropriate level of security requires investment in and implementation of technical tools and controls, and the development of a culture of security among all staff. During the last quarter of 2021, two main actions were carried out for that purpose:

a) Delivery of an information security training for Swift users

Two dedicated sessions were organised by the CISO in order to raise the level of awareness around cyber security for all staff related to Swift (Back Office users, IT support users and Compliance). During these sessions, an overview of the evolution of the cyber security threat globally was shared with all, as well as specific tips and recommendations which can be incorporated into CEB staff daily working life.

b) Organisation of a first phishing campaign

With one of the main cyber security threats currently being phishing, it has become a standard practice within companies now to organise regular test phishing campaigns for the staff. One such campaign was organised within the Bank, with a fake email pretendedly coming from Google and distributed to all staff, asking them to open an attachment to check details about a suspicious connection to their account. Opening this attachment was obviously not harmful for the Bank, but served the purpose of bringing the users' attention to an awareness message explaining the dangers of such a practice.

Day-to-day security requests and advisory

The CISO is also involved daily in various operational actions related to information security, such as:

- Providing opinions and recommendations on IT projects
- Following various action plans with IT security teams
- Authorising the opening of Internet websites
- Providing advice and guidance to staff on security-related questions and requests
- Providing support for Swift-sensitive administration actions (4-eyes principle with IT teams).

5. International relations

The CEB is actively engaged in international co-operation on integrity, AML/CFT and anti-corruption/ anti-fraud issues in order to keep abreast of its peers, support the efforts of relevant international organisations and intergovernmental reference bodies, participate in the development and dissemination of best practice, and work efficiently with other IFIs in the common fight against corruption and fraud.

OCCO constantly contributes to the CEB's enhanced corporate visibility and rigorously promotes the image of the CEB as a multilateral development bank active in the fight against money laundering, terrorist financing, fraud and corruption, with high standards of integrity and business ethics.

Given the COVID-19 pandemic and although many already planned missions were cancelled or postponed, close bilateral and multilateral relationships with peer groups were successfully held virtually to ensure continuity in the fields of anti-money laundering, combating the financing of terrorism, harmful tax practices, anti-fraud, anti-corruption, anti-bribery, integrity, due diligence and data protection.

OCCO continued to engage

as an observer/member with
key intergovernmental initiatives

- Money Laundering Measures and the Financing of Terrorism (MONEYVAL)
- Group of States Against Corruption (GRECO)
- OECD on Transparency and Exchange of Information for Tax Purposes
- The 5th annual "MDB Privacy" symposium
- Opening Plenary of the 2021 OECD Global Anti-Corruption & Integrity Forum
- Anti-Corruption Network for Eastern Europe and Central Asia (ACN)

in
International Fora

- 21st Conference of International Investigators (CII)
- Annual Meeting of the Ethics Network of Multilateral Organisations (ENMO)
- European Chief Compliance Officers (ECCO) meeting
- Women's Forum Global Meeting 2021
- Global Summit of all Public Development Banks
- EIB Investing in Climate Action: *The Make-or-Break Decade*

Abbreviations

AML	Anti-Money Laundering
CCO	Chief Compliance Officer
CEB	Council of Europe Development Bank
CFT	Combating the Financing of Terrorism
CISO	Chief Information Security Officer
CRC	Credit Risk Committee
DPC	Development Project Committee
DPO	Data Protection Officer
ECCO	European Chief Compliance Officers
EIB	European Investment Bank
ESG	Environmental, Social and Governance criteria
GDPR	General Data Protection Regulation
GRECO	Group of States against Corruption
IDD	Integrity Due Diligence
IFI	International Financial Institution
MDB	Multilateral Development Bank
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
NCJ	Non-Compliant / Uncooperative Jurisdictions
NIST	National Institute of Standards and Technology
OCCO	Office of the Chief Compliance Officer
OECD	Organisation for Economic Cooperation and Development
PAC	Project Appraisal Committee

Photo credits: Cover: Rawpixel



CEB
COUNCIL OF EUROPE DEVELOPMENT BANK
BANQUE DE DEVELOPPEMENT DU CONSEIL DE L'EUROPE

55 avenue Kléber
FR-75116 PARIS
Tel: +33 (0) 1 47 55 55 00
Fax: +33 (0) 1 47 55 55 74
E-mail: compliance@coebank.org
Web: www.coebank.org

ISSN 2957-7209 (Online)