CIB Third Parties' Handbook

Table of Contents

Welcoming Word

CIB Welcoming Word

As we go on board with the CIB transformation phase, we're delighted to introduce the Third-Party's Handbook.

This initiative underscores CIB's commitment to excellence and highlights the importance of fostering strong, transparent, and collaborative relationships with our valued third parties' business relationships. In today's dynamic business environment, effective partnerships are more crucial than ever for achieving our common goals. This handbook serves as a comprehensive resource, outlining our mutual expectations, roles, and responsibilities. By establishing clear communication channels and incident resolution mechanisms, we aim to enhance our collaboration and ensure a seamless working relationship.

As we navigate this transformative journey, our reliance on third- party service providers will undoubtedly increase. Together, we have the opportunity to tackle challenges and seize new opportunities while aligning our interests and values. We encourage you to view this handbook as a vital tool in our shared journey toward success.

Thank you for your partnership and dedication to our collective growth.

Introduction

About CIB

As a valued and success partner contracted by CIB to provide services and products, CIB places great importance on maintaining secure and resilient business relationships; that is why this handbook is designed, mainly to serve as a comprehensive guide outlining our expectations, requirements, and best practices for managing third parties' risks effectively. By adhering to the principles and guidelines in this handbook, we can work together to strengthen our risk management processes, enhance operational security, and have a trusted beneficial partnership. CIB genuinely appreciates your commitment to maintaining these standards to protect the mutual interests, the customers, and all stakeholders.

CIB (Commercial International Bank) is the leading private- sector bank in Egypt, offering a broad range of financial products and services to its customers, which include more than 500 of Egypt's largest corporations, enterprises of all sizes, institutions, and households. CIB's strong brand and growth in retail and SME banking segments continue to introduce new customers to the bank. As a result, CIB has succeeded in becoming the most profitable commercial bank operating in Egypt for more than 40 years.

Our Vision

To be at the forefront of change, building for the future, and turning aspirations into reality.

Our Mission

To transform traditional financial services into simple and accessible solutions by investing in people, data, and digitalization to serve tomorrow's needs today.

Our Values

People are the cornerstone on which our bank is built - brick by brick, byte by byte, transaction by transaction, day in and day out. At tellers' counters and in our operation centers, in conversations with large corporate clients and fresh graduates entering the workforce, our people are helping customers chart their financial futures. As they do so, every one of them plays a role in creating value for all our stakeholders, from our clients to our shareholders and the communities in which we do business.

"Customers First, Lead the Market, Agility & Integrity"

Business Imperative

This handbook contains rules, requirements, policies, procedures, and other items governing the relationship between our valued third parties (TPs) and CIB. Its primary purpose is to ensure understanding, eliminating the need for personal decisions on matters of bank-wide policy, and to help promote consistency throughout our relationship journey.

Our third parties (TPs) need to have a thorough look at this handbook so we can together navigate the evolving landscape of risk and ensure a resilient and secure future for our business relationships.

Declaimer

CIB reserves the right to make any changes or to discontinue any policy at its sole discretion, without advance notice.

The policies, procedures and benefits summarized in this handbook are not a contract, express or implied, between CIB and its third parties. CIB is not obligated to notify our third parties with any internal policies and procedures changes

Before the Ship Sails

Regulatory Requirements

Given the importance and criticality of engaging third parties, whether assigned by the bank to perform various functions and activities, provide goods and services to CIB, or act as intermediaries for certain products and services, it is essential to ensure clarity and mutual understanding.

The Central Bank of Egypt's circular dated September 19, 2024, and its updates outline minimum requirements that must be maintained in contracts with third parties. These obligations include ensuring the quality of services in accordance with predefined standards, safeguarding the confidentiality of all information related to the bank and its clients, and providing the bank with the ability to terminate contracts without financial penalty in cases of breach. Third parties are also required to seek prior approval before making changes to services and must comply with the bank's supervisory procedures, including providing regular performance reports.

It is essential that these third parties allow the bank access to relevant information and promptly notify the bank of any events that could impact their ability to meet obligations. Additionally, contracts must permit access to the Central Bank's regulatory sector for oversight purposes.

These instructions serve as examples and may be subject to updates, highlighting the importance of ongoing compliance with existing and future third parties' regulations.

Due Diligence Process
(Know Your Partner!)

Due diligence is one of the most important steps before starting a partnership with a third-party business.

What is Third Party Due Diligence?

Third Party's due diligence is the investigation that a person or business is expected to take on before entering into a contract or agreement with another party. When CIB seeks to outsource work or take on a new third party, CIB conducts TP due diligence in order to understand any problems or risks associated with this new relationship.

Conducting TP due diligence is important for CIB to make informed decisions about who we will work and contract with so as to avoid potential problems associated with compliance, regulations, and the bank's reputation.

Why is Third Party (TP) Due Diligence Important?

As we grow as a bank, our dependency on Third parties services & products increases along with the need to capture various regulatory environments, data privacy rules, sanctions, and common types of corruption, including money laundering and bribery. And with a greater number of regulatory and compliance resources available, CIB is held to higher standards by CBE, which means that we are increasingly obliged to prioritize due diligence. TP relationships also introduce a number of risks beyond legal and compliance to include exposure to cyber threats and negative publicity.

In other words, TP due diligence is important because not performing it exposes the bank to potentially devastating consequences that may not be recoverable from in a competitive and increasingly complex market.

Contractual Protections

Key Components of a Third Party's Agreement.

There are numerous clauses you may find in a third-party agreement that are essential when negotiating third-party contracts* that would vary according to the nature of the third party, the provided products & services.

Among the most common components typically included, but not limited to, are clear specifications regarding the third party's status as an independent contractor, ensuring they cannot act on behalf of the bank.

Additionally, the agreement provides a detailed description of the products or professional services to be delivered, incorporates a limitation of liability clause that excludes certain damages and sets monetary caps, and outlines the costs associated with the products or services, including payment details and penalty application criteria.

Furthermore, it is crucial for the contract to address the handling of confidential information, defining what constitutes "confidential" and specifying the duration of its protection.

The contractual agreement also defines the term of the relationship, delineates termination procedures, and clarifies ownership and usage rights in the case of intellectual property. Information about deliverables, their due dates, and compliance with applicable laws, regulations, and industry standards is clearly stated.

*In that sense, TPRM developed (TPs) Standardized Terms & Conditions, which would serve as the minimum base for terms and conditions that can be tweaked further according to the nature of the contractual agreement and the business needs.

Confidentiality and Data Security

In a confidentiality or non-disclosure agreement, CIB and the third party agree to keep private nonpublic information received during a business relationship, including in the early stages of exploring a potential business relationship.

What is a Confidentiality Agreement/ Non-Disclosure Agreement?

Confidentiality agreements/ Non-Disclosure Agreements protect both parties, CIB and the third party, entering into business relationships or transactions that require the exchange of sensitive, private information otherwise inaccessible to TPs. Confidential information is the heart of any confidentiality agreement. For the agreement to adequately protect against unwanted disclosure, both parties must clearly describe the information or types of information they wish to protect and the scope of each party's non-disclosure obligation.

CIB has a separate form for non-disclosure agreements (NDA) that has to be signed prior to signing any binding agreement with any third party

Conflict of Interest:

What is Conflict of Interest?

A conflict of interest is any situation where a person or organization has outside obligations that prevent them from carrying out their duties in the most honest and effective way they can.

Why is Conflict of Interest Important?

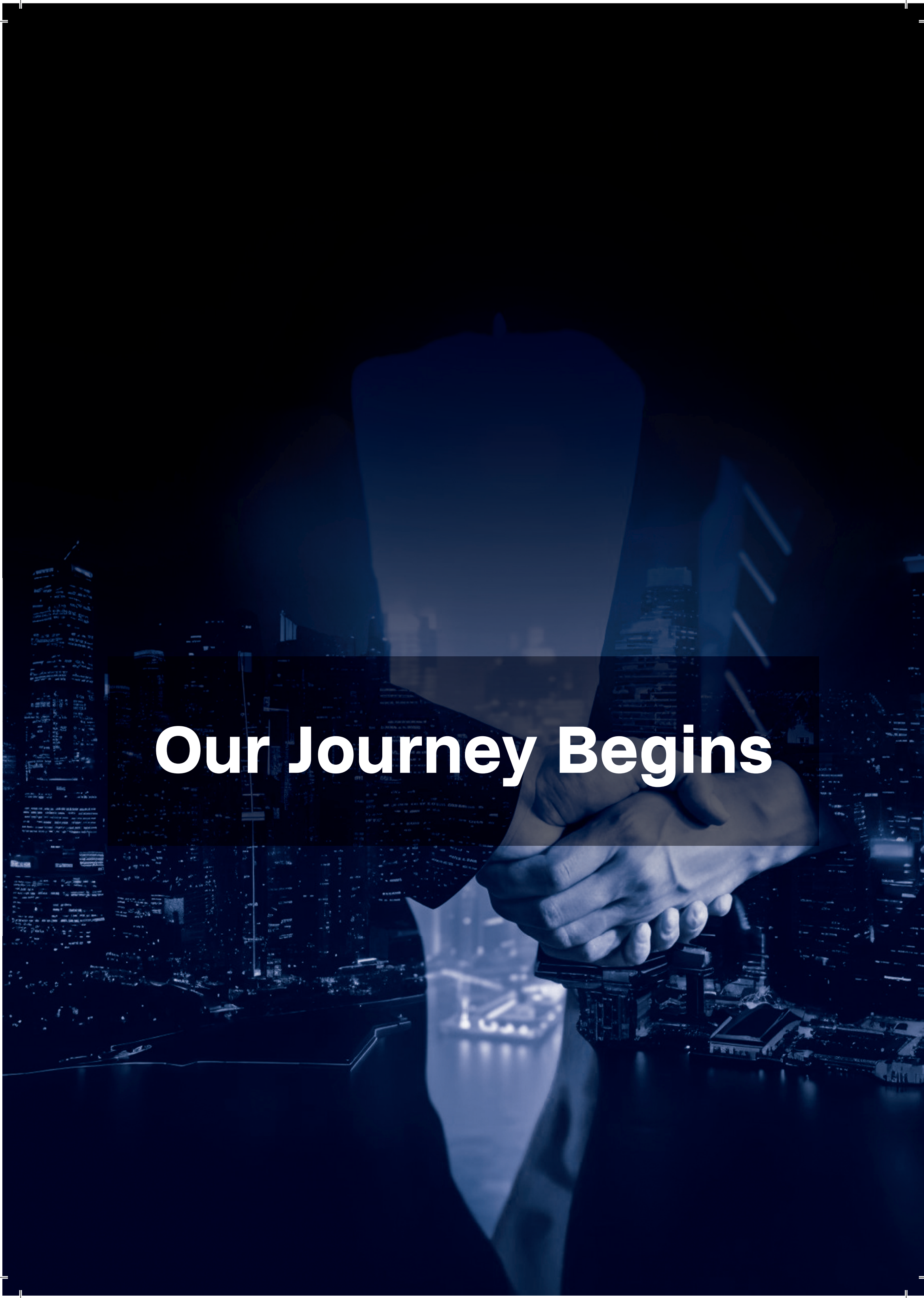
Everyone brings their own interests and obligations when they join our business. This isn't an inherently bad thing, but it's important for both individuals and TPs themselves to be honest when potential conflicts present themselves. Additionally, in light of the regulator's directives, it is crucial to fully understand and effectively implement the conflict-of-interest requirements. These mandates are essential to ensure our compliance and to uphold our commitment to ethical standards.

If our involvement with a third party compromises our integrity, this can cause a variety of problems:

· Damage to brand and reputation.
· Potential for legal action and/or regulatory violation.
· Loss of public trust.

CIB has a separate form for conflict of interest that has to be signed prior to signing any binding agreement with any third party, and at the time of renewing contractual agreements.

Our Journey Begins



Monitoring and Overseeing
(Reporting)

What is TP Risk Monitoring and How Does It Work?

TP monitoring is the practice of continually gathering and analyzing externally observable data.

CIB is always eager for continuous insights into the overall third party's performance, that serves as a defense of the bank's internal processes/ systems, reviewing records, and might include conducting site visits

Why is TP's Risk Monitoring Important?

Actively monitoring TPs for cybersecurity, financial, ethical, reputational, and legal risk is critical to ensuring the stability, and resilience of CIB. TP risk monitoring ensures sustainability, trust and transparency in a third-party relationship.

To accurately evaluate TP risks, CIB adopts advanced and scientific methodologies of which:

· TP Risk Assessment
· TP Key Risk Indicators
· TP Key Performance Indicators
· TP Incidents & Complaints Monitoring
· TP Stress Testing & Scenario Analysis
· TP Exit Assessment

Some Types of TPs Key Risks

ESG Risk Monitoring

CIB holds a great belief in its environmental, social & governance responsibility (ESG); recently, CIB was honored with the prestigious award for "Best Institution for ESG Integration in Egypt at the Annual Conference for the Arab Federation of Capital Markets (ACFM) hosted in Muscat, Oman. This recognition highlights CIB's commitment to effectively integrating Environmental, Social, and Governance (ESG) practices throughout its operations, policies, reports, capacity-building initiatives, and data digitization efforts. Notably, CIB was the sole institution from the Egyptian Stock Exchange (EGX) to receive this award.

The Bank is currently issuing an integrated report that includes a set of frameworks for sustainability, environmental and societal risk management, and climate change, in preparation for the implementation of the decisions of the International Sustainability Standards Board (ISSB) in the International Financial Disclosure Standards (IFRS). Having an ESG monitoring system is important for CIB because it helps maintain a good reputation. It also allows for identifying and mitigating risks related to environmental, social, and governance factors that could impact their operations and finances. By monitoring ESG factors, CIB can improve its financial performance, comply with regulations, and gain a competitive edge. It demonstrates commitment to sustainability and helps to attract socially conscious customers.

Continuous TP Monitoring

In the time between third risk assessments, a lot can happen. That is why it is important to provide ongoing visibility into TP threats. External risks to TPs are constantly tracked and analyzed by CIB's relevant departments based on each third party's essentiality and criticality level.

4th Parties and Beyond

At CIB, third parties (TPs) encompass suppliers, vendors, outsourced functions, and any entities that engage in business relationships with us. However, it is crucial to extend our focus to the next level: the partners and suppliers of our third parties, commonly referred to as fourth parties. These fourth parties, or "Nth parties" in the supply chain context, are not directly contracted with CIB but are connected through our third-party relationships.

In this regard, it is essential that our contracted third parties do not assign or subcontract any of their contractual obligations to other service providers without prior disclosure and approval from CIB. This ensures that we maintain oversight and control over the entire supply chain, safeguarding our operations and mitigating potential third parties' risks.

Incidents Response Plan

What is The Meaning of a Third party's Incident?

An incident is any event where there is a potential or actual impact resulting from any activity or service provided by a TP. Impacts could be Financial (loss or gain) or Non-Financial, of Regulatory sanctions or negative staff experience. This definition also includes any penalties or compensation paid to or from a TP.

How to Effectively Respond and Handle a TP's Risk Incident?

Establish Clear Roles and Responsibilities

CIB has a third-party Risk Incidents team dedicated to investigating TPs' incidents, relying on our TPs' collaboration in order to ensure the sound implementation of action plans and provide recommendations in order to prevent or mitigate any financial or non-financial risks that may impact CIB or our TPs

Review and Improve the Incident Response

After resolving the incident, the CIB Third Party Risk Management Team (TPRM) provides a thorough review and evaluation of the incident.
CIB also identifies and documents the lessons learned, best practices, gaps, and weaknesses of the incident, and provides feedback and recommendations for improvement.
That might include updating and revising the concerned third party's contract, SLA, or signed Annex, our internal policies, procedures, and tools based on the review findings, and implementing any necessary changes or enhancements.

Report and Comply with the Incident Requirements

Depending on the nature and impact of the incident, CIB might need to report and comply with various legal, regulatory, contractual, or ethical requirements related to the incident

Monitor and Follow-Up on the Incident

Finally, CIB Third Party Risk Management Team (TPRM) monitors and follows up on the incident with all concerned teams to ensure that there are no residual or recurring issues, risks, or threats related to the incident. CIB should also maintain regular communication and collaboration with the third party to address any outstanding or emerging concerns, questions, or disputes arising from the incident in order to avoid reoccurrence of the incident. One of the aspects CIB considers when reviewing and evaluating the relationship with the third party is the third party's performance and accountability during and after the incident.

Cyber Security

What is the Meaning of Cyber Security?

CIB has implemented a set of processes and strategies to safeguard its critical systems and sensitive information. These measures aim to manage the risks associated with various relationships. It is crucial to uphold these standards, as any compromise could potentially lead to cyber-attacks and data breaches. CIB relies on its TP partners to prioritize the protection of the bank's interests, ensuring that both financial and non-financial impacts stemming from security vulnerabilities are minimized. This is important to maintain the security of the bank's and its customers' data, as well as to prevent potential cyber-attacks and avoid negative repercussions on the bank's reputation.

Why is Cyber Security Important for CIB?

As CIB and banks across Egypt increasingly embrace technology, the storage of sensitive information, such as customer data, has shifted to cloud-based solutions. This trend has been accelerated by the COVID-19 pandemic, which necessitated the widespread adoption of remote work practices. With this heightened reliance on digital systems, including cloud services, smartphones, the Internet of Things, and artificial intelligence, new security vulnerabilities have emerged that were not present in previous years.

In response to these challenges, banks worldwide have intensified regulations surrounding cybersecurity. CIB - as other banks- is now required to take significant measures, including promptly communicating data breaches, appointing dedicated data protection arms, obtaining user consent for data processing, along with other security measures that should be in place to safeguard the bank as well as our customers and partners

What is the Cybercrime Impact on CIB?

In response to these challenges, banks worldwide have intensified Cyber-attacks can impact every business, regardless of size, in many ways, including:

· Financial losses
· Drop in productivity
· Damage to reputations
· Legal Liability
· Business continuity problems

How Can We Enhance CIB's Security Against Cybercrime in Third-Party Relationships?

To effectively safeguard CIB from cybercrime, particularly in relation to third-party interactions, several key security measures should be implemented. First, comprehensive cybersecurity training for both employees & outsourced staff should emphasize the unique risks associated with third-party partnerships, ensuring that staff are aware of potential vulnerabilities and know how to mitigate them.

Second, robust security access management protocols must be established for third-parties, allowing CIB to control and restrict access to sensitive information based on the principle of least privilege. This helps prevent unauthorized access and protects critical data.

Lastly, continuous monitoring and management of security risks associated with third-party relationships are essential. Regular assessments and audits should be conducted to identify potential threats and ensure that all third parties adhere to CIB's security standards, thereby strengthening the overall security posture.

Conduct Risk & Customer Rights Protection

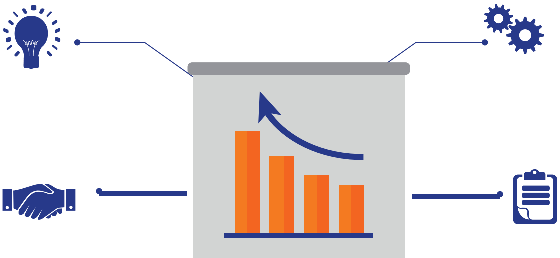
At CIB, ensuring the fair treatment of customers and safeguarding their rights are fundamental principles of responsible banking. As a third- party service provider, your commitment to upholding Conduct Risk and Customer Rights Protection standards is vital for building trust and ensuring compliance with our values and regulatory requirements.

Every interaction you have with our customers must be transparent, fair, and devoid of misleading information, as these practices are essential to protect their rights and enhance their overall banking experience.

You are expected to maintain clear disclosures, engage in honest communication, and adhere to ethical practices in all dealings. These obligations not only fulfill regulatory expectations but also serve as the bedrock for fostering strong, long-term relationships with our customers

Together, we can cultivate a banking environment that prioritizes integrity, accountability, and customer confidence.

Training and Awareness



CIB is deeply committed to providing comprehensive training and learning opportunities, extending not only to our employees, but also to all outsourced staff, demonstrating our dedication to their professional development. Our bank prioritizes investing in training in order to ensure the growth and success of both our internal team members and our valued outsourced partners. Training comes from our strong belief that helps employees keep pace with banking industry trends, technological advancements, and high standards of quality services.

Especially in the banking industry, we are counting on our successful business partners to maintain - as we always do- compliance with legal and regulatory requirements and accordingly mitigate risks associated with non-compliance.

Speak up!

How to Speak Up:

At CIB, we are committed to conducting our business with honesty and integrity. We expect everyone working on behalf of the bank to uphold these high standards. The CIB Whistleblowing Policy explains what constitutes a Speak Up concern and facilitates third parties in safely and confidentially raising concerns about suspected or actual wrongdoing in a work-related context, without fear of penalization.

CIB's Whistleblowing form and contact email are available via the bank's website and contain all the relevant contact details and information on resources/support to help you raise a Speak Up/Whistleblowing concern, which is handled confidentially. We want to hear from you.

Contact us through:

For reporting any form of suspected or actual wrongdoing in a work- related context, such as but not limited to theft, embezzlement, fraud, breach of the anti-money laundering laws,...etc.

Sending an email to: cib.whistleblowing@cibeg.com

Submitting a report through our online whistleblowing form, Link: https://www.cibeg.com/en/whistleblowing

Calling the CIB whistleblowing hotline from 9:00 am to 4:00 pm at (+2) 0237472220

Disclose to CIB Anti Bribery and Corruption Team via email (CIB.anti-Bribery@cibeg.com) any requests or pressure to provide bribes/benefits in any form, to any party, directly or indirectly related to CIB Egypt, that may try to influence or provide an unfair business advantage.

Other than this, please contact us with any feedback or questions you may have through our official website https://www.cibeg.com, or send a message through our social media platforms mentioning your Company Name and indicating that you are a Third Party in order to easily direct your concerns to the correct channel.

- https://www.facebook.com/CIBEgypt/
- https://www.instagram.com/cibegy: pt/
- https://www.linkedin.com/company/cibegypt
- https://www.youtube.com/user/CIBEgypt

Thank you for being an integral part of CIB's journey toward excellence in Third Party Risk Management.

Together, we are building resilient partnerships founded on trust, transparency, and shared goals. We hope this handbook serves as a valuable guide to strengthen our collaboration and navigate challenges successfully.

As we continue working hand in hand, know that your commitment and contributions are deeply appreciated.

With warm regards, CIB Team.

THE BANK TO TRUST