



Investigation and response procedure

June 2018 (v1)

Contents

0.	VERSION CONTROL	4
1.	Objective	5
2.	INVESTIGATION PROCEDURE	5
2.1.	Preventative investigation	5
2.2.	Confirmatory investigation	6
2.2.1.	Origin of the indications of a breach	7
2.2.1.1.	Indications identified during the supervision of the Model	7
2.2.1.2.	Receipt and analysis of the notifications via the Whistle-blowing Channel.	7
2.2.1.3.	Indications identified by other means	9
2.2.2.	Examination phase of the investigation	10
2.2.2.1.	Investigation documentation	11
2.2.3.	Defensive investigation	12
2.2.3.1.	Investigation documentation	12
3.	Reporting and response	12
3.1.	Submission of investigation file	12
3.2.	Adoption of appropriate measures	13
3.3.	Filing and safekeeping of information on the investigations	14
4.	GRAPHIC DEPICTION OF THE RESPONSE MODEL UPON IDENTIFICATION OF SIGNS OF BREACH	15

0. VERSION CONTROL

Version	Date	Amendments
1	27 June 2018	Initial Version.

1. OBJECTIVE

The aim of this document is to set out the guidelines, procedure, tools and mechanisms for managing the various types of investigation conducted by the organisation within the Crime Prevention Model and the Code of Ethics and Conduct (hereinafter the Model) Oversight Function, in light of the relevant goals and having regard to the process for reporting to the Compliance Committee and the Board Secretary, as applicable.

2. INVESTIGATION PROCEDURE

As a crime prevention body, oversight is one of the Compliance Committee's key functions, as regulated in article 31 bis 2, sections 2 and 4 of the Criminal Code. Such oversight takes the form of a range of activities, one noteworthy example being the conduct of investigations, which, depending on the relevant aims, may be classed as preventative, confirmatory or defensive in nature.

Types of investigations:

- **Preventative:**
Where any indications of an infringement come to light over the course of the work to oversee the design and effectiveness of the Crime Prevention Model.
- **Confirmatory:**
Investigations activities that seek to confirm the existence of an offence where indications that such an offence has been perpetrated has been identified via:
 - The ordinary or preventative supervision of the Crime Prevention Model
 - Notifications/complaints received via the Whistle-blowing Channel.
 - Any other notification or reporting channel.
- **Defensive:** Investigation activities seeking to mitigate the criminal liability of the legal entity or release it from such liability when faced with charges levelled against FCC as a legal entity.

2.1. Preventative investigation

Periodic investigations of the design and effectiveness of the model form part of the ongoing oversight, within the context of freedom of enterprise and defined in the work plan of the Corporate Compliance Officer, approved by the Compliance Committee and in large part performed in collaboration with Internal Audit, as well as with the Business Unit Compliance Officers. With a view to ensuring that such activities are documented, this type of investigation includes the following phases:

- a) Definition of the scope of the specific investigation in the form of a periodic review plan.
- b) Gathering of information on the investigation, including, where required, the following activities:

- a. Interviews conducted with the persons in charge of the relevant processes with a view to gathering further information and gaining a better insight into the process, as well as obtaining the proof and/or evidence deemed appropriate.
 - b. Requesting information from the departments concerned (evidence), public registries and third parties.
 - c. Accessing working and communication tools (technological resources), including corporate e-mail and other communication channels, respecting personal privacy in line with article 18.3 of the Spanish Constitution, the legislation in force and the Policy on the Use of Technological Resources, with a view to checking the design and effectiveness of the model-related activities and the proper use of such resources in the performance of the activities specific to each position. Note that there is a technological resources user policy or guide governing access to the information housed on these resources, of which the employees have been informed and which makes no provision for privacy.
 - d. Other means, as and when required by the investigation.
- c) Preparation and submission of the report summarising the investigation to the Compliance Committee. On finalisation of the investigation, a report will be prepared, including the results, any subsequent actions and, where applicable, the measures to be adopted (as well as the persons tasked with implementing such measures), detailing the data and resources used in the investigation and on which the results are based.
 - d) Filing and safekeeping of the documentation on the investigations on the protected database created for such purpose.

If in the course of a preventive investigation they were detected any indications of a breach of the Code of Ethics and Conduct or a breach of any nature that might entail criminal implications for FCC come to light, the notification and confirmatory investigation process detailed below will be set in motion.

2.2. Confirmatory investigation

The confirmatory investigation process gets underway with a view to confirming a potential offence, with criminal consequences for the company or a breach of the Code of Ethics and Conduct with criminal consequences for the company, provided the following circumstances have arisen:

- Where indications of a breach come to light during the periodic supervision of the model (preventative investigations within the annual model review plan).
- Where any type of notification is received via the Ethics Channel.
- Where news of any event that may constitute a breach of the Code of Ethics and Conduct or a potential offence is received by any other means of communication or information.

In each of the scenarios detailed above, the investigation process is similar, getting underway on approval by the Compliance Committee, subject to a preliminary analysis by the Corporate Compliance Officer. Nonetheless, the manner in which such indications are presented by the Compliance Officer to the Committee and the speed of internal reporting must be in line with the potential repercussion of the facts.

2.2.1. Origin of the indications of a breach

2.2.1.1. Indications identified during the supervision of the Model

Should any indications of a perpetration of a criminal offence or a breach of the Code of Ethics and Conduct be detected in the ordinary course of supervision under the Model, through investigation of its design and effectiveness, the Corporate Compliance Officer, in his/her capacity of providing executive support to the supervision process, will classify the relevance of the facts identified in accordance with the terms defined in the following section (high risk, medium risk, other) and will inform the Compliance Committee at its next monthly meeting; the latter may then agree to commence an examination phase in accordance with the provisions of section 2.2.2 hereafter. Notwithstanding the foregoing, the mechanism for informing and reporting to the Committee may be brought into line with the seriousness of the facts identified and the potential repercussions or awareness of such facts beyond the scope of supervision of the Model, and the Committee may be called on an emergency basis.

2.2.1.2. Receipt and analysis of the notifications via the Whistle-blowing Channel.

- **Receipt** Anyone who becomes aware of any breach of the Code of Ethics and Conduct and/or the Crime Prevention Model may report such breach via the Whistle-blowing Channel created for such purpose, in line with the Whistle-blowing Procedure. Where the Corporate or Business Compliance Officer are notified or are aware of a potential breach of the Code of Ethics and Conduct and/or the Crime Prevention Model, it must be included in the Whistle-blowing circuit. It will fall to the Compliance Officer to classify and evaluate such notifications, in the first instance, before informing the Compliance Committee.
- **Analysis** The Compliance Officer will perform an analysis to determine the type of notification per the following classification:
 - **Consultation:** where the reporting party raises doubts, as opposed to a declaration, concerning a fact that may constitute a breach of the Code of Ethics and Conduct or the Crime Prevention Model, the Corporate Compliance Officer will respond to such party within not more than five business days or will forward the notification to the Business Unit Compliance Officers, when dealing with specific issues of their areas, within not more than five business days.
 - **Non-pertinent notification/complaint:** where the notifications/complaints in question do not refer to a breach of the Code of Ethics and Conduct

or the Crime Prevention Model or imply indications of any type of unlawful act with Corporate criminal liability, the Corporate Compliance Officer will notify the reporting party that no investigation proceedings are to be instituted, forwarding such notification to the relevant unit.

- ***Pertinent notification/complaint:*** where the notification/complaint is admitted for consideration as a potential breach of the Code of Ethics and Conduct or the Crime Prevention Model, the Corporate Compliance Officer will classify it in one of the three categories, defined hereafter.
-
- **Classification. Classification of the risk of the pertinent notifications or complaints.** (see the Ethics Channel Procedure for further details):
 - ***High risk:*** Complaints referring to acts perpetrated by members of the management or any other employee, and which may pose a criminal risk to the legal entity.
 - ***Medium risk:*** Reports without a relevant impact on the reputation of the FCC Group or the legal entity, essentially concerning the application of the Code of Ethics and Conduct.
 - ***Other notifications:*** Other notifications mean those that, given their subject matter, do not fall within the remit of the Compliance Committee, and, even where reported to the Committee by the Corporate Compliance Officer for informative purposes, it will fall to the latter to delegate the handling and resolution of such notifications to other specific areas of the organisation, when seen fit.
- **Reporting:** Once the documentation concerning the complaint has been reviewed, the Corporate Compliance Officer will prepare a report to be submitted for the evaluation of the Compliance Committee, which must contain the following information:
 - A notification classification file.
 - Information describing the incident reported.
 - Evaluation of the content and the relevant circumstances.
 - Identification of the potential offence and its impact on the legal entity.
 - Analysis of the information received and proposed evaluation of the need for an investigation.
 - Measures proposed for notifications managed previously and solution for any potential internal control weaknesses identified.

The Compliance Officer may conduct preliminary investigations of the incident reported in order to draft the report.

- **Proposed actions:** proposed resolution or proposed investigation.

For such purposes and depending on the urgency, the Compliance Committee will be informed at its next meeting, or an emergency meeting may be called, in line with the procedures detailed in the Compliance Committee Regulations.

2.2.1.3. Indications identified by other means

Should notification be received by any other means, for example:

- Court notification or demand (generally received by the Legal Counsel of the business).
- News in the media.
- Actions taken by the State security forces.

The following measures will be adopted:

In the first two cases, provided the criminal offences are deemed to pose a high risk or where the seriousness so requires, the events shall be notified by the Legal Counsel that receives the notification or by the communications manager or by the person responsible for identifying relevant news to the Office of the General Secretary and/or the General Management of the Legal Counsel, which shall be in charge of evaluating the seriousness of such risk.

A serious risk shall be considered to exist for the organisation in the following scenarios:

- Crimes relating to corruption, bribery and influence peddling.
- Crimes relating to natural resources and the environment having a significant impact on the FCC Group.
- Fraud in the preparation of financial statements, the impact of which is material.
- Crimes relating to money laundering.
- Financing political parties.

Should it be determined that the notification does not pose a serious risk to the organisation, the Corporate Compliance Officer will be notified so that the risk may be classified and, where applicable, a confirmatory investigation may be performed to verify the facts. The Corporate Compliance Officer may draw on the support of the Compliance Officers of the businesses, depending on which company the notification applies to. The Legal Counsel of the business will also be informed so that it may comply with the notification.

Should the notification be deemed to pose a serious risk to the organisation, on the date of receipt or the following day, the Office of the General Secretary and/or the General Management of the Legal Counsel will immediately inform the CEO, the head of communications and/or the corresponding Business Unit Legal Counsels so that they may coordinate communication and messages to be sent out, while simultaneously evaluating the criteria to respond to the notification and defence mechanisms, where applicable.

In addition, either the General Secretary or the General Manager of the Legal Counsel will inform the Corporate Compliance Officer of the facts so that the latter may call an emergency meeting of

the Compliance Committee within two business days in order to present the facts and request approval to commence the examination phase of a confirmatory investigation process and appoint the investigator.

In the third scenario, in the event of law enforcement, the person in charge of receiving the police officers (receptionist) must notify the Business Manager, the General Secretary and the General Management of the Corporate Legal Counsel of the arrival of the security forces. The Business Manager shall be responsible for notifying this fact to the Chairman of the business and to the Legal Counsel of the business, whereas the General Secretary and/or the General Management of the Legal Counsel must inform the CEO and the head of Communications, in order to implement an emergency communication management mechanism. When all of the parties have been informed, the Legal Counsel of the business and the General Secretary/General Manager of Legal Counsel will perform a preliminary evaluation of the seriousness of the event and notify the Corporate Compliance Officer so that an extraordinary Compliance Committee meeting may be called within the next two business days.

Following this preliminary evaluation, it shall be determined whether or not to provide legal assistance to the employee, in which case the legal strategy to be used shall be determined, evaluated and approved by the CEO, paying a bond where necessary. If assistance is not provided to the employee, the potential impact on the legal entity must be evaluated, as must the need to carry out a defensive investigation.

2.2.2. Examination phase of the investigation

Depending on the information received, the risk involved and the classification of the facts, the Compliance Committee shall determine the phases of the investigation necessary for its understanding and clarification.

In particular, the Compliance Committee will perform the following:

- Identify the agent or person(s) reported who show signs of non-compliance or unethical behaviour with a view to confirming whether or not they have performed any actions or activities that imply the perpetration of a criminal offence or a breach of the Code of Ethics and Conduct.
- Determine the person(s) responsible for performing the investigations, who may be internal agents (requesting the support of Internal Audit and/or the areas concerned) or external experts in the subject matter (to provide a higher level of independence in certain processes, if required), taking into account their knowledge and the circumstances of the specific case.
- Evaluate the functioning of the risk prevention mechanisms and determine, where applicable, whether or not they should be reviewed.

The non-violation of the fundamental rights of the persons being investigated must be guaranteed throughout the investigation process.

Once the investigations have been approved and the persons responsible or the investigators from the Compliance Committee have been determined, the Corporate Compliance Officer will be responsible for notifying the investigating team of the facts, the items subject to investigation and the mechanism thereof.

In the event of liaison with Internal Audit, an agreement will be reached between the Corporate Compliance Officer and the Director of Internal Audit (who shall be a Committee member for the purposes of this matter) on the design of the tests to be performed and the performance of the investigation.

Should the participation of an independent external expert be required, the Corporate Compliance Officer will invite one or various suppliers to submit bids, maintaining the confidentiality of the matter.

2.2.2.1. Investigation documentation

The investigation will comprise at least two phases:

- a) Appointment of the investigating team, which may differ depending on whether an individual or the organisation is being investigated.
- b) Opening of an internal file, for safekeeping by the Corporate Compliance Officer.
 - a. Investigation of an individual
 - Interviewing the notifying parties or the areas involved, in order to gain further information and an understanding of the situation. The notifying party may be offered the possibility of holding a face-to-face or telephone interview with the person appointed as investigator of the process in order to confirm, extend upon or qualify submissions. Should the notifying party so wish, it may also provide written submissions and/or any proof or evidence it deems pertinent.
 - Interviewing the reported parties or the persons involved in the events, in order to understand the other party's side of the story and contrast the incidents reported.
 - Requesting information from the departments, public registries and third parties.
 - Following approval of the Compliance Committee, potentially requesting professional expert reports from external personnel.
 - b. Investigation of the organisation
 - Evaluating the degree of effectiveness of the existing control model on the date of perpetration of the alleged breaches.
 - Any other means of investigation, within the applicable legal framework.

- c) Monitoring of the case by the Corporate Compliance Officer and the Compliance Committee.
- d) The investigations will generally last for two months at the most, extendable should circumstances so require. This term shall be reduced to one month for complaints of harassment.
- e) Preparation of an internal report and an action proposal by the Corporate Compliance Officer, to be presented to the Compliance Committee, which will propose the actions necessary to the corresponding bodies.

2.2.3. Defensive investigation

Defensive investigations are prepared when the company has been charged and criminal proceedings have been initiated. In this case the company must commence the **legal entity's defence** by searching for evidence in relation to the perpetration of the criminal offences, with a view to achieving exemption from criminal liability under the criteria set out in article 31 bis. In this way, the following can be evidenced: a) the company has adopted and effectively implemented an adequate management and organisational model to prevent criminal offences or to significantly reduce the risk of their perpetration; b) the individual involved perpetrated the criminal offences by fraudulently eluding the control mechanisms implemented by the organisation to prevent such acts; and c) the oversight function was duly implemented, and there were no shortcomings in its operation.

The General Management of the Legal Counsel will carry out the preliminary evaluation and also the judicial management of the charge and will notify the Corporate Compliance Officer, who will then call a Compliance Committee meeting as a matter of urgency in order to decide whether or not to commence and carry out the defensive investigation with regard to the person(s) responsible.

2.2.3.1. Investigation documentation

The defensive investigation process shall take place in liaison with the Legal Counsel and following the same procedure as that of the confirmatory investigations.

3. REPORTING AND RESPONSE

3.1. Submission of investigation file

Upon finalisation of any of the aforementioned investigations (depending on the type, in accordance with the aforementioned classification), the Compliance Corporate Officer will present the results to the Compliance Committee and submit a written report which must contain, at least, the following:

- a. The initial risk classification of the notifications/complaints made (if the indications were notified through the Whistle-blowing Channel), which will be included in the "initial evaluation file".
- b. A brief outline of the methods used for the investigation.

- c. Documented and proven results of the investigation, indicating whether or not the Code of Ethics and Conduct or the Crime Prevention Model have been breached.
- d. Conclusions of the investigation and proposed measures to be taken.

Once the investigation file has been submitted, the Compliance Committee, supported by the Corporate Compliance Officer, will do the following:

- a) Shelve the complaint if the event in question does not give rise to a breach of the principles and values included in the Code of Ethics and Conduct or in the Model and is not a criminal offence.
▶
- b) Shelve the complaint if there is insufficient evidence or information to determine who is responsible for the incident reported.
- c) In the event of a breach of the Code of Ethics and Conduct, corrective or disciplinary measures shall be established having regard to each specific case, based on the corresponding collective bargaining agreements or on the applicable employment legislation, and the possibility of filing a complaint shall be considered, provided it is duly substantiated and justified.
- d) Should a criminal offence be detected, the possibility of filing a complaint shall be considered, provided it is duly substantiated and justified.
- e) In the event of a criminal charge, the modus operandi shall be determined by the court ruling.

3.2. Adoption of appropriate measures

In the case of ordinary investigations, within two business days of the adoption a ruling by the Compliance Committee, the Compliance Officer shall notify this ruling by email with acknowledgement of receipt:

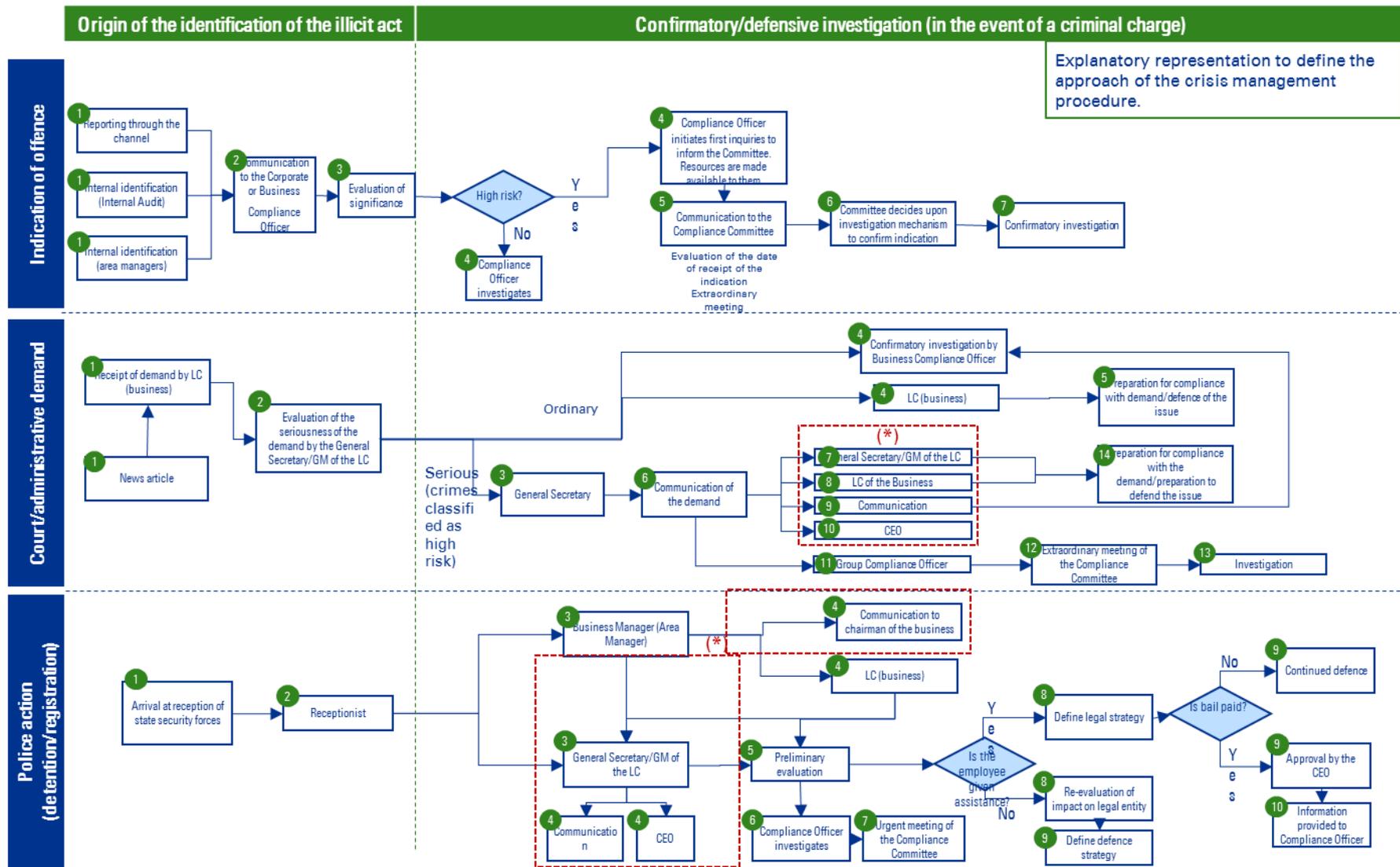
- to the party under investigation.
- to the notifying party, if applicable.

Should a disciplinary regime be applied, the hierarchical superior of the notified party, in liaison with Human Resources, shall adopt the pertinent disciplinary measures pursuant to the decision of the Compliance Committee as soon as possible.

3.3.Filing and safekeeping of information on the investigations

FCC has a filing mechanism in place for such information, namely a data base created to this end, access to which is restricted to the members of the Compliance Committee and the Corporate Compliance Officer and which is duly protected (Complaints Management System) in accordance with the indications of the Whistle-blowing procedure. The file generated in the investigation shall be in the safekeeping of the Corporate Compliance Officer.

4. GRAPHIC DEPICTION OF THE RESPONSE MODEL UPON IDENTIFICATION OF SIGNS OF BREACH



(*) Members comprising the crisis nucleus. Notifications shall be made as a matter of urgency.