

SUMITOMO CORPORATION ESPAÑA S.A.

# COMPLIANCE MANUAL

Crime Prevention and Detection System



<b>COMPLIANCE MANUAL</b> .....	6
OBJECT .....	6
SCOPE OF APPLICATION .....	6
COMPLIANCE CULTURE AT SCSP .....	6
TONE FROM TOP MANAGEMENT .....	7
<b>CRIME PREVENTION AND DETECTION POLICY</b> .....	8
OBJECTIVE OF THE CRIME PREVENTION AND DETECTION POLICY .....	8
SCOPE OF ACTION .....	8
PRINCIPLES OF ACTION .....	9
WHAT IS AN ILLEGAL ACTIVITY? .....	9
EVALUATION AND REVIEW. CONTROL .....	11
POLICY STATEMENT .....	12
<b>CODE OF ETHICS AND CONDUCT</b> .....	14
IINTRODUCTION .....	14
OVERVIEW .....	14
PURPOSE OF THE CODE .....	14
SCOPE OF APPLICATION .....	15
SCSP ETHICAL COMMITMENT .....	15
HEALTH AND SAFETY AT WORK .....	17
OBJECTIVES .....	17
OBLIGATIONS .....	18
AVOIDING CONFLICTS OF INTEREST .....	18
OBJETIVES .....	18
OBLIGATIONS .....	19
CONFIDENTIALITY OF COMPANY INFORMATION .....	19
OBJETIVES .....	19
OBLIGATIONS .....	20
PROTECTION OF PERSONAL DATA .....	21
OBJETIVES .....	21
OBLIGATIONS .....	21
USE AND PROTECTION OF COMPANY ASSETS .....	22
OBJECTIVES .....	22
OBLIGATIONS .....	22
PREVENTING CORRUPTION IN BUSINESS .....	23



OBJETIVES .....	23
OBLIGATIONS.....	23
GIFTS AND HOSPITALITY .....	24
OBJETIVES .....	24
OBLIGATIONS.....	25
STAKEHOLDER RELATIONS.....	25
SUPPLIER RELATIONS.....	25
CUSTOMER RELATIONS .....	26
RELATIONS WITH PUBLIC ADMINISTRATIONS .....	26
RESPECT FOR THE ENVIRONMENT .....	26
COMPLIANCE STRUCTURE AND CONTROL ENVIRONMENT .....	27
COMPLIANCE STRUCTURE .....	27
CONTROL ENVIRONMENT .....	28
MISCELLANEOUS PROVISIONS .....	29
COMMUNICATION, DISTRIBUTION AND EVALUATION .....	29
DISCIPLINARY REGIME .....	30
UPDATE .....	30
ACCEPTANCE .....	30
VALIDITY .....	31
<b>CRIME PREVENTION AND DETECTION PROTOCOL.....</b>	<b>33</b>
OBJECT .....	33
GENERAL DEFINITIONS .....	33
SCOPE.....	34
CRIME PREVENTION AND DETECTION SYSTEM .....	35
SCSP COMPLIANCE COMMITTEE .....	35
CRIME PREVENTION AND DETECTION PROTOCOL.....	36
COMMUNICATION CHANNEL .....	38
TRAINING .....	39
CRIME PREVENTION AND DETECTION SYSTEM .....	40
DETECTION AND RESPONSE PROTOCOL.....	43
<b>COMMUNICATION CHANNEL PROCEDURE.....</b>	<b>50</b>
INTRODUCTION .....	50
WHAT DOES THE COMMUNICATION CHANNEL CONSIST OF?.....	50
WHAT IS AN ILLEGAL ACTIVITY?.....	51
WHO SHOULD REPORT AND HOW THEY ARE PROTECTED? .....	56



WHO SHOULD I CONTACT? .....	57
HOW WILL THE ORGANISATION RESPOND? .....	57
FALSE OR UNFOUNDED ACCUSATIONS .....	59
COMMUNICATION CHANNEL COMPLAINT FORM .....	60
<b>RULES OF PROCEDURE OF THE SCSP COMPLIANCE COMMITTEE .....</b>	<b>61</b>
OBJECT .....	61
PROFILE OF THE COMPLIANCE COMMITTEE .....	62
PURPOSES AND COMPETENCES .....	63
COMMUNICATION CHANNEL.....	64
<b>TRAINING .....</b>	<b>65</b>
OBJECT .....	65
TRAINING SCOPE .....	66
TYPES OF TRAINING.....	66
TRAINING REVIEW .....	66



SUMITOMO CORPORATION ESPAÑA, S.A.

# CULTURE OF COMPLIANCE

Crime Prevention and Detection System

## COMPLIANCE MANUAL

---

### OBJECT

---

The main objective of this Compliance Manual is to establish the necessary procedures, as well as to improve the existing ones, for the proper implementation and management of the Crime Prevention and Detection System in **SUMITOMO CORPORATION SPAIN, S.A.**, hereinafter **SCSP**, which aims to effectively detect and prevent the possible commission of crimes within the Organisation.

The Compliance Manual contributes to establishing a "Culture of Regulatory Compliance" in the Organisation, which ultimately makes it possible to exonerate or at least mitigate its criminal liability in the event of the possible commission of a crime within the Organisation.

In addition to this Compliance Manual, Sumitomo Corporation Group's policies including Sumitomo Corporation Group Compliance Policy and Principles and Rules of SC Europe & CIS Group including SC Europe & CIS Compliance Manual are applicable to **SCSP** and its the Directors, Officers and employees, as a member of Sumitomo Corporation Group and a Regional Company of SC Europe & CIS Group.

### SCOPE OF APPLICATION

---

This Compliance Manual is applicable, in the terms expressed therein, to the Directors, Officers and Professionals of SCSP, hereinafter "the Addressees", who shall act in accordance with its content, regardless of their hierarchical level or their geographical or functional location.

### COMPLIANCE CULTURE AT SCSP

---

**SCSP** is committed to maintaining and improving an effective "Culture of Compliance" in the Organisation, which leads each and every one of **SCSP's** professionals to comply at all times with current legislation in all areas of its activity.

**SCSP's** Compliance Manual includes the different documents on which its Crime Prevention and Detection System is based, which are listed below:

- **The Crime Prevention and Detection Policy** reflects the commitment of senior management to the observance of the highest standards of transparency, ethics and responsibility, with the aim of preventing and detecting the commission of any type of illegal act. This commitment must be transferred to the rest of the professionals that make up SCSP, as well as to those third parties and organisations with which it has relations.

- **The Code of Ethics and Conduct** is framed within the context of SCSP's Crime Prevention and Detection System, detailing the principles by which its professionals must abide in order to comply with current legislation and the ethical framework, with the aim of guiding the behaviour of all its members in their relations with the different stakeholders.
- **The Crime Prevention and Detection Protocol** describes the elements that make up the SCSP Crime Prevention and Detection System. It specifies the operations to be followed to prevent and mitigate the potential risks identified in its sphere of action, establishing the procedures, controls and measures required by the current Criminal Code that allow accreditation that the Organisation exercises due control over its managers and employees.
- **The Communication Channel** is an essential element of the Crime Prevention and Detection System as it facilitates SCSP professionals how, and what illegal activities or actions contrary to the Code of Ethics and Conduct can and/or must be communicated, without fear of being persecuted, discriminated against or suffering any other type of reprisal.
- **The SCSP Compliance Committee** assumes the function of control and supervision of the compliance structure at SCSP. Acting with autonomy and independence, it will periodically evaluate the effectiveness of the Crime Prevention and Detection System, as well as the procedures and controls implemented, proposing the corrective measures it deems appropriate.
- **Training and Awareness** is essential to effectively implement a "Culture of Compliance" in the Organisation, providing knowledge and generating a climate of respect for the law in order to prevent the possible engagement of unlawful conduct or conduct contrary to the Code of Ethics and Conduct.

## TONE FROM TOP MANAGEMENT

---

SCSP's Regulatory Compliance Culture is based on compliance with the Law, as well as with national and international ethical standards, with the aim of reinforcing the confidence of its stakeholders. The Board of Directors and senior management will continue to disseminate this message among all the professionals who make up SCSP, setting an example of strict compliance with current legislation.

## CRIME PREVENTION AND DETECTION POLICY

---

### OBJECTIVE OF THE CRIME PREVENTION AND DETECTION POLICY

---

The Board of Directors of SCSP, within the scope of its functions of supervision and definition of strategies and policies of the organisation, approves this Crime Prevention and Detection Policy.

The main objective of the Crime Prevention and Detection Policy is to convey from the Board of Directors to the management team and employees, as well as to those third parties and organisations with which it has relations, that the organisation is committed to achieving and respecting the highest standards of transparency, ethics and responsibility with the aim of preventing the commission of any type of illegal act.

In order to adapt to the new obligations imposed by Organic Law 5/2010, of 22 June, which modifies Organic Law 10/1995, of 23 November, of the Criminal Code and by Organic Law 1/2015, SCSP is going to develop a programme for the prevention, detection and reaction to the possible commission of crimes. This programme includes the creation of a "compliance committee" to supervise and coordinate all the assets involved.

Through this programme, SCSP intends to guarantee and accredit that it exercises due control over its managers and employees vis-à-vis the judicial and administrative bodies, as well as other third parties related to SCSP. The purpose of these controls will be to detect potential risk situations that may arise in SCSP's sphere of action, as well as to establish measures to reduce this risk, not only at the level of illegal criminal acts but also of irregular conduct in general that contravenes the Organisation's Code of Ethics and Conduct.

### SCOPE OF ACTION

---

This Crime Prevention and Detection Policy applies to all members of SCSP, i.e. it shall apply to members of the Board of Directors, management team and employees.

When members of SCSP participate as representatives of the organisation in other entities, they shall also remain committed to this Policy and shall promote the application of the principles of action in these entities as far as possible.



## PRINCIPLES OF ACTION

---

The principles of action on which this Crime Prevention and Detection Policy is based are as follows:

- Pursue the highest standards of transparency, honesty and responsibility, promoting zero tolerance for irregular and illegal actions within SCSP.
- To respect the legislation in force applicable to the Organisation's sphere of action and, specifically, its internal regulations as set out in the Code of Ethics and Conduct.
- To implement the appropriate measures to prevent the commission of unlawful acts by establishing control processes within the reach of employees, managers and Governing Bodies. These controls must be up to date and continuous and aimed at avoiding the existence of any person not subject to them.
- Promote the involvement of staff in the prevention and detection of illegal acts through training on the subject, as well as promoting the promotion of the "Whistleblower Channel" as a means of communication of conduct that could imply criminal risks for SCSP, as well as any conduct contrary to the Code of Ethics and Conduct and to the law in general.
- Create a figure to coordinate these actions. In the case of SCSP, the figure of the "SCSP Compliance Committee" is defined.
- Facilitate the actions of the "SCSP Compliance Committee", providing it with the appropriate means and tools necessary to carry out its work in an optimal and efficient manner.
- React promptly and effectively to a report of an allegedly criminal act and proceed with its investigation, respecting the rights of both the complainant and the accused(s) and taking care to avoid acting in a disproportionate and discriminatory manner when establishing sanctions and any other type of disciplinary measures.
- Bring suspected offences to the attention of the competent authorities, offering full cooperation in any subsequent investigations that may arise.

## WHAT IS AN ILLEGAL ACTIVITY?

---

Any illicit and/or illegal behaviour that falls under any of the types established in our Criminal Code (currently article 31 bis) and which entails the criminal liability of the Organisation within which and for whose benefit it has been implemented.

Risk activities are those conducts inherent to the different SCSP activities in the exercise of which the commission of a crime could occur. The classification of an activity as "risky" does not imply that

it is illicit or criminal, but rather that it is an activity in which, if due precautions are not taken, situations may arise that may generate conflicts with criminal implications.

Spanish Criminal Code contemplates a catalogue of crimes in which the organisation can be charged together with those who have intervened in their commission, although only some of them are likely to be committed, since the rest, either because of the organisation's own activity or because they correspond to crimes usually committed by organised criminal networks, have not been considered probable. The list of criminal offences are as follows:

Criminal Type	Criminal Code Articles
Illegal Organ Trafficking	156 bis
Human trafficking	177
Crimes relating to prostitution, sexual exploitation and corruption of minor	187 - 189
Crimes of Discovery and Disclosure of Secrets	197
Scams and frauds	248 y 251
Frustration of enforcement	257 y 258 bis
Punishable insolvency	259 - 261
IT damage	264
Intellectual and industrial property, market and consumer crime	270 - 286
Business corruption	286 bis - ter
Money laundering and terrorism	301 - 580
Illegal financing of political parties	304 bis
Crimes against the Treasury and Social Security	305 - 308
Accounting crimes	310
Illegal trafficking and illegal immigration crimes	318 bis
Crimes against town and country planning and urban planning	319
Environmental crime	325 - 327
Crimes relating to nuclear energy and ionising radiation	343
Risk crimes caused by explosives and other agents	348
Crimes against public health and drug trafficking	359 - 369
Counterfeiting currency and means of payment	386 y 399 bis
Bribery	419 - 427

Criminal Type	Criminal Code Articles
Influence peddling	428 - 430
Crimes relating to fundamental rights and public freedoms	510
Financing terrorism	576

The following criminal offences will also be reviewed:

Criminal Type	Criminal Code Articles
Price-fixing crimes in public tenders and auctions	262
Corporate crimes (impeding supervisory activity)	294
Crimes against workers' rights (freedom of association and prevention of occupational hazards)	311 - 316

## EVALUATION AND REVIEW. CONTROL

### 1. Assessment and Review.

The "SCSP Compliance Committee" has the power of initiative and control to evaluate and supervise the effectiveness of the Crime Prevention and Detection Policy at SCSP. It shall evaluate at least once a year the implementation and development of the Crime Prevention and Detection Policy in order to be able to report information on its effectiveness and the need for improvements, if any, to the Board of Directors of SCSP.

### 2. Control.

The "SCSP Compliance Committee" is responsible for controlling and supervising the correct implementation and compliance of the Crime Prevention and Detection Policy, as well as SCSP's Code of Ethics and Conduct.

Given that the Board of Directors of SCSP has been attributed the functions of management and supervision and, specifically, that of "exercising the senior management of SCSP by determining its strategic action plans and the general guidelines for their execution", it is envisaged that the "SCSP Compliance Committee" will report to the Board of Directors of SCSP on the conclusions relating to the implementation and compliance with the Crime Prevention and Detection Policy periodically through the "Report on the review of the status of the Crime Prevention and Detection System".

## POLICY STATEMENT

---

As a commitment and collaboration of the SCSP Management towards the Crime Prevention and Detection Policy, the following declaration is presented:

At the express wish of the SCSP Management, we declare our commitment, engagement and initiation of the appropriate actions to achieve the implementation of the Crime Prevention and Detection System, based on the requirements of Law 5/2010 amending the Criminal Code, which introduced for the first time a criminal liability of a legal entity for the performance of certain unlawful actions of their administrators and Law 1/2015 which develops liability assumptions, requiring companies and managers to incorporate new compliance obligations.

The framework of the Crime Prevention and Detection System is based on the following objectives:

- To ensure an adequate level of Crime Prevention and Detection managed by SCSP, providing our clients and employees with services based on the highest standards of transparency, honesty and responsibility, promoting zero tolerance for irregular and illegal actions within our organisation.
- To improve training and awareness among staff involved in the provision of services.
- To increase the effectiveness and efficiency of internal processes.
- The objectives for this period will be set annually by management.

This level is based on the relevant risk analysis. Risks to SCSP's processes have been identified and will be assessed on an ongoing basis, planned to be controlled and reduced where possible, and continuously monitored, in accordance with SCSP's risk analysis methodology, which sets out the criteria for risk estimation.

In order to achieve our goals, this Crime Prevention and Detection Policy has been established at all levels of SCSP. This Policy allows for continuous improvement of our business processes and greater training of our staff in the Prevention and Detection of Crimes, guaranteeing, among other aspects, that the System is aligned at all times with the objectives of SCSP, with the established risk management, taking into account the legal requirements, regulations and contractual obligations, and that it has the necessary resources for its correct operation, maintenance and continuous improvement.

To achieve this level, it is necessary, and this is understood by SCSP management, to achieve total commitment and collaboration between the various departments, facilitating the appropriate channels of communication and collaboration.

SUMITOMO CORPORATION ESPAÑA, S.A.

# CODE OF CONDUCT AND ETHICS

Crime Prevention and Detection System



## CODE OF ETHICS AND CONDUCT

---

### INTRODUCTION

---

At its meeting in September 2019, the Board of Directors of SCSP approved this Code of Ethics and Conduct, which reflects the company's commitment to act with integrity, responsibility and transparency, in accordance with the Law and high ethical and moral values.

This Code is framed within the context of the implementation of a Crime Prevention and Detection System, with the vocation of guiding the behaviour of all its members in their relations with the different stakeholders.

The Code includes the ethical and deontological values of SCSP and details the principles by which the behaviour of its members must be governed in order to comply with current legislation.

The guidelines of this Code of Ethics and Conduct contribute to reaffirming SCSP's commitment to improving the management and transparency of its activities, which will result in a better service and contribute to improving its positioning and reputation in the market.

### OVERVIEW

---

#### PURPOSE OF THE CODE

---

SCSP's Code of Ethics and Conduct is intended to develop and formalise its mission and values, and to serve as a guide for the actions of its professionals in a global, complex and changing environment.

The Code of Ethics and Conduct has been drawn up taking into account national and international recommendations in this area, constituting a basic reference for its monitoring. It also responds to the new prevention obligations imposed in the field of criminal liability of legal entities by Law 1/2015.

The Code of Ethics and Conduct reflects SCSP's commitment to the principles of ethics and transparency in all its areas of activity, establishing a set of principles and guidelines for conduct aimed at guaranteeing the ethical and responsible behaviour of all its professionals in the development of their activity.

The Code of Ethics and Conduct forms part of the SCSP Compliance Manual.

## SCOPE OF APPLICATION

---

This Code of Ethics and Conduct is applicable, in the terms expressed therein, to the Directors, Officers and employees of SCSP, hereinafter "the Addressees", who shall act in accordance with its content, regardless of their hierarchical level, geographical or functional location.

The Code of Ethics and Conduct, by its nature, does not cover all possible situations, but establishes criteria to guide the conduct of SCSP employees.

The recommendations contained in this Code do not replace any provision established by any existing Agreement, Law or Regulation, but complement them. In case of doubt about the conduct to be followed in a professional situation, advice shall be sought from the line manager or the SCSP Compliance Committee.

## SCSP ETHICAL COMMITMENT

---

The purpose of this Code of Ethics and Conduct is to determine the principles of behaviour and action of SCSP members.

SCSP individuals must diligently perform their assigned tasks, acting in accordance with the ethical and conduct principles outlined below.

### 1. Ethical Principles

---

SCSP employees:

- a) Respect the Constitution and the rest of the rules that make up the Legal System.
- b) Base their actions on objective considerations oriented towards impartiality and the common interest, without consideration of any other factor that expresses personal, family, corporate, client or clientelist positions or any others that may collide with this principle.
- c) They shall act in accordance with the principles of loyalty and good faith towards SCSP, their superiors, colleagues and subordinates.
- d) Base their conduct on respect for fundamental rights and public freedoms, avoiding any action that could lead to any discrimination, for whatever reason, on the grounds of birth, racial or ethnic origin, gender, sex, sexual orientation, religion or beliefs, opinion, disability, age or any other personal or social condition or circumstance.
- e) Abstain in those matters in which they have a personal interest, as well as from any private activity that could give rise to a conflict of interest with their position at SCSP.

- f) Do not enter into financial obligations or intervene in financial transactions, property obligations or legal transactions with persons or entities when this could lead to a conflict of interest with the obligations of their position at SCSP.
- g) Act in accordance with the principles of effectiveness, economy and efficiency, and are vigilant in pursuing the general interest and the fulfilment of SCSP's objectives.

## 2. Principles of Conduct

---

SCSP employees:

- a) Treat clients, their superiors, their colleagues and the rest of the people who make up SCSP with attention and respect, refraining from violating the rights and dignity of their colleagues, harming their physical or mental health or compromising their professional future.
- b) Carry out the tasks corresponding to their job in a diligent manner, complying with the established working day and timetable.
- c) Maintain a working environment in which respect and professionalism prevail, avoiding any type of inappropriate or unprofessional behaviour.
- d) Obey the professional instructions and orders of their superiors, unless they constitute a clear breach of the legal system, in which case they must immediately inform the SCSP Compliance Committee or SCEU Compliance Committee (collectively "Compliance Committee") and/or the competent authorities.
- e) Manage SCSP's resources and assets with austerity and do not use them for their own benefit or for the benefit of persons close to them. They also have the duty to ensure their conservation.
- f) Do not accept or request any favourable treatment or situation that implies privilege or unjustified advantage from individuals or private entities.
- g) Refuse any gift, favour or service on advantageous terms that goes beyond the usual social and courtesy customs (promotional material, Christmas gifts), that could influence the impartiality with which they must perform their duties and that constitutes a commitment by the recipient to grant preferential treatment to the donor.
- h) Do not influence in the speeding up or resolution of administrative formalities or procedures without just cause and, in no case, when this entails a privilege for the benefit of the holders of public office or their immediate family and social environment or when it entails a detriment to the interests of third parties.



- i) diligently perform the tasks assigned or entrusted to them and, where appropriate, resolve matters within their competence in a timely manner.
- j) Keep confidential matters confidential and maintain due discretion on those matters that come to their knowledge by reason of their position and may not make use of the information obtained for their own benefit or that of third parties, or to the detriment of the public interest and/or SCSP.
- k) Ensure that documents are recorded and kept for their transmission and delivery to those subsequently responsible for them.
- l) Observe the rules on occupational health and safety.
- m) Bring to the attention of their superiors or the competent bodies any proposals they consider appropriate to improve performance of the area's functions.
- n) Inform the Compliance Committee of any irregular and/or unlawful conduct within SCSP, through the Communication Channel.

### 3. Commitment to Human Rights

---

- a) SCSP professionals must comply with applicable employment laws, avoiding at all times forced or underage labour.
- b) No SCSP employee shall be discriminated against on the basis of race, religion, age, nationality, gender or any other personal or social status.
- c) Any conduct that could create an intimidating, offensive or hostile working environment is prohibited at SCSP.
- d) SCSP Professionals have the recognised right to organise, freedom of association and collective bargaining.

### HEALTH AND SAFETY AT WORK

---

#### OBJECTIVES

---

SCSP's objectives in the area of Health and Safety at Work are as follows:

- To prioritise the prevention of incidents as a guarantee of safeguarding the health and safety of professionals.
- To promote the health and safety of professionals through the application of measures and the development of activities necessary for the prevention of risks arising from work.

- That SCSP professionals know and comply with the rules of occupational risk prevention, ensuring compliance with the prevention measures adopted in each case, for their own health and safety and for that of others who may be affected by their professional activity, due to their acts and omissions at work, in accordance with their training and the company's instructions.

## OBLIGATIONS

---

The Health and Safety regulations oblige all SCSP professionals and collaborators to comply with the following premises:

- Correctly use the resources and protective equipment provided by the company in accordance with the instructions received from the company, as well as safety devices existing or to be installed in the environments related to their activity or in the workplaces where this activity takes place.
- Immediately inform their direct hierarchical superior of any situation that, in their opinion, entails, on reasonable grounds, a risk to the safety and health of the professionals.
- Contribute to the fulfilment of the obligations established by the competent authority in order to protect the safety and health of professionals at work.
- Cooperate with the company to ensure safe working conditions that do not pose a risk to the safety and health of professionals.

## AVOIDING CONFLICTS OF INTEREST

---

### OBJETIVES

---

The objectives of the Conflict of Interest Policy are:

- Maintain at all times a level of integrity that allows confidence in the judgement and actions of our professionals. To this end, they will carry out their work with honesty, correctness and responsibility, respecting the law and disclosing the appropriate information in accordance with the law and their professionalism.



- Avoid situations that may involve a conflict between their personal interests and those of the company. They must also abstain from representing the company and from intervening in or influencing the taking of decisions that interfere with the correct fulfilment of their professional duties and responsibilities or in which, directly or indirectly, they or a third party linked to them, have a personal interest.
- Not to use their position in the company to obtain financial or personal advantages or business opportunities of their own.
- Inform the company through their line manager or the SCSP Compliance Committee in order to resolve the situation in a fair and transparent manner.

## OBLIGATIONS

---

SCSP Professionals must not:

- Receive remuneration and/or advantages from suppliers, competitors or customers.
- Engage in any business or activity that directly or indirectly competes or interferes with SCSP.
- Allow an SCSP professional to be a supplier to the company at the same time.
- Participate in or influence the requirements, negotiations and decision-making processes with clients or suppliers with whom they have a direct or indirect personal relationship, or any interest other than that of the company, by which any of them may obtain a personal benefit.

## CONFIDENTIALITY OF COMPANY INFORMATION

---

## OBJETIVES

---

The objectives of our Information Confidentiality Policy are:

- Protect our confidential information and respect the confidential information of others.
- Avoid disclosure of SCSP's proprietary and/or confidential information.

## OBLIGATIONS

---

All SCSP Professionals have an obligation to protect the information and knowledge generated within the organisation and its property:

- The Confidential Information of SCSP to be protected is:
  - a) SCSP's Accounting and Financial Information.
  - b) The Business and/or Strategic Plan, as well as Operations related to financing.
  - c) Business Policies and Practices.
  - d) Judicial or administrative disputes.
  - e) Research and development of new products.
  - f) Personal information of professionals, customers, partners, etc.
  - g) Intellectual and industrial property, such as trade secrets, trademarks, patents, etc.
  - h) Lists of customers, suppliers and pricing policy.
- Must not disclose or communicate confidential information to third parties, except in compliance with applicable regulations, or when they have been expressly authorised to do so, and must refrain from using any data, information or document obtained in the course of their professional activity for their own benefit.
- Must not copy or share confidential information without first making sure that they are authorised to do so. In case of doubt, they shall first consult their line manager or the Compliance Committee.
- Must commit to maintaining the confidentiality of the information, using it only for the purpose for which it was obtained.
- The obligation of confidentiality shall remain after the employment relationship with SCSP has ended and shall include the obligation to return any company-related material in their possession at the time of termination of the employment relationship.
- Employees shall not use inappropriately obtained or confidential information from other companies without the authorisation of their legitimate owners, and it is prohibited to take possession of written or electronic documents, computer media or other means of discovering confidential information from these companies.



- Employees shall immediately report to their hierarchical superior or to the SCSP Compliance Committee any suspicion of improper use or unauthorised dissemination of confidential information of the Company.

## PROTECTION OF PERSONAL DATA

---

### OBJETIVES

---

SCSP guarantees the right to privacy of professionals and clients under the terms set out in the current legislation, protecting their privacy and their Personal Data, not disclosing them except with the consent of the interested parties or in the event of a legal obligation or in compliance with judicial or administrative resolutions.

### OBLIGATIONS

---

SCSP employees:

- Those who have authorised access must protect Personal Data against unauthorised or accidental disclosure, modification, destruction or misuse, whatever the medium on which the data is contained.
- They must maintain the utmost confidentiality for an indefinite period of time, not disclosing or transferring Personal Data contained in any type of medium to third parties, unless duly authorised to do so.
- They may create files containing Personal Data but only for temporary use, provided that this is necessary for the performance of their work. Such temporary files must be destroyed when they are no longer useful for the purpose for which they were created. The Head of Information Technology and Systems shall be notified, for registration and notification, if it is deemed appropriate for such files to remain open.
- If they access Personal Data, they must immediately return the media containing the data, their possession being understood to be strictly temporary after the completion of the tasks that have caused the use of the information.
- If they use devices or media (CD, pendrive, etc.) containing Personal Data, they must keep them in a safe place and always under lock and key when they are not in use, especially outside the working day.

- They must notify the Head of IT and Systems of any incident or accident they detect that affects or may affect the security of Personal Data, such as: the loss of lists, CDs, pendrives or any other medium containing files with data on individuals, or suspicions use by third parties of unauthorised access to the computer network or applications, or alterations to data or recovery of data from unauthorised backup copies, etc.

## USE AND PROTECTION OF COMPANY ASSETS

---

### OBJECTIVES

---

- Proper use and care of the company's assets.
- Avoid accidents and increase the useful life of assets.
- Protect the company's assets (including furniture, installations and equipment).

### OBLIGATIONS

---

#### SCSP EMPLOYEES:

- Must protect the company's assets and property against the risks of loss, damage or misappropriation, making good use of them.
- Must protect and care for the resources at their disposal or to which they have access, making no more use of them than is necessary for the proper performance of their duties, in a responsible, efficient and appropriate manner to the environment of their professional activity.
- May not use technological resources to: (i) Issue personal opinions on behalf of SCSP or access forums or social networks for the same purpose, except with express consent to that effect. (ii) Store or distribute or visit internet sites with inappropriate material that violates human rights, privacy, honour, self-image, religious freedom, or the dignity of persons, such as racism, xenophobia, apology for violence or terrorism, and pornographic or sexist material. (iii) Use, introduce, download, copy, transmit, reproduce, distribute or store any type of software, published work or invention protected by intellectual or industrial property without the corresponding licence or authorisation.
- You should be aware that SCSP reserves the right to audit user access to: programmes, data, internet, software installed on your equipment, use of mail and in general access



to and use of the company's information systems by the user, in accordance with the policies that it has developed and communicated in this respect in a timely manner.

## PREVENTING CORRUPTION IN BUSINESS

---

### OBJETIVES

---

The objectives of our Anti-Corruption Policy are:

- Preventing corruption in business and actively and permanently combating it.
- The actions of the people who work at Sumitomo Corporation Group must always be based on criteria of efficiency of the organisation linked to the fulfilment of its mission and the guidelines of Management.
- Reject corruption in all its forms, prohibiting the offering or acceptance of gifts, bribes or any other form of corruption, aimed at the payment or receipt of illicit benefits to/ or from customers, suppliers and public officials.

### OBLIGATIONS

---

The Anti-Bribery and Anti-Corruption regulations oblige all persons on SCSP's governing bodies and professionals to comply with the following premises:

- **Transparency**

To observe the greatest possible transparency in the processes of decision-making, planning and effective use of resources, objectives and their fulfilment, maintaining their independence and rigour.

To provide truthful, complete and reliable information about the company and, under no circumstances, knowingly provide incorrect or inaccurate information that could mislead the recipient.

- **Obligation to Unmask Corruption**

On the other hand, there is a right and obligation to report and expose any corrupt action in which they are witnesses or victims.

Any well-founded suspicion of the commission of a corrupt action must be reported to the Compliance Committee through the Communication Channel, which will analyse and assess the

information received, safeguarding the rights of the affected parties in accordance with its action protocol.

- **Prevention of Money Laundering**

All professionals must comply with the applicable legal provisions and pay particular attention to cases where there are indications of lack of integrity of persons or entities with whom business relations are maintained, such as, inter alia, payments that are unusual in view of the nature of the transaction, payments made to or by third parties not mentioned in the contract, payments to persons or entities resident in tax havens or to bank accounts opened in offices located in tax havens, payments to entities where it is not possible to identify the partners or ultimate beneficiaries, extraordinary payments not foreseen in the contracts.

## **GIFTS AND HOSPITALITY**

---

All SCSP Professionals should avoid receiving gifts in order to show that the company's dealings are within a framework of transparency and ethics, i.e. that they do not constitute a commitment by the recipient to give preferential treatment to the donor, such as being granted contracts, better prices or more favourable bargaining terms.

Do not solicit, offer or accept: gifts, hospitality and/or favours, including hospitality details or payments for travel or expenses, offers of entertainment, political or charitable donations, community benefits, club memberships and confidential or privileged information, which may affect a decision of the company, customers, suppliers or third parties, that are not produced on reasonable grounds. Small gifts or presents are permitted as a courtesy in the context of business relationships (both giving and accepting).

## **OBJETIVES**

---

The objectives of our Gifts and Gifts Policy are:

- No gifts should influence the business decisions of SCSP or its customers, suppliers or related third parties.
- No employee may take advantage of the company's business contacts for his or her own benefit, for the benefit of others or to the detriment of the company.
- Avoid legal consequences for the company and for the own professionals.
- Professionals should consult their line manager or the SCSP Compliance Committee if there are doubts about the appropriateness of accepting or offering a gift or attention.



- If the Gifts and Hospitality Policy does not clarify any doubts about what is acceptable, the offer should be declined or, where appropriate, discussed with the SCSP Compliance Committee.

## OBLIGATIONS

---

- It is forbidden to solicit or receive gifts and hospitality, except when they are promotional materials or hospitality with acceptable and customary industry standards and practices.
- Be cautious in accepting gifts and hospitality and ensure that the acceptance of gifts or hospitality does not compromise integrity or objectivity, or create an expectation of obligation to the third party, especially when dealing with suppliers or public authorities.
- Any gifts or hospitality offered must be accounted for in accordance with current accounting standards.
- Gifts in excess of the established financial limit, which currently stands at 200 euros or other amount provided in SC Europe & CIS Group's relevant rule, whichever is lower, will not be accepted.

## STAKEHOLDER RELATIONS

---

### SUPPLIER RELATIONS

---

SCSP's suppliers shall at all times maintain ethical behaviour that enables them to establish legitimate and productive relationships with SCSP. This means that they shall not make or offer any payment in cash, in kind or any other equivalent or benefit to any individual within the company in order to obtain or be favoured in any business dealings or cause relating to contracting with SCSP.

SCSP practitioners should seek out and select only suppliers whose business practices respect human dignity, do not violate the law, and do not jeopardise the reputation of the company. Professionals working to select suppliers should follow a set of criteria with the objective of reconciling the interests of the company and the desirability of maintaining stable relationships.

## CUSTOMER RELATIONS

---

SCSP professionals must act with integrity towards the company's clients, aiming to anticipate their needs and provide clients with a quality product and service, committing ourselves to the values of good treatment, attention, respect, honesty and service.

SCSP professionals will respect the commitments acquired with clients, but if any unforeseen circumstance should arise that makes it impossible to carry out or fulfil the commitment made, it is the obligation of the person involved to inform their immediate superior and the client in due time.

## RELATIONS WITH PUBLIC ADMINISTRATIONS

---

SCSP Professionals, in their relationship with Public Administrations, shall comply ethically with all legal and contractual obligations, responding to requests and requirements for information from them.

They shall not request, offer or accept gifts and hospitality to or from representatives of Public Administrations that may affect the impartiality of either party, influence a business decision, lead to improper performance of professional duty or involve unjustified favourable treatment.

They shall treat each other courteously, without gifts or distinctions, maintaining strictly professional relations with the different representatives of the Public Administration and the Authorities.

SCSP shall not make contributions for political purposes contrary to the Law, nor shall it obtain favourable treatment by using sponsorship or donations, direct or indirect, to parties, political or trade union organisations, their representatives and candidates, as a means to achieve it.

## RESPECT FOR THE ENVIRONMENT

---

SCSP and its Professionals, within the scope of their competences, are actively and responsibly committed to the conservation of the environment, respecting the legal requirements and carrying out their activities in such a way as to minimise their environmental impact, following the recommendations and procedures that, where appropriate, will be established by SCSP, taking into account the environment in which it operates.

Conservation and respect for the environment is manifested in compliance with the best environmental practices in all its activities, a firm commitment against climate change, the promotion of energy saving, the rationalisation of water use and management, the responsible use of resources, effective waste management, the prevention of pollution and the protection of the natural

environment and biodiversity, all through the prevention and minimisation of adverse environmental impacts and the conservation of natural resources.

All SCSP professionals must be aware of and accept this policy and strive to minimise the environmental impact of their activities and the use of the facilities, equipment and working resources placed at their disposal.

## COMPLIANCE STRUCTURE AND CONTROL ENVIRONMENT

---

### COMPLIANCE STRUCTURE

---

#### 1. SCSP Compliance Committee

---

The SCSP Compliance Committee, appointed by the Board of Directors of SCSP, is responsible for supervising the application and compliance with this Code of Ethics and Conduct.

The SCSP Compliance Committee shall have the material and human resources necessary for the performance of its functions.

Any doubts that may arise for SCSP professionals regarding the interpretation of this Code of Ethics and Conduct must be consulted with the SCSP Compliance Committee.

The SCSP Compliance Committee shall report, at least annually and whenever it deems necessary or is required to do so, to the Board of Directors of SCSP on the measures adopted to promote awareness and ensure compliance with the Code of Ethics and Conduct.

The SCSP Compliance Committee shall have the following functions:

- a) To promote the disclosure, knowledge, application and compliance with the Code of Ethics and Conduct.
- b) Resolving any queries or doubts that may arise in relation to the content, interpretation, application or compliance with the Code of Ethics and Conduct.
- c) Annual assessment of the degree of compliance with the Code of Ethics and Conduct, which shall be reported to the Board of Directors.
- d) To manage the SCSP Communication Channel and to carry out the corresponding investigation and processing of the complaints received.
- e) Any others, of a singular or permanent nature, that may be assigned to it by the Board of Directors, or that may be attributed to it by the Crime Prevention and Detection Policy.
- f) To promote and ensure compliance by the entire SCSP team with current legislation.

## 2. Communication Channel

---

SCSP has a Communication Channel managed by Compliance Committee and an external entity ("External Reporting Line") in order to promote compliance with the law and the rules of conduct of the Code of Ethics and Conduct (hereinafter collectively referred to as "Communication Channel"). SCSP professionals are provided with a card containing the contact details of the External Reporting Line.

The Communication Channel is confidential in order to facilitate the communication by SCSP professionals of conduct that may imply the commission of any irregularity or any act contrary to the law or to SCSP's rules of conduct set out in the Code of Ethics and Conduct.

The processing of enquiries or complaints made through the Communication Channel shall be the responsibility of the Compliance Committee, unless the complaint is directed against it, in which case it shall be processed by the Board of Directors. In any investigation, the rights to privacy, to defence and to the presumption of innocence of the persons under investigation shall be guaranteed.

The provisions contained in the Crime Prevention and Detection Policy relating to the operation of the Communication Channel are developed in a specific procedure.

## CONTROL ENVIRONMENT

---

The control environment is made up of the set of ethical principles and codes of conduct, as well as the policies, procedures and controls that regulate the operation of the Company and which, consequently, determine the conduct and guidelines for action of its professionals, managers and members of the Board of Directors of SCSP.

Within the structure of the control environment, this Compliance Manual includes the following protocols for the Prevention, Detection and Reaction to the perpetration of criminal acts within SCSP, which are specifically developed in the document "Protocol for the Prevention and Detection of Crimes".

### 1. Prevention Protocol:

---

Its purpose is to prevent potential breaches or violations of the Compliance Manual and, therefore, to mitigate the likelihood of criminal acts being committed within SCSP.

In this context, the main activities carried out are:

- a. The identification of activities at risk of committing crimes;
- b. The implementation of preventive controls;
- c. Communication and training of SCSP staff.

## 2. Detection Protocol:

---

Its objective is focused on detecting certain breaches of the Compliance Manual, resulting from an ineffective operation of the preventive controls, as a consequence of errors in the execution of these controls, either unintentionally or as a consequence of malicious attitudes involving fraud or deceit.

In this context, SCSP has the following means at its disposal:

- a. A Code of Ethics and Conduct,
- b. A Communication Channel, and
- c. Procedures for periodic evaluation of the controls set out in the SCSP Compliance Manual.

## 3. Reaction and Response Protocol:

---

Its objective is to establish the guidelines for action once it has become aware of the existence of possible criminal or irregular conduct within it, whether as a result of the operation of internal control mechanisms, a formal complaint or through the media, social networks, etc., or due to an investigation by the Public Prosecutor's Office or the initiation of criminal legal proceedings.

In this context, SCSP has the following procedures:

- a. Pre-Procedural Action Protocol.
- b. Collaboration in the Investigation.
- c. Protocol for Procedural Action.
- d. Designation of the Procedural Representative.
- e. Reparation of Damage.
- f. Complaint/Disciplinary Measures.

## MISCELLANEOUS PROVISIONS

---

### COMMUNICATION, DISTRIBUTION AND EVALUATION

---

The Code of Ethics and Conduct shall be communicated and distributed among SCSP professionals by the SCSP Compliance Committee and shall be made available to them on the corporate intranet. The external diffusion of the Code of Ethics and Conduct shall be the responsibility of the SCSP management team.

The SCSP Compliance Committee shall evaluate and produce an annual report on the degree of compliance with the Code of Ethics and Conduct. The report shall be communicated to SCSP management.

## DISCIPLINARY REGIME

---

SCSP shall develop the necessary measures for the effective application of the Code of Ethics and Conduct.

SCSP may formally request, with supporting documentation, its employees and third parties to periodically confirm compliance with the Code. Likewise, ethics and compliance issues may be included in training programmes, performance evaluation processes and/or the assessment of potential candidates or third parties.

Non-compliance with any of the principles contained in the Code will be analysed in accordance with internal procedures, existing agreements and legal regulations. When a breach is identified, the Human Resources Department will analyse the application of disciplinary actions in accordance with the system of offences and penalties set out in the collective bargaining agreement or in the applicable employment law legislation, if it is considered an action contrary to the principles of contractual good faith.

No one, regardless of their level or position, is authorised to request a professional to commit an illegal act or an act that contravenes the provisions of the Code of Ethics and Conduct. In turn, no professional may justify improper or illegal conduct or conduct that contravenes the provisions of the Code of Ethics and Conduct on the grounds of an order from a hierarchical superior.

The following shall be considered very serious breaches: the commission of unlawful or criminal conduct, as well as the adoption of retaliatory measures against any employee who has reported unlawful or criminal conduct.

In the case of SCSP, it is applicable the Collective Bargaining Agreement for Offices which establishes the disciplinary regime and the applicable procedure. SCSP also has an Employee Manual which sets out the conducts that can be sanctioned and the corresponding disciplinary measures.

## UPDATE

---

The Board of Directors of SCSP shall periodically review and update the Code of Ethics and Conduct, taking into account the annual report of the SCSP Compliance Committee, as well as the suggestions and proposals made by SCSP professionals.

## ACCEPTANCE

---

SCSP employees expressly accept the values, principles and rules of conduct set out in the Code of Ethics and Conduct.

Professionals who, in the future, join or become part of SCSP, expressly accept the rules of conduct set out in the Code of Ethics and Conduct.

## VALIDITY

---

This Code of Ethics and Conduct has been approved by the Board of Directors of SCSP at its meeting in September 2019, and shall remain in force until such time as it is amended.

SUMITOMO CORPORATION ESPAÑA, S.A.

# CRIME PREVENTION AND DETECTION PROTOCOL

Crime Prevention and Detection System



## CRIME PREVENTION AND DETECTION PROTOCOL

---

### OBJECT

---

Within the framework of the Crime Prevention and Detection programme developed at SCSP, and in order to ensure compliance with general regulations within the organisation, the Crime Prevention and Detection Protocol is defined.

Its objective is to specify the actions to be followed at SCSP in relation to the activities develop, in order to identify, prevent and mitigate potential risks that have been identified, establishing:

- The activities and procedures necessary for its effective implementation in SCSP.
- Risk identification and mitigation mechanisms.

This protocol is complemented by the documents developed as part of the Crime Prevention and Detection System, such as:

- Crime Prevention and Detection Policy.
- Regulations of the compliance committee.
- Code of Ethics and Conduct.
- Risk Analysis Methodology.
- Risk Analysis Report.
- Improvement Plan.
- Communication Channel Procedure.

### GENERAL DEFINITIONS

---

The following general definitions are established: <sup>1</sup>:

- **Risk criteria:** terms of reference against which the importance of a risk is assessed.
- **Collaborator:** SCSP employee and subcontracted personnel.
- **Offence:** unlawful act or omission, wilful or negligent, intentional or reckless, to which a penalty is attributed by law.

---

<sup>1</sup> Definitions mostly taken from the document published by AENOR "Sistema de Gestión de Riesgos para la Prevención de Delitos en las Organizaciones. Requirements".

- **Risk assessment:** the process of comparing the results of the risk analysis with the risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
- **Risk management:** coordinated activities to direct and control an organisation regarding risk.
- **Board of Directors:** guarantor of the proper functioning of the organisation. Executive nature and external relations.
- **Executive Committee:** executes the guidelines and policy decided by the Board of Directors.
- **Governing Council:** Highest hierarchical level of the organisation, in charge of establishing policies and lines of action for subsequent execution by the administrative and management bodies.
- **Legal entity:** any type of public or private organisation capable of rights and obligations, with the capacity to act as a subject of law.
- **Risk management process:** the systematic deployment of policies, procedures and management practices to the activities of communication, consultation, context setting, and risk identification, analysis, assessment, evaluation, monitoring and review.
- **Risk:** the effect of uncertainty on the achievement of objectives.
- **Residual risk:** risk remaining after risk treatment.
- **Crime prevention management system:** set of internal measures that enable compliance with the crime risk prevention policy established by the legal person and that demonstrate sufficient diligence in preventing the commission of acts constituting crimes, as well as repairing and mitigating the effects of the crimes committed, to mitigate the criminal liability of the legal person for acts that may be committed under the cover of the organisation.
- **Risk treatment:** process aimed at modifying the risk.

## SCOPE

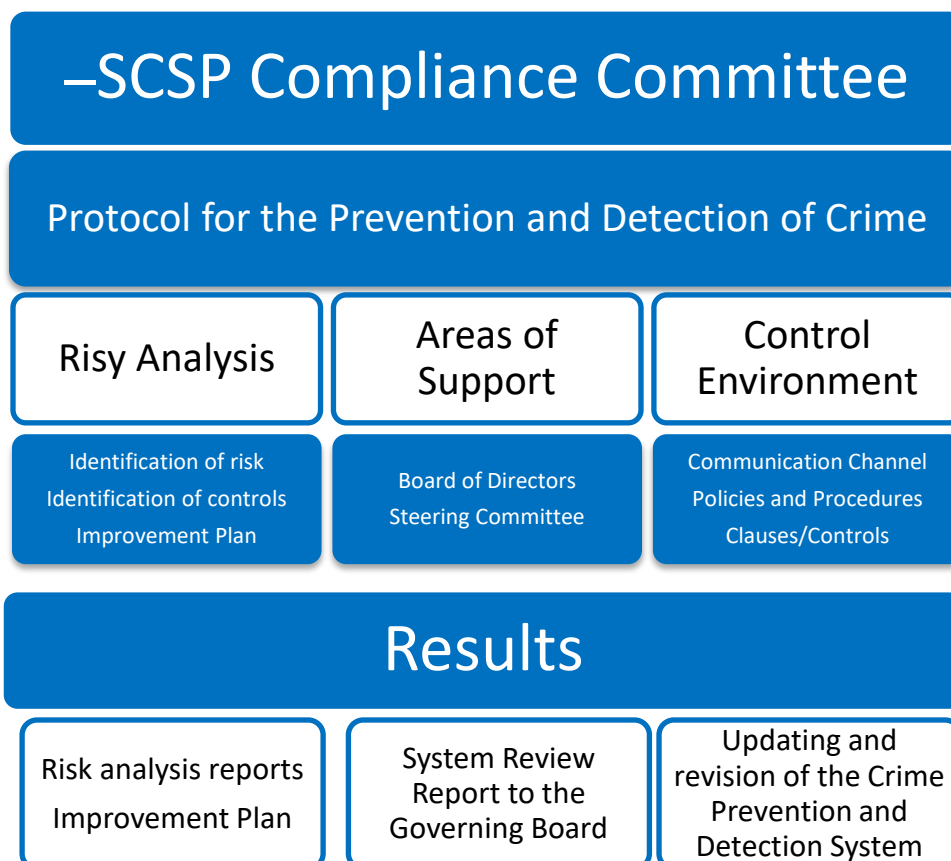
---

The scope of the following protocol includes SCSP professionals, the Board of Directors, management team, employees, subcontractors, consultants and any person who may be affected by the Crime Prevention and Detection System.

SCSP expects all those identified above to behave uprightly, strictly and diligently in compliance with the rules related to crime prevention.

## CRIME PREVENTION AND DETECTION SYSTEM

The Crime Prevention and Detection System established at SCSP is as follows:



## SCSP COMPLIANCE COMMITTEE

The SCSP Compliance Committee shall be appointed by the Board of Directors of SCSP and its appointment shall be recorded in the minutes.

The SCSP Compliance Committee may resign from its post after giving one month's notice to the Board of Directors, stating the reasons why it has decided not to continue in the post.

Likewise, the Board of Directors may agree to change the SCSP Compliance Committee if it is detected that it is not carrying out the tasks entrusted to it in these Regulations.

This change shall be communicated by the Board of Directors to the SCSP Compliance Committee, explaining the reasons for the decision.



The SCSP Compliance Committee, in the performance of its duties, shall be autonomous in the exercise of its duties and shall have the material and human resources necessary to carry out the implementation, development and review of the system.

It shall have access to all areas and the necessary information to carry out or coordinate the execution of the following activities:

1. Carrying out specific investigations,
2. Monitoring the system of crime prevention and detection.
3. Requesting and reviewing information for the execution of its duties,

The SCSP Compliance Committee shall report annually to the Board of Directors on the development of the management system for the prevention and detection of criminal offences, specifically:

- Result of the risk analysis.
- Improvement plans.
- Training plan.
- Complaints made and their outcome.
- Procedures, standards and controls.
- Budget allocation for the year earmarked for these purposes.
- Any other matter that the SCSP Compliance Committee deems appropriate.

To this end, it shall draw up a report reviewing the status of the **Crime Prevention and Detection System** in which all these points shall be considered.

All these aspects shall be included in the Regulations of the **Compliance Committee**.

## CRIME PREVENTION AND DETECTION PROTOCOL

---

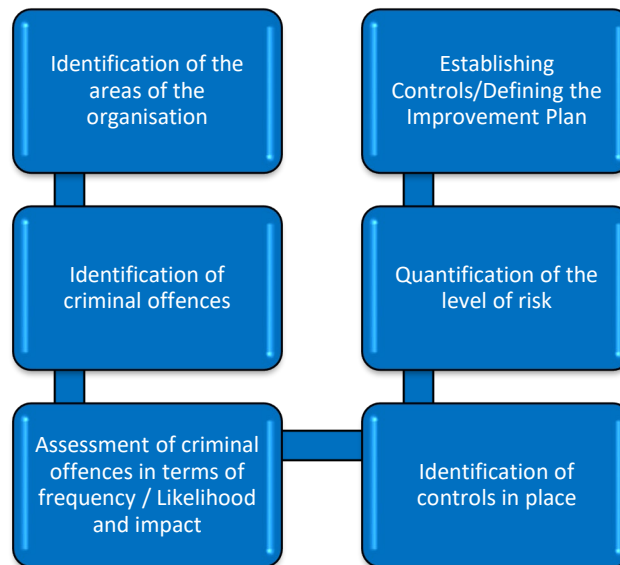
Within the Crime Prevention and Detection System, the components of the SCSP Crime Prevention and Detection Protocol are as follows:

### Risk Analysis

---

The SCSP Compliance Committee shall be responsible for carrying out the risk analysis on an annual basis or when significant changes occur in the organisation. As a result, a list of the levels of risk associated with crimes and unlawful conduct that could potentially occur in SCSP will be obtained.

The risk analysis process is described in the **Risk Analysis Methodology** and is represented graphically as follows:



The level of risk, as well as the results of the assessment, shall be set out in **the Risk Analysis Report**. In addition, the SCSP Compliance Committee shall draw up the **Improvement Plan**, with the planning and controls or actions to be implemented in order to reduce the existing level of risk.

## Support Areas

---

SCSP's Board of Directors and Management, together with the SCSP Compliance Committee, make up the areas supporting SCSP's Crime Prevention and Detection Protocol.

## Control environment

---

The following procedures shall be developed:

- **Crime Prevention and Detection Policy:** Establishes the general principles on which the system is based, this policy must comply with the following requirements:
  - Be appropriate to the scope and activities of the organisation.
  - Include a commitment to respect the general principles of risk management and the Code of Ethics and Conduct.
  - Include the organisation's commitment to establish a culture of compliance.
  - Reflect the commitment to continual improvement of the system.

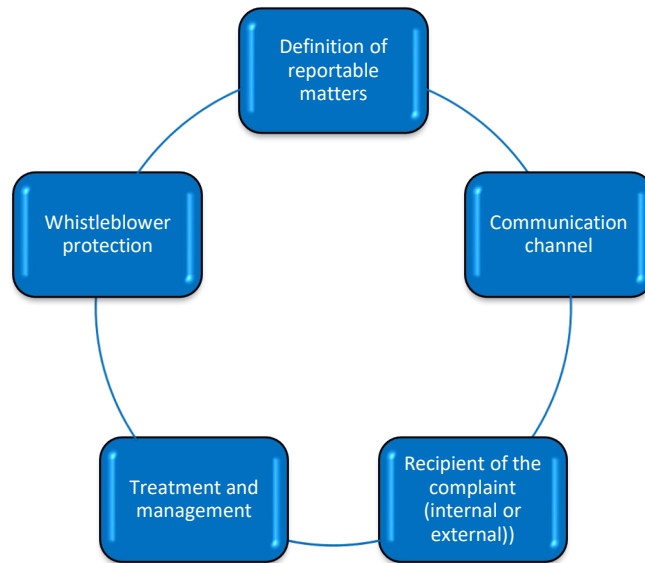
- To communicate and made available to, employees and third parties affected by it.
- **Code of Ethics and Conduct** Establishes a framework of conduct for employees and third parties, requiring adherence to it and respect for it.
- **Communication Channel Procedure:** This is a system implemented in the organisation, through an email address, which is intended to serve as an instrument for the submission of any complaint related to an irregularity or breach of internal policies, irregular conduct or the possible commission of any criminal act covered by the Criminal Code.
- **Clauses/controls:** In relation to the recruitment process of employees, SCSP will include in the contracts obligations regarding the standards set by the organisation in relation to the detection and prevention of crime. It shall also inform such personnel of the content and obligations contained in the Code of Ethics and Conduct, provide information on the role and functions of the SCSP Compliance Committee and the Communication Channel, as well as the procedures and controls established. In the case of suppliers and subcontractors, SCSP shall ensure that they are aligned with the company's ethical values.

## COMMUNICATION CHANNEL

---

SCSP has implemented a Communication Channel available to employees. Its objective is to establish a secure and confidential channel for employees and collaborators to communicate or consult irregular or illegal conduct that they detect in the performance of their duties.

The SCSP **Communication Channel Procedure** describes how the SCSP Communication Channel works. The process to be followed for the establishment of this channel is outlined below.



## TRAINING

---

SCSP shall be responsible for informing all its employees and collaborators of the existence and content of the Crime Prevention and Detection Protocol.

In addition, and in order for this policy to be integrated into the daily work of each member of SCSP, regular training will be given to employees in order to transmit the minimum knowledge needed on this subject and the application of the established procedures.

The training shall include, as a minimum, the following content:

- Definition of the crimes defined as relevant by the organisation according to its risk analysis.
- Policies of the organisation in relation to the Crime Prevention and Detection System.
- Brief description of the content of the Crime Prevention and Detection Protocol.
- Tools and mechanisms used for the implementation of the System and the Code of Ethics and Conduct.
- Warning signs.
- Examples of situations of risk of possible commission of these crimes.
- The SCSP Compliance Committee.



- Procedure for reporting unusual or suspicious transactions.
- Obligation to report.
- Disciplinary and legal consequences (civil, criminal, administrative) of non-compliance with internal and external regulations on criminal matters.
- Responsibility of each employee in this area.

Every SCSP employee shall receive at least one training per year, which may be face-to-face or virtual.

## CRIME PREVENTION AND DETECTION SYSTEM

---

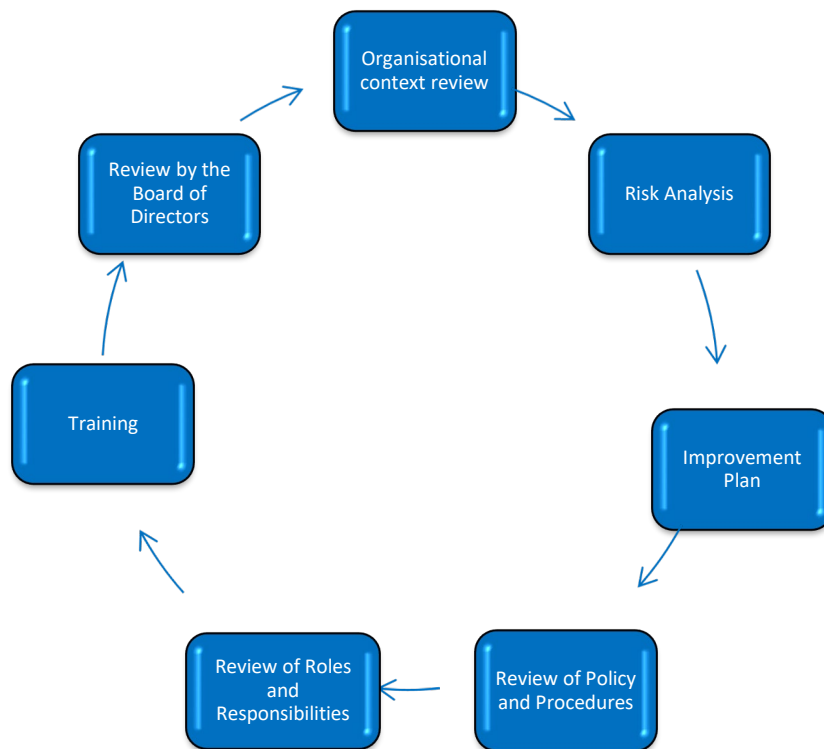
For the maintenance of the SCSP Crime Prevention and Detection System, the following actions are necessary as part of its updating and review:



Activity	Description	Process requirements	Interaction
<b>Review of the organisational context.</b>	<p>The context of the organisation will be reviewed annually to see if any of these aspects have changed:</p> <ul style="list-style-type: none"> <li>▪ Activities of the organisation</li> <li>▪ Functions</li> <li>▪ Services</li> <li>▪ Products</li> <li>▪ Employees</li> <li>▪ Suppliers</li> <li>▪ Existence of new rules or policies to which they must relate to.</li> </ul>		Risk Analysis
<b>Risk Analysis</b>	A risk analysis of the Organisation shall be carried out annually.	Context of the Organisation Participation of the Organisation's areas. Risk Analysis Methodology.	Improvement Plan
<b>Improvement Plan</b>	Once the risk analysis has been carried out by the organisation, appropriate measures (controls) shall be taken to reduce the level of risks.	Risk Analysis	Crime Prevention and Detection Policy Procedures.
<b>Review of the Crime Prevention and Detection Policy.</b>	The policy will be reviewed annually to adapt it to new requirements as they arise.	Organisational Context Legal requirements	Status review report on the Crime Prevention and Detection System.
<b>Review of the roles, responsibilities and authorities of those involved.</b>	Defined roles, responsibilities and authorities shall be reviewed annually to verify that those involved are up to date in relation to Crime Prevention and Detection activities.		Compliance Committee Procedures Risk Analysis Improvement Plan Annual Training Plan
<b>Review of procedures</b>	The procedures set out in the system shall be reviewed at least annually and updated according to the organisational context and risk analysis.	Organisational Context Risk Analysis	Review report on the status of the Crime Prevention and Detection Management System.
<b>Competence, Training and Awareness.</b>	Annually, the actions carried out must be established and reviewed so that those involved in the system are trained, know their functions and have the appropriate training to carry them out.	Review of roles, responsibilities and authorities.	Annual Training Plan

Activity	Description	Process requirements	Interaction
<b>Review by the Board of Directors.</b>	The review of the roles, responsibilities and authorities of the people involved in the Crime Prevention and Detection System is taken as an input.	Policy Risk Analysis Improvement Plan	

The system is represented graphically as follows:



## DETECTION AND RESPONSE PROTOCOL

### 1. Introduction

The criminal compliance dimension of the organisation should not only focus on crime prevention, but also on other aspects such as detection and response, especially since experience has shown that absolute crime prevention is impossible, and a criminal risk management model limited to crime prevention may not be sufficient.

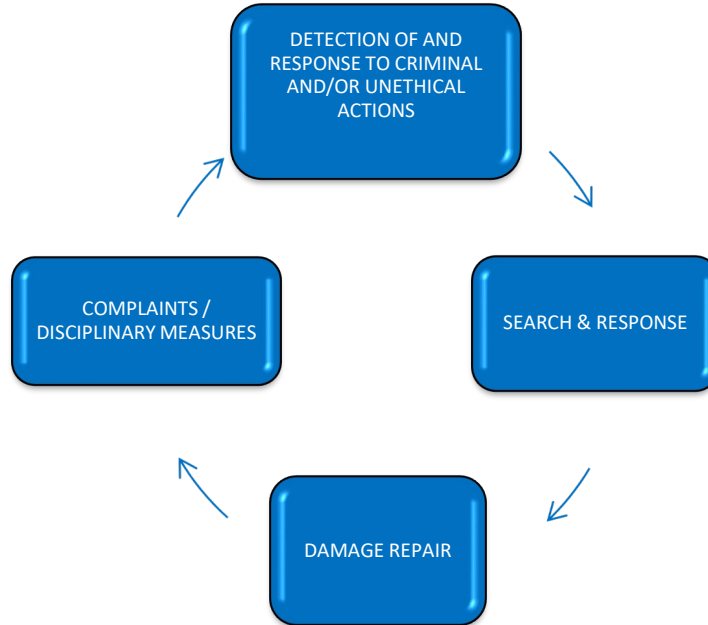
### 2. Object

Within the framework of the programme developed at SCSP for the Prevention and Detection of criminal acts and/or acts contrary to the Ethical Framework, and in order to attenuate and mitigate the possible sanction or penalty imposed by the legal system in relation to the commission of a criminal act and/or act contrary to the Ethical Framework, the following protocol for post-criminal actions has been defined within the organisation.

In order to guarantee the correct functioning and compliance with the SCSP's Organisation and Management Model for the Prevention and Detection of Crimes, a Detection and Response preventative protocol has been designed, completed and implemented, so that SCSP has an organised system for reacting when information is reported regarding the commission of

criminal actions and/or contrary to the Ethical Framework, linked to the activities of the organisation.

The Protocol for Detection and Response to criminal actions and/or actions contrary to the



ethical framework established in SCSP is as follows:

Its purpose is to specify the operations to be followed in SCSP when the alleged commission of a criminal act and/or an act contrary to the Ethical Framework is detected, for which the legal person can respond, prevent and mitigate the potential risks, as well as the possible sanctions or penalties that the criminal code provides for in Article 33.7 of the Criminal Code.

The possible penalties or sanctions that may be imposed on the legal person may be mitigated, according to Articles 21.4 and 5 and 31c (a), (b) and (c), in the following ways:

- Repairing the Damage.
- Detection of Delinquent Conduct and/or Conduct Contrary to the Ethical Framework.
- Whistleblowing / Disciplinary Measures.
- -Collaboration in the Investigation and Response.

### 3. Detection of Criminal Conduct and/or Conduct Contrary to the Ethical Framework.

---

SCSP becomes aware of allegedly criminal acts and/or acts contrary to the Ethical Framework through the following channels:

- As a result of the procedures of its internal control mechanisms: Communication Channel, Internal Audits, or interviews and work climate surveys, etc....
- By means of informal external communication: complaints through the Communication Channel or by other means, news appearing in the written or digital media.
- Notification of the existence of an investigation by the Public Prosecutor's Office, or the initiation of criminal proceedings, as well as the announcement by a third party of their intention to file a complaint against the organisation.

Whatever the route through which knowledge is acquired, the organisation has protocols on how to manage the information received, and what reaction decisions to take. These protocols differ depending on the information source.

## 4. Investigation and Response

---

In the event of suspicion or evidence that an irregularity or crime is being committed, SCSP has created a Communication Channel that functions as a mechanism for detecting irregularities or crimes in an agile, guaranteed and effective manner. A means that allows us to draw up the most appropriate strategy for the organisation in the event of an alleged commission of a criminal act and/or contrary to the Ethical Framework.

### 4.1 Protocol for pre-trial proceedings

---

SCSP has established an internal corporate investigation system for the clarification of an alleged criminal act and/or an act contrary to the Ethical Framework.

Upon learning of the commission of an alleged criminal act and/or an act contrary to the Ethical Framework within the organisation, the SCSP Compliance Committee shall initiate an internal corporate investigation procedure in order to:

- Compile all available preliminary information in a dossier.
- Initially assess the degree of veracity of the information provided by the internal or external (informal) source.
- Likewise, the SCSP Compliance Committee may directly agree or urge the competent areas to adopt the necessary precautionary or preventive measures to guarantee its actions and the correct progress of the internal investigation, in order to avoid any negative consequences for the organisation and to protect its professionals and directors.
- In order to guarantee that the resolution of a presumed criminal act and/or an act contrary to the Ethical Framework has the maximum guarantees, SCSP, when it so

considers, will call on external advice that provides greater consistency and legal security to the results, derived from its greater specialisation, allowing it to have an objective and impartial vision complementary to the internal corporate investigation.

- Once the corporate investigation has been completed, a report shall be submitted to the Board of Directors of SCSP containing the conclusions thereof, with reasoned proposals for action. This report shall contain, in all cases, a list of the actions taken to clarify the facts, as well as the conclusions reached, which shall be duly supported by documentation of the evidence obtained.
- Depending on the outcome of the investigation, the SCSP Compliance Committee may urge the competent areas to adopt the decisions they deem appropriate (e.g. inform HR in the event that there are grounds for disciplinary dismissal or any other employment sanction, provide evidence of the offence to the competent authorities, etc.), with the prior agreement of the Board of Directors of SCSP, as the case may be.
- A record should be kept of all proceedings initiated, incorporating the relevant documentation for each case.

#### 4.2 Collaboration in the investigation

---

Likewise, in parallel, SCSP will collaborate as much as possible with the Judicial and Police Authorities, Supervisory Bodies and the Public Administration in any investigation that they initiate, providing them with the results of the internal investigation and without hindering the investigation with the aim of mitigating the possible penalty or sanction that the alleged criminal act and/or contrary to the Ethical Framework may entail.

#### 4.3 Legal procedures protocol

---

The protocol for legal procedures must be activated when criminal proceedings or an investigation by the Public Prosecutor's Office are brought directly against the organisation.

The SCSP Compliance Committee, under the guidelines and supervision of the SC Europe & CIS Group's Legal Department, shall be responsible for managing the basic lines of the procedural strategy, as well as any other corporate strategy to react to the initiation of criminal proceedings against the organisation (e.g. internal and/or external communication actions).

In order to carry out these actions, the Compliance Committee shall initiate an internal investigation procedure and shall also prepare a criminal legal assessment, which may be assisted by an external advisor, establishing the defence strategy to be followed by the organisation.

#### 4.4 Appointment of the legal procedural representative

---

If SCSP is charged with criminal liability, it must appoint a representative to appear in court.

In accordance with Law 37/2011, of 10 October, on procedural streamlining measures, by which the Criminal Procedure Act was amended, the main procedural action in cases of criminal charges against the legal entity is regulated as follows:

The summons shall be served at the registered office of the legal entity, requiring the organisation to appoint a representative, as well as a lawyer and a solicitor for the legal proceedings, all for the best interests of SCSP.

In view of the above, the person designated as procedural representative in the event of a hypothetical criminal charge against the organisation, must have the following characteristics:

- have sound technical knowledge of the matter to be judged, as well as of the Organisational and Management Model for Crime Prevention and, in general, of the SCSP's legal compliance policies (this Compliance Manual).
- be a person with a high hierarchical position within the organisation.
- Avoid persons who may have procedural conflicts of interest with SCSP, either because they are already charged or because they are presumably going to be charged.

### 5. Damage repair

---

One of the post-criminal actions that SCSP has established is the REPAIR OF DAMAGE. If a criminal act and/or an act contrary to the Ethical Framework is committed within the organisation, resulting in any damage, SCSP will take responsibility for its reparation, provided that the Surveillance and Control measures implemented have not functioned correctly, for which reason it could be declared criminally and/or civilly liable.

If SCSP is criminally and civilly liable for the commission of a criminal offence, it will proceed to repair the damages caused and, if it is not possible to repair them, to compensate them.

In the event of the possibility of suffering financial penalties, SCSP, in advance and duly advised, may choose to pay or guarantee the required amount in order to avoid the imposition of future surcharges.



## 6. Complaint/Disciplinary Measures

---

If a criminal act is allegedly committed by a member of the organisation, SCSP, through the SCSP Compliance Committee, shall carry out an internal investigation of the facts. If such internal investigation determines that there are enough indications and evidence to believe or sustain that the alleged criminal act has been committed, depending on its seriousness, SCSP shall proceed to report it to the appropriate Judicial Authorities, Police, Supervisory Bodies or Public Administration.

SCSP may adopt the appropriate disciplinary measures against those employees who fail to comply with the internal protocols and the measures established in the Prevention and Detection System for criminal acts and/or acts contrary to the Ethical Framework.



SUMITOMO CORPORATION ESPAÑA, S.A.

# COMMUNICATION CHANNEL PROCEDURE

Crime Prevention and Detection System

## COMMUNICATION CHANNEL PROCEDURE

---

### INTRODUCTION

---

SCSP adheres to the highest standards of transparency, honesty and accountability. One way in which this commitment is materialised is by making it possible for employees, or others working for SCSP who have concerns about any of the organisation's activities and/or specific actions, to effectively raise their concerns.

Generally, employees are the first to become aware of wrongdoing within the company they work for. However, they may choose not to voice their concerns, believing that to do so, would constitute a lack of loyalty, both to their colleagues and to the organisation itself. They are also likely to fear reprisals. In these circumstances, they may feel that it is easier to ignore the conduct they consider irregular than to report what may only be a suspicion of an illicit action.

Through this procedure, we intend to explain to employees or other people working for SCSP that they can and should report illegal activity without fear of persecution, discrimination or other retaliation.

The purpose of this Communication Channel is to raise awareness among employees so that if they are certain or have a well-founded suspicion that unlawful conduct is being committed within the organisation, related to the criminal actions listed in this document, they should confidentially report such information so that it can be investigated.

This Communication Channel reaffirms the commitment acquired by SCSP that any illicit activity on the part of the organisation, any of its employees, collaborators or subcontractors, will be dealt with confidentially and will be rigorously investigated, adopting the appropriate measures in accordance with internal and external regulations.

This procedure in turn implies a commitment by all employees or persons working for SCSP to act responsibly in order to maintain the good reputation of the organisation and to act honestly in the event of a possible infringement that could harm the organisation.

### WHAT DOES THE COMMUNICATION CHANNEL CONSIST OF?

---

The purpose of this procedure is to regulate a specific channel through which all SCSP employees can fulfil their duty to report or denounce to the SCSP Compliance Committee any irregular or illegal acts of which they may become aware, without fear of suffering reprisals of any kind. SCSP guarantees the security and confidentiality of whistleblowers by establishing the necessary measures. Likewise, SCSP will guarantee the rights of the reported party, principally their presumption of innocence.

The duty to inform or communicate, on the part of all SCSP professionals, constitutes one of the essential elements of the Crime Prevention and Detection System, as it implies reporting non-compliance with the rules and controls imposed by the Code of Ethics and Conduct and the Policies developed by SCSP, by those who have direct knowledge of the actions carried out within it and therefore the obligation to follow the guidelines for action established in this Procedure.

## WHAT IS AN ILLEGAL ACTIVITY?

Any illicit and/or illegal behaviour that falls under any of the types established in Spanish Criminal Code and which entails the criminal liability of the Organisation within which and for whose benefit it has been carried out.

Spanish Criminal Code contemplates a catalogue of crimes in which the Organisation can be charged together with those who have intervened, although only some of them are likely to be committed, as the rest, either due to the activity of the organisation itself or because they correspond to crimes usually committed by organised criminal networks, have not been considered probable.

The list of criminal offences is as follows:

Criminal Type	Articles Penal Code
Illegal Organ Trafficking	156 bis
Trafficking in human beings	177
Offences relating to prostitution, sexual exploitation and corruption of minors	187 - 189
Offences of discovery and disclosure of secrets	197
Scams and frauds	248 y 251
Implementation frustration	257 y 258 bis
Punishable insolvencies	259 - 261
Computer damage	264
Intellectual and industrial property, market and consumer crime	270 – 286
Corruption in business	286 bis – ter
Money laundering	301
Illegal financing of political parties	304 bis
Crimes against the Treasury and Social Security	305 – 308



Criminal Type	Articles Penal Code
Accounting crime	310
Illegal trafficking and illegal immigration offences	318 bis
Offences against town and country planning and urban planning	319
Environmental crime	325 – 327
Crimes relating to nuclear energy and ionising radiation	343
Risk crimes caused by explosives and other agents	348
Crimes against public health and drug trafficking	359 - 369
Counterfeiting currency and means of payment	386 y 399 bis
Bribery	419 – 427
Influence peddling	428 – 430
Crimes relating to fundamental rights and public freedoms	510
Terrorist financing	576

The following criminal offences will also be reviewed:

Criminal Type	Articles Penal Code
Price-fixing crimes in public tenders and auctions	262
Corporate crimes (impeding supervisory activity)	294
Crimes against workers' rights	318

Among the types of crimes most likely to be committed within SCSP's scope of action are the following:

**1. Crimes of discovery and disclosure of secrets:**

- Unauthorised access by any means or procedure, in violation of the security measures established to prevent it, to data or software contained in a computer system or part of it or maintained within it against the will of whoever has the legitimate right to exclude it.

**2. Scams and frauds:**

- Using deception for financial gain to induce someone to carry out an act of disposition, by using computerised means, credit cards, traveller's cheques or the data contained therein.

**3. Punishable insolvencies:**

- Admitted the application for bankruptcy and without the authorisation of the court or the CA, performs the acts described above in favour of one creditor to the detriment of others or knowingly submits false information concerning the accounting statement with a view to improperly obtaining a declaration of bankruptcy.

**4. Computer damage:**

- Recording, deleting, damaging, deteriorating, altering, suppressing, or rendering inaccessible data, computer programmes or electronic documents of others without authorisation and when the result produced would be serious.

**5. Intellectual property:**

- With the intention of obtaining a direct or indirect economic benefit and to the detriment of a third party, reproducing, plagiarising, distributing or publicly communicating, in whole or in part, a literary, artistic or scientific work, or its transformation, interpretation or artistic performance fixed on any type of support or communicated by any means, without the authorisation of the holders of the corresponding intellectual property rights or their assignees.
- Offences relating to the market and consumers: discovering a company secret by taking possession of data, documents and computer media, as well as the dissemination or disclosure of a company secret.
- Misleading advertising likely to cause serious damage.
- Altering freely competitive prices by means of violence, threat or deception.

**6. Corruption in business:**

- Promising, offering or giving to managers, directors, employees or collaborators of a commercial enterprise or company, by himself or through an intermediary, an unjustified benefit or advantage, of any nature whatsoever, for himself or for a third party, as counterpart to unduly favour him or a third party over others in the acquisition or sale of goods, contracting of services or in commercial relations.
- Receiving, soliciting or accepting an unjustified benefit or advantage of any nature whatsoever, for oneself or for a third party, as counterpart for unduly favouring another in the acquisition or sale of goods, or in the procurement of services or in business relationships.



- Offering, promising or giving any undue pecuniary or other improper advantage or benefit, corrupting or attempting to corrupt, whether by himself or through an intermediary, a public authority or public official for their benefit or for the benefit of a third party, or complying with their requests to act or refrain from acting in connection with the exercise of public functions in order to obtain or retain a contract, business or any other competitive advantage in the conduct of international business activities

#### **7. Money Laundering:**

- Acquiring, possessing or using property, knowing, at the time of receipt of the property, that it is derived from criminal activity or from participation in criminal activity.

#### **8. Crimes against the Treasury and Social Security:**

- Committing fraud against the State, regional, provincial or local Treasury, avoiding the payment of taxes, amounts withheld or that should have been withheld or payments on account, unduly obtaining refunds or enjoying tax benefits in the same way whose amount exceeds 120,000 euros or 50,000 euros in a calendar year in the case of committing fraud against the Treasury of the European Union.
- Committing fraud against the Social Security by evading the payment of Social Security contributions and joint collection concepts, unduly obtaining refunds of the same or unduly enjoying deductions for any concept whose amount exceeds 50,000 euros.
- Obtaining, for oneself or for another, benefits from the Social Security System, the undue prolongation of the same, or facilitating others to obtain the same, by means of error caused by simulation or misrepresentation of facts, or the conscious concealment of facts of which it was their duty to inform, thereby causing damage to the Public Administration.

#### **9. Accounting crimes:**

- Failure to record in the obligatory books business, acts, operations or, in general, economic transactions, or having recorded them with figures other than the true ones, omitting tax declarations or that those presented were a reflection of his false accounting and that the amount of the charges or credits omitted or falsified exceeds 240,000 euros for each financial year.
- Making fictitious accounting entries in the compulsory books, omitting tax declarations or making tax declarations that reflect false accounting and that the amount of the omitted or falsified debits or credits exceeds 240,000 euros for each financial year.

#### **10. Environmental crime:**

- Contravene laws or other general provisions protecting the environment by directly or indirectly causing or carrying out emissions, discharges, radiations, extractions or

excavations, landfalls, noise, vibrations, injections or deposits into the atmosphere, soil, subsoil or land, underground or sea waters, including the high seas, including transboundary areas, as well as the abstraction of water which, by themselves or jointly with others, cause, by themselves or jointly with others, the pollution of the environment, subsoil or water on land, underground or sea, including the high seas, including in transboundary areas, as well as the abstraction of water which, alone or jointly with others, causes or is likely to cause substantial damage to the quality of air, soil or water, or to animals or plants.

#### 11. Bribery:

- Receiving or requesting by an authority or public official, for one's own benefit or that of a third party, by oneself or through an intermediary, a gift, favour or retribution of any kind, or accepting an offer or promise to carry out an act in the exercise of one's office that is contrary to the duties inherent to the same, or to not carry out or to delay unjustifiably an act that should be carried out. Likewise, not to carry out an act proper to his office or to accept it in consideration of his office.
- Offering or giving a gift or retribution of any kind to an authority or public official to carry out an act contrary to the duties proper to their office or an act proper to their office, to avoid carrying out or delaying an act that should be carried out, or in consideration of their office and function. Likewise, if the surrender takes place at the request of the authority or official, including in both cases officials of the EU or of another Member State.

#### 12. Influence peddling:

- A private individual who influences a public official or authority by abusing his personal relationship with that official or another to obtain a decision that may directly or indirectly generate an economic benefit for himself or for a third party.

#### 13. Crimes against employee's rights:

- Preventing or limiting the exercise of trade union freedom or the right to strike.
- In breach of health and safety regulations and being legally obliged to do so, failing to provide the necessary means for employees to carry out their activity with the appropriate health and safety measures, in such a way as to seriously endanger their life, health or physical integrity.

**It should be remembered that the profit, benefit or advantage obtained from the commission of the crime must be for SCSP itself and not in the personal capacity of the employee who commits the offence, as in this case it will be the individual who will be liable for the act committed.**

On the other hand, the types of offences ruled out due to their low or zero probability of being committed within the scope of SCSP's activities are the following:

- Illegal organ trafficking
- Trafficking in human beings

- Crimes relating to prostitution, sexual exploitation and corruption of minors.
- Illegal financing of political parties
- Illegal trafficking and illegal immigration
- Crimes against town and country planning and urban planning
- Crimes relating to nuclear energy and ionising radiation.
- Counterfeiting currency and means of payment
- Crimes relating to fundamental rights and public freedoms
- Financing of terrorism
- Alteration of prices in public tenders and auctions

## WHO SHOULD REPORT AND HOW THEY ARE PROTECTED?

---

Any professional or person working for SCSP has a duty to report the existence of unlawful and/or irregular conduct, being protected, provided that:

1. Make the complaint in good faith;
2. Believe it to be substantially true;
3. Do not act in bad faith or make false accusations; and
4. Do not be motivated by revenge and/or seek personal gain.

All SCSP professionals who become aware of any breach of the rules and controls contained in the Code of Ethics and Conduct, especially if they constitute unlawful or criminal acts, are obliged to report it to the SCSP Compliance Committee as soon as possible.

The obligation to inform or communicate refers only to breaches committed by persons with any type of contractual relationship with SCSP (whether employment, civil or commercial) and which have any effective consequence on the maintenance or development of said contractual relationship.

Failure to comply with the obligation to report or inform the SCSP Compliance Committee of the commission of irregular or unlawful conduct of which there is certainty or well-founded suspicion, as well as the communication of a false or unfounded report, shall be considered very serious infringements.





## WHO SHOULD I CONTACT?

---

Any person who has a concern about a specific action should contact:

- 1- SCSP Compliance Committee (compliance.scsp@sumitomocorp.com);
- 2- SCEU Compliance Committee (sceu-er@sumitomocorp.com); and/or
- 3- External Reporting Line (by e-mail to [sumitomo@sumitomosafecall.co.uk](mailto:sumitomo@sumitomosafecall.co.uk), by visit the website [www.safecall.co.uk/reports](http://www.safecall.co.uk/reports) or by telephone on 0800 72 33 22 55)

providing a summary and specific description of the action in question, the person or persons involved and the documents or information supporting the complaint.

Complaints (communications) addressed to the Compliance Committee must comply with a series of formalities and must contain the following information as established in the Complaint Form (Annex I):

- Identity of the Complainant (optional).
- Description of the facts that are the subject of the complaint.
- Indications on which the complainant's suspicions are based.
- Identity of the person complained of, if known, who is responsible for the act that is the subject of the complaint.

Complaints must be accompanied by all evidence such as documents available to the complainant.

## HOW WILL THE ORGANISATION RESPOND?

---

The Compliance Committee shall (i) receive the communication directly or through the External Reporting Line, (ii) respond to the whistleblower and (iii) request, where appropriate, any clarifications it deems necessary, and (iv) initiate a process of verification and investigation of the facts.

The SCSP Compliance Committee shall not provide the identity of the whistleblower to the person(s) reported or to any other employee, with the exception of employees or external professionals involved in the investigation of the facts, who shall in any event have a duty of confidentiality. Likewise, it may not initially inform the person/s involved, if this would benefit the verification of the facts and, in any case, it shall keep the identity of the complainant confidential when informing of the existence of the complaint and the facts to those concerned.

If it is necessary, due to the seriousness of the conduct, to act immediately, the relevant authorities shall be notified, subject to prior authorisation by the Board of Directors of SCSP.



Within ten (10) working days following receipt of the complaint, the SCSP Compliance Committee shall send a confidential communication to the complainant in order to:

- Acknowledge receipt of the complaint;
- Indicate how it proposes to deal with the matter;
- State whether any further enquiries have been made; and
- Confirm whether further investigations will be carried out and, if not, the reasons for not doing so.

The nature of the issue raised, the specific nature of the information and documentation provided shall determine the period of enquiry and response.

If no non-compliance is found, the SCSP Compliance Committee shall close the complaint, recording this in a report in which it justifies and substantiates the reasons for the closure.

If there are indications of non-compliance, the complaint shall be admitted for processing and an internal investigation shall be initiated to ascertain whether the facts reported are true. The internal investigation conducted by the SCSP Compliance Committee, as well as the imposition of precautionary measures, where appropriate, shall be carried out in accordance with the provisions of the protocol for detection and response.

The organisation will take the necessary measures to maintain confidentiality and prevent the whistleblower from suffering any kind of reprisal, sanction or negative consequence for the mere fact of having made a complaint. Any attempt at retaliation or breach of confidentiality will be considered a very serious offence and will be subject to disciplinary action.

Unless prevented by police or judicial decisions, the whistleblower shall be informed of the outcome of the investigations carried out.

### **Data Protection**

The personal data obtained on the occasion of the complaint and the internal investigation shall be processed solely for the management and control of this Communication Channel Procedure.

The reports made shall be recorded in a file that shall be registered in the General Data Protection Register and the holders of the Personal Data may exercise their rights of access, rectification, cancellation and opposition by sending an e-mail to the SCSP Compliance Committee ([compliance.scsp@sumitomocorp.com](mailto:compliance.scsp@sumitomocorp.com)).

However, such rights may not be exercised in the following cases:

- The exercise of the right of access by the reported person does not include the disclosure of the reporting person's identification data.

- The exercise of the right of access by the respondent does not include the disclosure of the complainant's identification data.
- Where these rights are exercised on the basis of a complaint related to the prevention of money laundering and terrorist financing, the provisions of Article 32 of Law 10/2010 of 28 April 2010 on the prevention of money laundering and terrorist financing shall apply.

The data contained in the Communication Channel system shall be treated with due confidentiality, respecting data protection regulations, and shall be deleted within two (2) months after the complaint has been filed or when the legal proceedings arising from the complaint are concluded, as the case may be. Personal data may only be kept in separate custody during the period of limitation of the liabilities related to the complaint, to be made available to the authorities, where appropriate.

## FALSE OR UNFOUNDED ACCUSATIONS

---

The Organisation, aware of its commitment to the Crime Prevention Policy, will invest the necessary personal and financial resources to implement and maintain the effectiveness of the Communication Channel, undertaking to investigate any complaint received.

Likewise, it will consider any false or malicious accusation made in a deliberate manner as a very serious offence, which may be sanctioned in accordance with the provisions of the Code of Ethics and Conduct, by application of employment and/or criminal law.

It should be emphasised, firstly, that we could be dealing with a crime of false accusation or complaint (art.456), or a crime of calumny (art.205) contemplated in the Penal Code.

Indeed, the **Penal Code**, in its article 456. 1, concerning the crime of **false accusation or complaint**, establishes that the person who, with knowledge of its falsehood or reckless disregard for the truth, accuses another person of facts which, if true, would constitute a criminal offence, if this accusation is made before a judicial or administrative official who has the duty to proceed with its investigation, **shall be punished with a prison sentence of six months to two years and a fine of twelve to twenty-four months, if a serious offence is accused; a fine of twelve to twenty-four months, if a less serious offence is charged; and a fine of three to six months, if a criminal offence were to be charged.**

On the other hand, the crime of **calumny** contemplated in Article 205 of the Penal Code establishes that "calumny is the imputation of a crime made with knowledge of its falsity or reckless disregard for the truth" **and can be punished with a prison sentence of six months to two years or a fine of twelve to 24 months, if it is spread with publicity, and, otherwise, with a fine of six to 12 months.**



Secondly, with regard to labour regulations, Article 58 of the **Labour Regulation** establishes that "employees may be sanctioned by the management of companies for employment breaches, in accordance with the grading of the offences and sanctions established in the legal provisions or in the applicable collective agreement".

In the case of SCSP, the applicable collective **negotiating agreement for offices** of each work centre, which in its articles establishes the sanctioning regime and the applicable procedure.

## COMMUNICATION CHANNEL COMPLAINT FORM

---

### Reporting of criminal conduct or conduct contrary to the Code of Ethics

---

The purpose of the Communication Channel is to detect illicit or irregular conduct within the Organisation, in relation to the provisions of the SCSP Code of Ethics and Conduct.

It must be used exclusively to report allegations and/or irregularities related, among others, to the following matters:

- Non-compliance with laws, regulations, rules and procedures.
- Any unlawful act against our key stakeholders.
- Unethical or dishonest conduct and/or Conflicts of Interest.
- Any other alleged breach of the regulatory and ethical principles set out in SCSP's Code of Ethics and Conduct.

The communications or complaints must always be formulated under criteria of truthfulness, clarity and in a complete and detailed manner, and must not be untruthful or malicious, as the charge of facts with knowledge of their falsity or with reckless disregard for the truth, could result in criminal, labour or civil liabilities for the complainant.

The personal data you provide will be incorporated into a file under the responsibility of SCSP CORPORATION ESPAÑA, S.A., with tax identification number: A28806115- , with registered address for these purposes at Calle Infanta Mercedes, 90, 7ª Plta, CP 28020, Madrid, Spain, for the purpose of managing your notification, investigating the reported facts, adopting the pertinent corrective measures, and if necessary, informing you of the outcome of the procedure.

Your data will be treated confidentially and will not be communicated to any third party, unless it is essential for the investigation of the reported facts.

In any case, you may exercise your rights of access, rectification, cancellation and opposition by post to the address indicated, providing a copy of your ID card or equivalent document, and identifying yourself as a user of the Communication Channel.

SUMITOMO CORPORATION ESPAÑA, S.A.

# RULES OF PROCEDURE OF THE SCSP COMPLIANCE COMMITTEE

Crime Prevention and Detection System

## **RULES OF PROCEDURE OF THE SCSP COMPLIANCE COMMITTEE**

---

### **OBJECT**

---

Within the framework of the Crime Prevention and Detection programme developed in SCSP, the figure of the "compliance committee" has been created.

The objective is to centralise the roles in this area to a single responsible person who reports to the Board of Directors periodically and who evaluates the effectiveness of the Crime Prevention and Detection System, as well as the procedures and controls implemented for this purpose, proposing the corrective measures considered appropriate.

The Organisation shall provide the SCSP Compliance Committee with enough resources and sufficient material means, as well as access to internal procedures, documentation and any other ordinary information. Access to any extraordinary or reserved information shall require prior authorisation from the Board of Directors of SCSP.

## PROFILE OF THE COMPLIANCE COMMITTEE

---

The profile of the persons appointed within SCSP as members of the SCSP Compliance Committee shall meet the following requirements:

- Occupy a position of responsibility within SCSP.
- A professional with in-depth knowledge of SCSP's operational functioning, as well as its administrative and business areas.

The members of the SCSP Compliance Committee shall be appointed by the Management of SCSP and their appointment shall be recorded in the minutes.

Any member of the SCSP Compliance Committee may resign from his or her post after giving one month's notice to the Board of Directors, stating the reasons for his or her decision not to continue in the post.

Likewise, the Board of Directors may agree to change any member of the SCSP Compliance Committee if it is detected that he or she is not performing the tasks entrusted to him or her under these Regulations. This change shall be communicated to the SCSP Compliance Committee, explaining the reasons for the decision.

In the performance of its functions, the SCSP Compliance Committee shall have total autonomy with respect to the Board of Directors of SCSP and shall have the material and personal resources to implement, develop and review the system.

It shall have access to all the areas and information necessary to carry out or coordinate the execution of the following activities:

1. Carrying out specific investigations,
2. Monitoring the crime prevention and detection system,
3. Requesting and reviewing information for the execution of its functions

The SCSP Compliance Committee shall report annually to the Board of Directors on the progress of the System for the Prevention and Detection of Crimes, specifically on:

- Results of the risk analysis.
- Improvement plan.
- Training Plan.
- Complaints made and their outcome.
- Procedures, controls and rules.
- Any other matter that you consider appropriate.

To this end, it will draw up a report reviewing the state of the crime prevention and detection system in which all those points will be considered.

## PURPOSES AND COMPETENCES

---

The purposes and powers of the SCSP Compliance Committee shall be as follows:

- To ensure compliance with the internal regulations relating to the Prevention and Detection of Crimes and to advise the organisation's governing bodies on this matter in order to guarantee quality standards.
- To circulate among the members of the organisation the internal regulations relating to the Prevention and Detection of Crimes and, specifically, to publish the SCSP Code of Ethics and Conduct.
- He/she shall be responsible for carrying out the risk analysis annually or when major changes occur in the organisation, as well as, minimising the risks detected by implementing the relevant procedures and controls.
- The risk analysis and the controls and procedures developed shall affect the different areas of the Organisation, identifying the potential threats in each of them. This analysis will include the probability and degree of impact in relation to the different types of conduct listed in the criminal offences that could be attributed to the organisation depending on its sphere of action.
- It shall analyse the effectiveness of the procedures and controls put in place in the organisation and draw up proposals for improvement if necessary.
- In terms of crime prevention, it will propose the drafting of rules, regulations, codes and other documentation for internal use, establishing the controls that avoid or minimise the threats and risk of the scenarios detected.



- It will deal with the queries and/or complaints that are communicated through the "Communication Channel", the corresponding response and/or the investigation and reasoned proposal for resolution. If the complaint is addressed to the SCSP Compliance Committee itself, the complainant must send the communication to the Board of Directors of SCSP. Similarly, if the complainant is the SCSP Compliance Committee itself, the investigation shall be carried out by a member of the Board of Directors.

## COMMUNICATION CHANNEL

---

Through this channel, the Compliance Committee may receive notifications regarding alleged breaches or uncertainties about the operation of the protocol for the prevention and detection of crimes, or about conduct in relation to which there are reasonable doubts that its implementation involves a breach of the Code of Ethics and Conduct.

These communications shall be treated by the Compliance Committee with the utmost confidentiality and respecting at all times the privacy and the presumption of innocence of the person(s) reported.

The SCSP Compliance Committee shall respond to the whistleblower within a period of no more than ten working days, confirming receipt of the communication and, if it deems it necessary, may request clarifications or information to expand on the material provided by the whistleblower. Likewise, the SCSP Compliance Committee shall inform the complainant of the reasons if it decides not to proceed with the investigation.

Once the SCSP Compliance Committee has obtained a clear and objective view of the facts, it shall report its findings to the governing body; that is to the Board of Directors and the person(s) reported, independently of the possible communication to the police or judicial authorities and upon the seriousness of the known conduct.



SUMITOMO CORPORATION ESPAÑA, S.A.

# TRAINING

Crime Prevention and Detection System

## TRAINING

---

## OBJECT

---



The objective of the Training established by SCSP to its professionals, is to raise awareness of its Crime Prevention and Detection System, providing theoretical and practical knowledge in relation to possible crimes that could eventually be committed in the development of SCSP's activities, as well as the procedures, policies, internal rules, specifically the Code of Ethics and Conduct, and the controls established to prevent and where appropriate, detect the commission of unlawful conduct/s or contrary to the ethical framework.

Training is a key element in SCSP's Crime Prevention and Detection System. It is an essential element to facilitate:

- Prior knowledge of the job performance of new recruits.
- The adaptation of human resources to regulatory and operational changes.
- The creation and consolidation of a true "Compliance Culture" in the organisation.

At SCSP we want all professionals to be fully aware of the possible criminal risks involved in the development of their work in order to recognise these risks and prevent their occurrence.

## TRAINING SCOPE

---

Training will be given to employees as well as to managers and administrators, reaching to all professionals at SCSP.

## TYPES OF TRAINING

---

SCSP, on the basis of its Crime Prevention and Detection System and within the framework of its activities, will establish a general training for all its professionals and, if necessary, specific training for those who are more exposed to the risks detected.

## TRAINING REVIEW

---

SCSP will annually review its Crime Detection and Prevention System by identifying potential risks, adapting its training plan to regulatory and operational changes.