OCO MANAGEMENT GUIDELINES TO COMBAT CORRUPTION AND ORGANIZED CRIME THREATS AND RISKS

2013

OCOMS

Contents

Introduction

0.1 General remarks

0.1.1. Purpose of the standard

The OCOMS ™ standard is designed to meet the need for crime threats management in processes for preventing and handling criminal risks that may arise within a body. The standard is based on this international requirements and best practices, which proposes a level of requirements common to all types of bodies with a view to ensuring appropriate handling of criminal risks.

The requirements of the OCOMS ™ standard are incorporated into the body's existing processes.

Application of these requirements within the company creates what is properly called an OCOMS™ system.

0.1.2. General requirements

Bodies must realise that they are potentially exposed to criminal risks. Implementation of the OCOMS™ requirements within a body depends on its variable needs, its capacities, its size, its products and its existing processes. Adoption of an OCOMS™ system must flow from a strategic decision taken by the body.

The OCOMS™ standard applies internally, but the body may also use it to evaluate the criminal exposure risk of its Customers, Suppliers and Partners (hereinafter C/S/P).

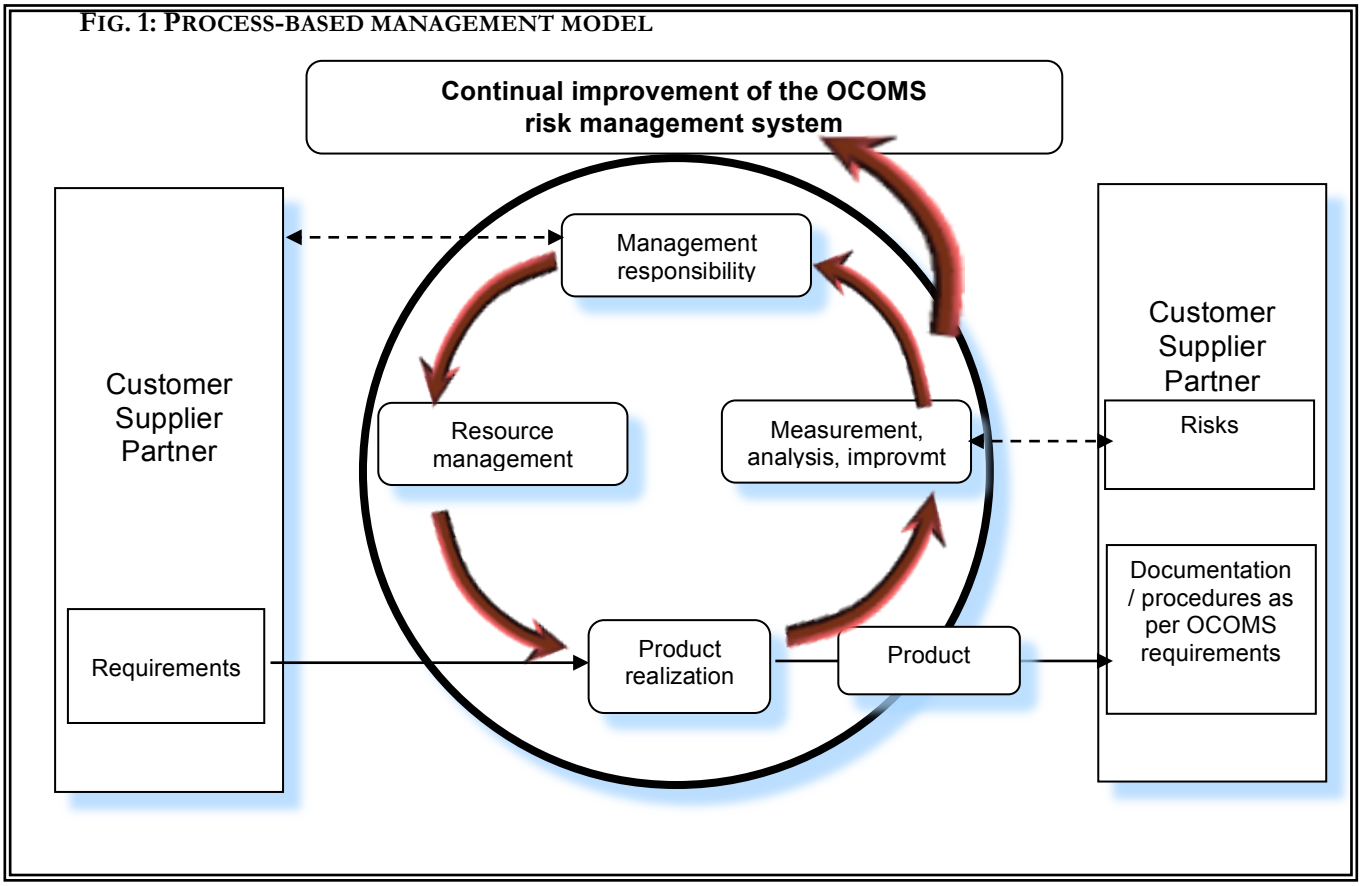
0.2 Process approach

The OCOMS™ standard is designed to encourage implementation of processes enabling the establishment to considerably enhance its resistance to possible internal or external criminal influences while improving the quality of its relations with its customers, suppliers and partners[1].

The body must first identify, adapt or, if necessary, create, the internal processes required for the implementation of an OCOMS™ system.

[1] See Fig. 1 for process diagram.

FIG. 1: PROCESS-BASED MANAGEMENT MODEL



To highlight the importance of the added value of the processes, these must be observed in relation to the principles of the Deming Wheel.
However, this diagram merely provides an indication; the body is free to install its processes based on its systemic organization.

0.3 Relationship to other standards

The OCOMS™ standard can be compatible with other standards provided that its requirements are respected[2].

1 Field of application

1.1 General remarks

The OCOMS™ standard spells out the indispensable requirements for countering the influence of criminal structures. With OCOMS™ requirements, the body can introduce its own policy to check influences of a criminal nature that may arise in connection with its actions and decisions.

1.2 Perimeter of application

The requirements of the OCOMS™ standard are generic and may apply to any body whatsoever, regardless of its size, type or goals.
In the event that the body is composed of several services, offices, subsidiaries, branches, controlled companies, etc., the requirements may apply either to the financial group as a whole or to one or more of its components [3].

Implementation of the requirements of the OCOMS™ standard implies the prior definition, by the body, of a perimeter of application that will be subject to implementation.

For a component, subsidiary, branch, etc. willing to implement OCOMS™ separately from the rest of its group, it must:

- Enjoy a decision-making autonomy;
- Have at least shareholders or decision-making power corresponding to a *de facto* or *de jure* blocking minority (depending on the domestic legal framework) over its own perimeter;
- Be responsible for establishing internal rules and regulations;
- Be in direct possession of information relating to its C/S/P ;
- Be responsible for relations with them and with its own staff.

2 Normative reference

Normative references are references published by Swiss law (recommendations, ordinances, penal code) and the laws and regulations of the European Union, the United States of America, the laws and regulation of the United Kingdom (especially the UK Anti-Bribery Act) and international bodies, as well as all documents listed in Annex A of this standard.
The body is responsible for conducting normative monitoring enabling it to ensure constant compliance with the requirements set out in the laws in force and any amendments thereto.

3 Terms and definitions

The main terms and definitions are defined in Annex B of this standard.

4 OCOMS™

4.1 General remarks

Implementation of an OCOMS™ system involves the body in its legal, technological, economic and social environment. The broad lines proposed by the OCOMS™ standard pertain to the relations that the body may have with its C/S/P.

As far as the body is concerned, implementing an OCOMS™ system implies managing and /or adapting a documents management system that is kept up to date and allows for follow-up of transactions with the C/S/P. The body will have to constantly improve efficiency in a measurable fashion.

The body must in particular:

a) Identify existing processes;
b) Define the perimeter of application;
c) Ascertain and document precisely the identities of the C/F/P with which it does business;
d) Identify and document the transactions which it conducts or in which it is directly involved with or on behalf of a C/S/P;
e) See to it that a criminal risk identification system is set up;
f) Establish regular integrity checks for C/S/P, employees, managers and the main shareholders;
g) Determine the internal criteria and methodologies needed to ensure the proper functioning of the OCOMS™ system;
h) Guarantee the availability of the resources and information needed to operate and monitor the OCOMS™ system;
i) Take the necessary steps to meet the requirements of the OCOMS™ standard and improve its implementation.

All of these points are set out below in this standard.

4.1.1. Requisite prior requirements

The body must meet two prior requirements before implementing the internal processes required by the standard. The body must have passed:

a) A feasibility study; and
b) A criminological assessment.

These evaluations must be carried out by neutral entities at a predetermined rate.

4.1.1.A. FEASIBILITY STUDY

The feasibility study is designed to ascertain:

- Whether the body has the proper structures and resources required for the effective application of the OCOMS™ standards and procedures;
- That the body has not been previously involved in a situation conducive to crime that would place experts, consultants or auditors at risk.

4.1.1.B. CRIMINOLOGICAL ASSESSMENT (INTERNAL AND EXISTING RELATIONSHIP DUE DILIGENCE)

The purpose of the criminological assessment is to establish with a reasonable degree of certainty that the body is independent of interests known to be criminal.
In the course of the criminological assessment, the expert(s) must determine whether:

a) The body is or has been subject to de facto or de jure decision-making dependency on third parties which have been recognized by at least one court of law to be part, either directly or indirectly, of a known criminal structure:
b) The body is or has been subject to abusive use of its assets by third parties which have been recognized by at least one court of law to be part, either directly or indirectly, of a known criminal structure;
c) The body has a level of exposure to high criminal risk that can damage its integrity.

Loss of independence is taken to mean situations that can, in a justified, demonstrable fashion:

d) Render inoperative the decision-making structure of the body, as described and implemented by it and identified during the feasibility study;
e) Render inoperative the decision-making and/or production structure if such criminal interests were eliminated over a three-month period.

The body may no longer be considered as independent:

f) If the conditions described under points d) and e) are no longer accompanied by clear contractual clauses that are understood by the contracting body;
g) If the conditions described under points a) and b) are such as to cause grave physical or moral damage to the body as a whole or to key figures within in[4].

4.2 Documentation requirements

The OCOMS™ documentation system must include the following:

1. External documentation:

a) Documentation relating to the feasibility study;
b) Documentation relating to the criminological assessment;
c) The OCOMS™ Specific Terms and Conditions.

2. Internal documentation:

a) Records relating to the identity of C/S/P;
b) Records relating to information on transactions performed by or on behalf of C/S/P;

[4] Grave moral damage is deemed to have occurred when a medically attested nervous illness develops subsequent to a defined action or when a loss of resources occurs that leaves the person financially destitute.
Physical damage is understood as a physical constraint exercised against the person, ranging from the threat of the exercise of physical violence all the way to murder.

c) Records on the risk rates associated with C/S/P transactions and profiles;
d) Records on the compliance rates performed by Self-Assessment in relation to the OCOMS™ standard;
e) Documents relating to the incorporation of the threat assessments processes and internal good governance required by the OCOMS™ standard;
f) The necessary documents for effectively planning, operating and controlling the processes, required by the OCOMS™ standard.

4.2.1. External documentation[5]

4.2.1.A. FEASIBILITY STUDY AND CRIMINOLOGICAL ASSESSMENT

The documentation relating to the feasibility study and the criminological assessment must allow the body to see where it stands in terms of both external and internal criminal risks on the basis of reports supplied by accredited entities.
On the basis of this documentation, the body must implement and document:

a) Steps taken to monitor the problematic situations that have been brought to light;
b) Documents and their records concerning the feasibility reports and expert assessments as well as their follow-up down to the details of their processes, making it possible to manage the related documents properly.

4.2.1.B. SPECIFIC TERMS AND CONDITIONS

The Specific Terms and Conditions act as a specific standard for the body. They take into consideration all of the applicable reservations mentioned in the OCOMS™ standard with regard to the specific situation of the body and take due account of:

a) The size of the body;
b) The complexity of the processes and their interactions;
c) Staff competence;
d) The geographical zone(s) in which the said processes operate;
e) Applicable legal and professional regulations.

4.2.2. Internal documentation

The body generates internal documentation. Documentary needs and records-related requirements differ depending on the type of process to which they refer. These processes may be broken down as follows:

- Two identification processes (identities and transactions);
- Two detection processes (detection and management);
- Two treatment processes (records and improvement);
- One ethical process and consequences;
- One criminal threats assessment process.
- One documents management and monitoring process.

[5] External documentation is produced not by the body but rather by the third party accredited to conduct feasibility studies and expert assessments. However, by providing documentation, the body makes a substantial contribution to the implementation of such studies.

4.2.2 A. C/S/P IDENTIFICATION PROCESSES

The general principle for C/S/P identification is always to establish a link of responsibility with one or more private individuals who effectively benefit from the relations that the body maintains with C/S/P (principle of beneficial owner - BO)

4.2.2.A1 . Private individuals

In the event that the C/S/P is a **private individual**, the body will have to, on the basis of official and/or verifiable documentation:

a) Ascertain and verify C/S/P identity;
b) Establish whether or not there are one or more possible principals or beneficial owners for the relations established with the body;
c) Establish whether or not there are specific contractual clauses delimiting the modalities of the relations between the C/S/P and one or more third parties and the body;
d) Ensure that the data collected in this way are fully monitored and recorded for a period of 10 years.

4.2.2.A2 . Legal entities

In the event that the C/S/P is a **legal entity**, the body will have to, on the basis of official and/or verifiable documentation:

a) Determine and verify that the C/S/P exists as a legal entity (Registrar of Companies or the equivalent);
b) Ascertain and verify the identity of the private individuals or entities that are the beneficial owners of the said legal entity or of another legal entity to which it belongs;
c) Guarantee and verify the right of representation;
d) Establish whether or not there are one or more possible principals or beneficial owners for the relations established with the body;
e) Establish whether or not there are specific contractual clauses between the C/S/P and one or more third parties delimiting the modalities of the relations with the body;
f) Ensure that the data collected in this way are fully monitored and recorded for a period of 10 years.

4.2.2.A3 Persons acting as principals

In the event that the C/S/P is a **person acting as a principal**, the body will have to, on the basis of official and/or verifiable documentation:

a) Determine and verify that the C/S/P exists if it is a legal entity (Registrar of Companies or the equivalent), or determine and verify the identity of the C/S/P if it is a private individual;
b) Ascertain and verify the identity (private individual) or the existence (legal entity) of the principal and the private individual or entities that are the beneficial owners of the relations;
c) Guarantee and verify the right of representation, contractual documents and conditions of the mandate relating to the relations with the body;
d) Establish whether or not there are one or more possible principals or beneficial owners for the financial relations established with the body;
e) Establish whether or not there are specific contractual clauses delimiting the body's relations with the C/S/P and one or more third parties,

f) Ensure that the data collected in this way are fully monitored and recorded for a period of 10 years.

4.2.2.A4 . Public institutions

In the event that the C/S/P is a **public institution**, the body will have to, on the basis of official and/or verifiable documentation:

a) Determine and verify the existence of the institution or party (C/S/P) that establishes the relations with the body;
b) Ascertain and verify the identity (private individual) or existence (legal entity) of the principals and the institution or institutions that are the beneficial owners of the relations;
c) Guarantee and verify the right of representation, legal and contractual bases and conditions allowing the institution or its part (C/S/P) to establish relations with the body;
d) Establish whether or not there are one or more possible principals or beneficial owners for the financial relations established with the body;
e) Establish whether or not there are specific contractual clauses between the C/F/P and one or more third parties delimiting the modalities of the relations with the body;
f) Ensure that the data collected in this way are fully monitored and recorded for a period of 10 years.

4.2.2.A5 Online relations

In the event that the C/S/P is a **virtual person** (online C/S/P), the body will have to, on the basis of official and/or verifiable documentation:

a) Limit its relations to only those C/S/P that have been previously identified by the body or by another reliable body acting according to similar rules checked by an independent third party;
b) Ensure that the data collected in this way are fully followed up and recorded for a period of 10 years.
c) Guarantee the integrity and security of computer data with regard to their capture, transmission and storage.

4.2.2.A6 . Reservations with regard to application

Instructions concerning the identification of private individuals or legal entities or entities acting as principals shall only apply in the case of business relations based on goods or services between the body and the C/S/P:

- If these relations involve trade in objects deemed "sensitive";
- For written or tacit contractual relations between one or more C/S/P and the body which exceed the cumulative amount, over a period of 1 month, of EUR 250,000 (two hundred and fifty thousand Euros);

or

- For written or tacit contractual relations between one or more C/S/P and the body which exceed 5% of the body's annual turnover (gross profits) (calculated on the basis of gross turnover certified for at least the two financial years preceding the transaction in relation to the date for the closing out of accounts, weighted by month – rule of three – by the results for the current financial year). In the event that the body is in its first

financial year, gross turnover for the current year, extrapolated over the (linear) year, will be taken into consideration.

4.2.2.B. TRANSACTION IDENTIFICATION PROCESSES

Here, "transaction" is taken to mean any exchange effectively concluded between two parties of any kind entering into the framework of a business or financial relationship, namely, the delivery of a service in exchange for compensation according to pre-established rules in written form (records, evidence, etc.).
The different types of transactions are virtually infinite in number.
The various forms of transaction have been broken down here according to two types of objects and two types of logics, giving four different types of transaction in all.

The two types of objects are:

4.2.2.B1 Transactions involving GOODS or SERVICES:

GOODS refer to merchandise that is real and tangible (i.e. it can be touched). SERVICES refer to acts which entail the formalized use of specific know-how in a pre-defined environment (for example, accounting, fiduciary and consulting services fall into this category).

4.2.2.B2 Transactions involving FINANCIAL ASSETS:

By FINANCIAL ASSETS we mean any object whose intrinsic value is generally not equal to its nominal value. Financial assets mainly consist of money (in its broad generic sense), securities of various sorts (stocks, bonds and shares, but also claims, IOUs, etc. (paper securities)). Art objects are in a separate category and are classified as GOODS, not FINANCIAL ASSETS.

The two types of logics are:

4.2.2.B3 PHYSICAL transactions:

PHYSICAL transactions refer to exchanges that are effectively conducted by means of a concrete exchange between the body and the contracting party (a C/S/P). This implies that the body must perform an act involving a direct exchange.

4.2.2.B4 VIRTUAL (or cashless) transactions:

So-called VIRTUAL transactions refer to exchanges that are effectively conducted but do not entail a physical exchange between the contracting parties (the body and one or more C/S/P). One generally speaks of virtual exchanges in cases where the body makes entries in its books without itself performing the relating physical exchange (e.g. a bank transfer).

Combining these logics and these objects gives us four different types of transactions:

4.2.2.B5 PHYSICAL transactions of GOODS or SERVICES (for example, any "conventional" business exchange);

4.2.2.B6 PHYSICAL transactions of FINANCIAL ASSETS (any real and physical exchange of objects recognized as financial assets);

4.2.2.B7 VIRTUAL transactions of GOODS or SERVICES (any business exchange whereby the body makes an entry corresponding to such a transaction (for example, trading) rather than itself engaging in the relating physical exchange);

4.2.2.B8 VIRTUAL transactions of FINANCIAL ASSETS, typically any financial service that performs transactions by making and recording entries (for example, bank transfers, stock market investments, trading, various deals).

The beneficiaries and principals of the transactions, together with any intermediaries who take part therein in any way whatsoever, must be identified and recorded in such a way as to ensure the effective traceability of the service and the corresponding consideration. In order to ensure maximum transparency and effective traceability, the standard of identification of transactions is designed to enable identification of all of the actors effectively involved in the "transaction chain" as well as their respective roles.
The "transaction chain" is not necessarily a linear progression from A to B, but may involve different actors on different levels.
Each link between each actor has intrinsic constraints that must be formalized in advance. These constraints or "conditions" are generally stipulated in the contractual documents or in legal or professional regulatory provisions that apply depending on the type of transaction performed.

The transaction chain may also be viewed from a temporal perspective which is subdivided into three events that are decisive for any transaction:

4.2.2.B9 Planning the transaction

Identification of the parties involved and the respective roles in a specific transaction chain. These elements must be formalized.

4.2.2.B10 . Performing the transaction

A process that entails actual execution of the exchange. The body must formalize performance during this phase.

4.2.2.B11 Checking the transaction

The correspondence between the actions undertaken when the transaction was performed and the elements planned for this same transaction. Checking to make sure that the purpose of the transaction has been respected. Transmission to auditors or experts of the necessary documentation to carry out an audit or check the books.

Transactions may be checked at any moment.

4.2.2.B14 . Reservations

The following steps pertaining to identification and record-keeping apply to any transaction of a value equalling or exceeding a limit fixed and justified by the body.
This lower limit does not apply to transactions featuring the following characteristics:

4.2.2.B15 .Retail transactions with individuals (private individuals representing only themselves, including the self-employed or partnerships) shall be considered if falling into reservation or not by the body and justified by it.

When the annual accumulated value of transactions with a single C/S/P equals or exceeds EUR 50,000, the reservations no longer apply and identification standards must be respected. For companies located in the United States, this limit drops to USD 10,000 for bodies with a banking or financial intermediation licence.
As for companies or legal persons (with the exception of ordinary partnerships) engaging in commercial transactions of goods or services with other persons, the following identification and

record-keeping measures apply only in the case of transactions involving financial assets or "high-risk" transaction objects.

4.2.2.B17 Documentation

A transaction implies that the following actors must be present:
1) A **sender**, and
2) A **receiver**

The exchange works both ways: from the sender to the receiver (concerning the object of the transaction) and from the receiver to the sender (concerning the compensation for the object of the transaction).

A distinction is also made with regard to another type of actor, who may or may not take part in the transaction and who is appointed:
3) The **intermediary or intermediaries** (logistics of the transaction between the sender and the receiver).

The body must identify, verify and document the following four transactional elements:

a) The actors
The body identifies the transactional actors on the basis of verifiable official and/or contractual documents.

b) The nature of the transaction
The body must identify the reason(s) leading the parties to perform the transaction in which it is directly involved on the basis of documents ruling out any doubt as to the nature of the transaction. The elements to be identified are the transactional schema (the flows and actors of services and compensation) and the reason for the transaction (moment and schema).

c) The purpose of the transaction
The body identifies and verifies the reality of the transactional service and its compensation and checks to see whether they comply with prevailing standards and practices.

d) Transaction-related documentation
The body introduces a system making it possible to manage the checks and the documentation produced in order to being able to link any transaction to at least one existing C/S/P. The documentation must allow the body to provide third parties with proof of the transaction's compliance.

e) Special instructions
The body must ensure that none of its own staff members can loan, rent or grant a customer or a third party rightful claimant partial or full disposal over a relation to which the beneficiary is another third party, the body's employee(s) or the body itself without the express, valid and verifiable authorization of the said beneficiary stipulating the exact modalities of the loan, rental or grant.

The body must enter and carry over onto its balance sheet all transactions performed. Regular transactions must be checked thoroughly at set intervals.

4.2.2.C. DETECTION PROCESSES (RISK RATES AND RECORDS)

The body implements a detection system that generates a criminal risk index as well as a documentary system making it possible to trace its actions and link them to the C/S/P and related transactions, as mentioned in parts a) and b) above. This might include a due diligence process.

All of the elements making it possible to set up a detection system must be recorded in such a way as to ensure ease of understanding by third parties as well as constant traceability between the different parties directly involved in the transactional processes.
The records system must enable the body to directly link the documentation required by the OCOMS™ standard concerning the C/S/P to the transaction(s) performed in which it is directly involved.

4.2.2.D. MANAGEMENT PROCESSES

The detection system will have to set thresholds (at least two) that will imply specific action by the body in relation to the situations detected, depending on the level of criminal risk reached.
The body will have to introduce procedures for dealing with cases that are contentious or feature a high risk rate according to the thresholds set.
The setting of thresholds, the method used for their calculation and the corresponding reasons will have to be set out in an internal document. This document must enable each and every one of the body's staff employees to understand and apply the system that has been introduced in an optimal fashion for the body.
The management procedures must allow for the possibility of disinvestment in the case of a C/S/P with an excessively high risk rate.

4.2.2.E. ETHICAL REQUIREMENTS AND CONSEQUENCES

The body must draft a Code of Ethics that is valid for the entire body, its majority shareholders, its directors and, as necessary, its employees.

This document must contain at least the following elements:

a) The body must under no circumstances take part in or tolerate operations involving corruption, money laundering or other illegal practices. Nor may it engage in the trafficking of arms or other materials intended for terrorist activities, drug trafficking or any other activity relating to organized crime, or in general in any dealings that are prohibited by the international and national standards that apply to it.
b) The body may not hold, keep or create undeclared sums (slush funds) with a view to using them in a way that contravenes international legal standards and the national standards of the country in which it conducts its business.
c) The body may not act in a way that hinders legal proceedings brought against one or more employees or customers, rightful claimants, etc. by the legal or police authorities of its place of domicile or other authorities who are legally entitled to do so or are acting by power of attorney.

d) The body may not offer benefits in cash, in kind or in any other form whatsoever to private individuals or legal entities with public responsibilities with a view to changing their acts or judgments in connection with the goals pursued by the body, barring any relevant legal provisions.
e) The body must refuse to establish business or financial relations with private individuals or legal entities that have committed acts punishable under international humanitarian legal and regulatory standards[6].

In this document, a section relating to employees, owners and other directors must clearly define appropriate behaviour and acceptable limits with regard to corruption, nepotism or other unjustified or clearly formalized forms of arbitrariness or favouritism that are known to all within the body.
All persons in positions of responsibility within the body must be familiar with this document and have access to it. It must also be made available to the C/S/P and other third parties.

This document must also be updated and presented in an appropriate, consistent fashion, according to a procedure established by the body.

4.2.3. Documents control

The OCOMS™ contact person in the company must have control over the documents required for the OCOMS™ management system.

A documented procedure must be established to:
a) Check the correspondence of documents prior to dissemination;
b) Review, update and approve any new system or procedure;
c) Ensure that amendments to and the status of the prevailing version of documents, systems and procedures are identified and listed in a document kept up to date;
d) Ensure that the latest versions of the documents, systems or procedures to be implemented are available when they are applied;
e) Take pains to identify and control the dissemination of documents from outside;
f) Take the necessary steps to prevent any unintentional or intentional use of outdated, fraudulent or forged documents.

4.2.4. Records control

Records must be made and kept in conformity with the requirements set out under point 4.2 above in order to provide proof of compliance with requirements and of the proper functioning of the system.

4.2.5. Records storage requirements

Records must be easy to understand, identify and access. A documented procedure must be established to guarantee the identification, storage, protection, accessibility, duration of conservation, management and elimination of records.

[6] For example, human rights, children's rights, UN resolutions, FATF or OECD recommendations concerning international humanitarian law and any other regulations, precedents and recommendations issued by official bodies in respect of international humanitarian law.

Computerized or digital records must be stored and protected in such a way as to avoid, as much as possible, according to the degree of confidentiality required for the documents in question by the body's policy, intrusions leading to unauthorized access to data, data corruption or data theft.

5 Management responsibilities

5.1 Management commitment[7]

Management must provide proof of its commitment by:

a) Ensuring regular communication within the body and with the parties directly involved in the OCOMS™ process;
b) Introducing a corporate policy and culture that is conducive to OCOMS, thus enabling it to assure its customers that the services and products offered comply with stringent standards and are fully transparent in terms of legal and regulatory requirements;
c) Promoting business with C/S/P that respect the same ethical standards;
d) Introducing a process for monitoring and checking the ethical and transparency goals of the system established by the body;
e) Conducting regular management reviews; (ISO 9001/9004 is acceptable);
f) Earmarking the necessary resources for the proper fulfilment of the requirements set out in this international standard.

5.2 Customer satisfaction

Management must ensure that customers' needs and requirements are determined and met in order to increase customer satisfaction.

5.3 Criminal risk policy

Management must ensure that its criminal risk policy:

a) Takes into account all applicable ethical, professional, legal and regulatory aspects;
b) Details with the structures and procedures implemented and is suited to the actual circumstances and goals of the body;
c) Commits all of its employees and majority shareholders to ensuring and constantly enhancing the effectiveness of the system;
d) Provides a specific framework for setting, adjusting and checking its objectives with regard to criminal risks and quality, OCOMS and integrity in the conduct of its business;
e) Disseminates its objectives and policy within the body and sees to it that these elements are understood;
f) Performs checks ensuring constant compliance with the said policy and its components.

5.4 Planning

Management must ensure that:

a) The planning of the system and the integrity and OCOMS of its products or services in relation to the parties directly involved are implemented and respected;

[7] For companies located in and/or listed on markets situated in the United States of America, the management must personally vouch for the accuracy of the body's annual accounts.

b) The coherence of the system introduced is not affected when changes are made to the body or the standard.

5.5 Responsibility, authority and communication

Management must see to it that responsibilities and authority are defined and communicated within the body.

The management must appoint an officer in charge who will have the task and authority in particular to:

a) See to it that the required OCOMS™ standards and procedures are applied;
b) Ensure that the necessary processes for the application of requirements within the body are defined, implemented, followed and maintained;
c) Provide follow-up and assistance with the application and ongoing improvement of requirements;
d) Ensure internal and possibly external communication of the objectives, documents and other elements required and/or introduced and see to it that they are disseminated, accessible and easily understandable;
e) Monitor circumstances conducive to crime within the body through procedures as well as by any other means, as need be;
f) Report back to management and, as need be, depending on the procedures introduced, to the authorities, on the functioning of the OCOMS™ system set up by the body, any questions linked to criminal, legal and/or ethical issues as well as any need for improvement;
g) Make sure that the body's C/S/P are also aware of requirements.

5.6 Management review

5.6.1. General remarks

Management must, at regular and if possible scheduled intervals, review implementation of the body's OCOMS™ system in order to ensure that it remains compliant, relevant, adequate and effective. This review must include an evaluation of the body's compliance with the requirements of the present international standard, consideration and treatment of issues of a criminal, penal and/or ethical nature that impact on the body, one of its members or one of its C/S/P as well as an assessment of opportunities for improvement and the need to modify the system, including the policy relating to organized crime and related objectives.

A record must be kept of these management reviews (cf. subheading 4.2.4).

5.6.2. Management review inputs

The management review must encompass at least the following elements:

a) The body's process compliance rate with the requirements of the present international standard (evaluation or Self-Assessment);
b) The results of internal or spot checks as well as information on how cases of non-compliance were dealt with;
c) Information on possible problematic cases that have been brought to light and/or are being dealt with;
d) Information relating to the market and information from the C/S/P;
e) Planned and/or ongoing preventive and/or corrective action;
f) Changes that could affect the OCOMS™ system;

g) Internal recommendations and/or information pertaining to problematic cases within the body or to possible or desirable improvements to the system;
h) The results of Self-Assessments.

5.6.3. Management review outputs

Management review outputs must at the least include decisions and actions relating to:

a) Treatment of the cases and/or problematic situations announced;
b) Processing of information relating to the market and information from the C/S/P;
c) Improvement of products and services as per OCOMS™ requirements;
d) Resource requirements linked to the proper functioning of the OCOMS™ system.

6. Resource management

6.1 Resource availability

The body must ascertain and ensure the availability of the resources needed to implement the requirements stipulated by this OCOMS standard.

6.2 Human resources

The body must:

a) Ensure availability in terms of time and technological and material resources;
b) Ascertain the requisite skills for staff performing jobs that impact on the system;
c) Make sure that its own employees are properly trained and aware by enabling them to acquire the elements they need to understand the operational requirements, the actual situation and operational, legal and professional criminal risks as well as their impact on the security of the body;
d) Make sure that the members of its staff, its management and its majority shareholders and/or partners are mindful of the relevance and importance of their actions and decisions and of the way in which they contribute to achieving the body's objectives with regard to the policy on organized crime and other criminal structures and activities;
e) Keep appropriate records of basic and advanced training, know-how and experience in the fields identified and required, and use them to constantly improve the OCOMS™ system;

6.3 Infrastructure

The body must determine, supply and maintain/update, to the best of its means and policy, the necessary infrastructure to ensure that its internal processes comply with the requirements stipulated in the present standard. Such infrastructure includes, depending on the case:

a) Buildings, workspaces and related installations;
b) Equipment (both software and hardware) linked to the processes;
c) Support services (such as logistics and communication media).

6.4 Work environment

The body must determine and manage the necessary work environment to:

a) Make sure that its products and processes comply with the requirements of the OCOMS™ standard;

b) Guarantee, as much as possible, the physical integrity of its staff in relation to direct and related criminal risks.

7 Implementation of controls

7.1 Internal controls

The body must plan and implement the necessary controls in accordance with the procedures required by the present standard:

a) C/S/P identity controls must be ongoing;
b) Controls of transactions performed or executed by or on behalf of C/S/P must be ongoing;
c) Detection controls of C/S/P and related transactions must be ongoing;
d) Controls pertaining to ethical and professional regulations must be carried out according to the timetable established by the body;
e) Controls tied to the management review depend on the scheduling of the said reviews;
f) Self-Assessment compliance controls must be carried out at least once every six months.

7.2 External controls

7.2.1. General remarks

There are two types of external controls: feasibility studies and expert assessments.
Feasibility studies and expert assessments are conducted by an independent body that is accredited in accordance with the elements mentioned under subheading 4.1.1.

8. Measurement, analysis and improvement

8.1 General remarks

The body must plan and implement the necessary measurement, analysis and improvement processes in order to:
a) Demonstrate compliance with requirements;
b) Ensure compliance of the internal system;
c) Constantly enhance the effectiveness of the system introduced.

This must include the identification and introduction of the methods used and applicable, including possible statistical techniques as well as the scope of their utilization.

8.2 Monitoring and measurement

The body must schedule internal audits at planned intervals to determine whether the system:
a) Is compliant with provisions and requirements;
b) Is implemented effectively.

When planning the internal control programme, due consideration must be given to the status and importance of the processes and areas to be checked as well as the results of previous controls. Control criteria, fields, frequency and methods must be defined. The choice of auditors and the performance of controls must ensure the objectivity and impartiality of the

process. Auditors must not audit their own work performed (consulting, expert assessments, feasibility studies).
Responsibilities and requirements for planning, performing and reporting on the results of the audits conducted and for keeping the relevant records (cf subheading 4.2.4) must be defined in a documented procedure.

The necessary supervision must be provided to ensure that steps are taken without undue delay to eliminate both cases of non-conformity detected during controls and their causes.

The body must use appropriate methods for monitoring and measuring processes.

The body must take monitoring and follow-up steps relating to planning, implementation, communications and records pertaining to the fulfilment of requirements, primarily as regards:

- C/S/P identification;
- Related transactions;
- Indications and information collected and/or generated through use of the detection system.

8.2.1 Self-Assessment

The principle of Self-Assessment according to the following schema is a prerequisite.

a) The body must run internal courses to raise awareness of persons directly involved in the Self-Assessment process (evaluation by Self-Assessment based on a questionnaire);
b) The process for using the Self-Assessment must be incorporated into the process for internal and third party controls;
c) Self-Assessments must be incorporated into the body's annual programme;
d) There is a need to monitor the management control indicators generated by the Self-Assessment results.

8.3 Dealing with non-conformity

The body must see to it that cases of non-conformity brought to light by internal or third party audits are dealt with. The body must deal with and provide acceptable solutions to cases of non-conformity that come to light while the system is in operation:

a) By taking steps to eliminate the cases of non- conformity detected;
b) By changing its processes in order to eliminate the source of non- conformity.

A record must be kept of the nature of the cases of non- conformity and any subsequent action, such as waivers issued (cf. 4.2.4).

Once an element of non- conformity has been corrected, it must be checked once again to ensure that it meets requirements.

8.4 Data analysis

The body must determine, collect and analyse the appropriate data to demonstrate the relevance and effectiveness of the system and evaluate possibilities for improvement. This must include data generated by control activities, internal and external dissemination of the corporate policy and related documents, training and monitoring or any other pertinent source.

Data analysis must provide information on:

a) Compliance with requirements;
b) Compliance of compulsory processes with the body's other processes as well as its results and relations with its C/S/P;
c) Characteristics of and trends for criminal risks facing the body.

8.5 Improvement

The body must constantly improve the effectiveness of the system by following its policy on criminal risk in general, its ethical and professional objectives, audit results, data analysis, preventive and/or corrective action and management reviews.

8.5.1. Corrective action

The body must take steps to eliminate the causes of non- conformity by preventing their recurrence. This corrective action must be proportionate to the non- conformity it is designed to remedy and must not generate other, subsequent cases of non- conformity or be prejudicial to the body's other processes or objectives.

A documented procedure must be established in order to define the requirements for:

a) Reviewing cases of non- conformity;
b) Determining causes of non- conformity;
c) Evaluating the need to take action to prevent the recurrence of cases of non- conformity;
d) Determining and taking the necessary action;
e) Recording the results of action taken;
f) Reviewing or auditing corrective action taken.

8.5.2. Preventive action

The body must determine which types of actions would make it possible to eliminate the causes of non- conformity and its exposure to criminal risk with a view to preventing their recurrence. Such action must be tailored and proportionate to the effects of the potential problems.

A documented procedure must be established in order to define the necessary processes and records to implement such preventive action.

Annex A: Normative references

The following normative references were used in creating OCOMS™:

1. FATF, The 40 Recommendations of the FATF on Money Laundering, Paris OECD, 1998.
2. FATF , The 40 New Recommendations of the FATF, Paris OECD, 2004.
3. FATF , Methodology for assessing compliance with the FATF 40 Recommendations and the FATF 8 Special Recommendations, Paris, 2004.
4. BIS, Basel Committee on Banking Supervision; Customer due diligence for banks, Basel, 2001 and 2004.
5. FATF, Providing feedback to reporting financial institutions and other persons, Best Practices Guidelines, Paris, 1998.
6. FATF, Combating the abuse of non-profit organisations – International Best Practices, Paris, 2002.
7. UN, Political Declaration and Action Plan against Money Laundering, New York, 1998.
8. UN, International Convention for the Suppression of the Financing of Terrorism, New York, 1999.
9. Federal Law on Combating Money Laundering in the Financial Sector (LBA) – 955.0 – Bern, 1997.
10. Ordinance on the Registry of the Supervisory Authority for Combating Money Laundering (OReg-LBA), Bern, 2001.
11. Ordinance on the Bureau of Communication Concerning Money Laundering (OBCBA), Bern, 2000.
12. Swiss Penal Code.
13. Ordinance of the Supervisory Authority for Combating Money Laundering Concerning the Due Diligence Obligations of Financial Intermediaries Under Its Direct Supervision, Bern, 1998.
14. Circular CFB 98/1 and annexes.
15. Fedpol, Report on the Internal Security of Switzerland, Bern, 2002.
16. Fedpol, Report on the Internal Security of Switzerland, Bern, 2001.
17. CFB, Bulletin, special booklet: Combating Money Laundering, Bern, 44/2003.
18. MROS, 1st Report of Activities 1998-1999, Bern.
19. MROS, 5th Annual Report 2002, Bern.
20. OFP, Situation Report 1999, Bern.
21. OFP, Situation Report 2000, Bern.
22. OECD, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 2001.
23. FinCEN, USA Patriot Act – 2001.
24. FinCEN, USA Patriot Act Update 2003.
25. FinCEN, USA Patriot Act, 314(a), Facts, Feeedback, Statistics 1999-2004.
26. United States Congress, RICO Act, Washington DC, 1970.
27. United States Congress, RICO Act, RICO in a nutshell, Washington DC, 1970, www.ricoact.com.
28. European Union, Anti-Fraud Office (OLAF), 28 April 1999.
29. Regulation 1073/1999/EC of the European Parliament and the Council, of 25 May 1999, concerning investigations conducted by the European Anti-Fraud Office (OLAF).

30. Regulation (EURATOM) No. 1074/1999 of the Council, of 25 May 1999, concerning investigations conducted by the European Anti-Fraud Office (OLAF).
31. Inter-agency agreement, of 25 May 1999, between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning investigations conducted by the European Anti-Fraud Office (OLAF).
32. Sarbanes-Oxley Act – 2002
33. Sarbanes-Oxley SEC Rules & Regulations Nos 208, 301, 303, 306, 307, 401, 403, 404, 802, RMIC.
34. EGMONT GROUP: Best practices in information exchange between FIUs.
35. EGMONT GROUP: 100 cases.
36. CFB: CFB Ordinance on Money Laundering, Bern, 1998, 2003.
37. CFB: Form for examining implementation of the CFB ordinance on money laundering.
38. Wolfsberg Statement on Monitoring Screening and Searching - September 2003
39. Wolfsberg AML Principles for Correspondent Banking - November 2002
40. Wolfsberg Statement on The Suppression of the Financing of Terrorism - January 2002
41. Wolfsberg AML Principles on Private Banking - Revised Version May 2002.
42. ISO 9004: 2000
43. ISO 9000: 2000
44. ISO 10011-1:1990, Guidelines for auditing quality systems - Part 1 : Auditing
45. ISO 10011-2:1991, Guidelines for auditing quality systems - Part 2 : Qualification criteria for quality systems auditors.
46. ISO 10011-3:1991, Guidelines for auditing quality systems - Part 3 : Management of audit programmes.
47. ISO 10013:-1), Guidelines for developing quality manuals.
48. FATF: 2004: Annual Report 2003-2004, Paris OECD
49. FATF: 2003: Annual Report 2002-2003, Paris OECD
50. FATF: 2002: Annual Report 2001-2002, Paris OECD
51. FATF: 2001: Annual Report 2000-2001, Paris OECD
52. FATF: 2000: Annual Report 1999-2000, Paris OECD
53. FATF: 1999: Annual Report 1998-1999, Paris OECD
54. FATF: 1998: Annual Report 1997-1998, Paris, OECD
55. EU: 2004: Final Agreement against Fraud – 2004-0187 (CNS); Brussels.
56. Legge 13 settembre 1982, n. 646, Disposizioni in materia di misure di prevenzione di carattere patrimoniale ed integrazione alle leggi 27 dicembre 1956, n. 1423, 10 febbraio 1962, n. 57 e 31 maggio 1965, n. 575.
57. Legge 7 marzo 1996, n. 109, Disposizioni in materia di gestione e destinazione di beni sequestrati o confiscati. modifiche alla legge 31 maggio 1965, n. 575 , e all'articolo 3 della legge 23 luglio 1991, n. 223 . abrogazione dell'articolo 4 del decreto-legge 14 giugno 1989, n. 230, convertito, con modificazioni, dalla legge 4 agosto 1989, n. 282.
58. Legge 23 dicembre 2002, n. 279, Modifica degli articoli 4-bis e 41-bis della legge 26 luglio 1975, n. 354, in materia di trattamento penitenziario.
59. Articoli 416 bis (Associazione di tipo mafioso) e ter (Scambio elettorale politico mafioso).
60. Articoli 648 bis (Riciclaggio) e ter (Impiego di denaro, beni o utilità di provenienza illecita).
61. Legge 11 agosto 2003, n. 228 Misure contro la tratta di persone.

62. Protocollo addizionale della Convenzione delle Nazioni Unite contro la Criminalità organizzata transnazionale per combattere il traffico di migranti via terra, via mare e via aria.
63. Protocollo addizionale della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale per prevenire, reprimere e punire la tratta di persone, in particolare di donne e bambini.
64. Legge 22 dicembre 1999, n. 512, Istituzione del Fondo di rotazione per la solidarietà alle vittime dei reati di tipo mafioso.
65. La teoria degli stockholder e le preferenze morali dei consumatori in un contesto caratterizzato dall'ingerenza della criminalità organizzata nelle attività economiche 25/11/2006, www.addiopizzo.org.

Annex B: Terms and definitions

OCOMS™:	"OCO Management Integrity System"
Criminal organization:	"Any group having a corporate structure whose primary objective is to obtain money through illegal activities, often surviving on fear and corruption" (Interpol). **"A criminal organization is a group of actors, interconnected in a stable and structured way, acting in an autonomous manner with the objective to ensure maximal enrichment, primarily by systematic and coordinated exploitation of opportunities criminalized by law or any other form of regulations (traditions, customs, etc.)" (criminological definition).** This definition will be completed by legal definitions existing in the countries in which the certification will be applied.
Sensitive sectors and objects:	Branches of business dealing with goods, services or financial assets that have been statistically recognized to be at greater risk of infiltration by organizations or other criminal groups.
Geographical risk zones:	A geographical risk zone is a region in the world (not necessarily within strict national borders) in which the activity of organizations or other criminal groups is statistically high, endemic or historically linked.
Body:	Any legal entity or other individual, in full or in part, with its own, independent business dealings according to the terms mentioned under point 1 (field of application). Specific legal provisions will be applied in conformity with the provisions in force in the country in which certification will be applied.
Suspectabilization:	Refers to the procedure whereby possible suspicions of participation in a criminal organization or group are revealed and evaluated.
Physical transaction:	Any exchange directly involving one or more elements characterized by tangible reality (merchandise, services, etc.).
Virtual transaction:	Any exchange without a tangible physical movement or modification of one or more elements which have a tangible physical reality and are concerned by the transaction.
Traceability:	Ability to trace all components and dimensions (temporal and geographical) of an event.
Public institution:	Any group of persons acting in a concerted,

	coordinated fashion in the management of public property and under the direct or indirect authority of officials with recognized public duties.
Online means:	Any means of electronic or telephonic communication making it possible to maintain remote business or financial relations without recognized physical contact (paper letter, meeting, etc.).
Suspicion indicators:	A body of indicators making it possible to determine the suspectability rate of a customer or transaction. These indicators and their combination modules are made available to the body when it opts for OCOMS™ certification.
Evaluation procedure:	Internal procedures enabling the body to deal with cases with medium or high suspectability rates. These procedures are made available to the body when it opts for OCOMS™ certification.
C/S/P – General:	The C/S/P is always the beneficial owner of relations with the body that has undergone certification.
C/F/P – Customer:	A private individual or legal entity that purchases goods or services from a supplier.
C/F/P – Supplier:	A private individual or legal entity that provides the goods or services needed for the production or operation of a body or company.
C/F/P – Partner:	A body or person with which another entity works together to achieve jointly agreed objectives. *Body* is taken to mean a group, which may or may not be governed by institutions, that sets itself specific goals. This can be a body, company, association, syndicate or various bodies as well as any private individual or legal entity. In the context, the term *partner* is most often used in the plural.
Agent:	A private individual or legal entity that has been empowered to act on behalf of or represent another person, called a *principal*.
Grounds cited:	Reasons put forward to justify or explain an established fact.
Type (of transaction):	Reference to standardized structures for transactional schemas that can, owing to their repetitive nature, be classified in the form of a typology.
Structure (of transaction):	The way in which the transaction is constructed, including the way in which the roles of the various actors have been apportioned and the way in which performance is executed.
Correspondence:	Plausibility of combining two or more elements

	referring in this case to one or more transactions realized by one or more bodies (profiles).

****