DIIR Deutsches Institut für Interne Revision e.V.

DIIR Audit Standard No. 5

STANDARD FOR THE AUDIT OF THE ANTI-FRAUD MANAGEMENT SYSTEM BY THE INTERNAL AUDIT ACTIVITY

Issued by the DIIR under the auspices of the DIIR Working Group "Aversion of White Collar Crime in Companies"

Project Manager
Lars Riether, Attorney-at-law

Download at

http://www.diir.de/fachwissen/veroeffentlichungen/standards

Published in May 2012 and amended in September 2015 (Version 1.1), Frankfurt am Main

This document is the authorized translation of the original DIIR Revisionsstandard Nr. 5 "Standard zur Prüfung des Anti-Fraud-Management-Systems durch die Interne Revision".

Table of Contents

1. INTRODUCTION 2
   1.1 Objective of the standard 2
   1.2 Addressees 2
   1.3 Bindingness of the standard 2
2. DEFINITIONS AND LEGAL FRAMEWORK CONDITIONS 3
   2.1 The definition of “fraud” 3
   2.2 The definition of “anti-fraud-management” 3
   2.3 Statutory and legal requirements, standards and risks 4
      2.3.1 General requirements 4
      2.3.2 Specific requirements for credit institutions and financial services institutions, as well as insurance companies 5
      2.3.3 Specific requirements for public institutions 5
      2.3.4 Legal risks with a lack of implementation of an AFM 5
3. TASKS OF INTERNAL AUDIT WITHIN THE AFM 7
4. AUDIT STRATEGY AND APPROACH 9
   4.1 Auditing the organisational structure of the AFM 9
   4.2 Auditing the process organisation of the AFM 9
      4.2.1 AFM objectives 9
      4.2.2 Fraud risk identification and fraud risk assessment 10
      4.2.3 Fraud risk control and risk limitation 10
      4.2.4 AFM communication 11
      4.2.5 Informant system 11
      4.2.6 Forensic special investigations 11
      4.2.7 AFM response plan 12
      4.2.8 AFM reporting obligations 12
5. REPORTING OF THE INTERNAL AUDIT ACTIVITY 14

1. INTRODUCTION

In times of increasing white collar crime and complex white collar criminal methods, more and more companies and public institutions (hereinafter: organisations) are exposed to the risk of financial damage due to white collar crimes of their own employees – partially also through interaction with external parties. Improved methods of detection and preventative organisation-wide capture of fraud risks lead to an increased clear-up rate of fraud within the organisation.

For the avoidance of liability risks and reputational damage, it is therefore the responsibility of the organisation to install an effective anti-fraud management system (hereinafter: AFM) and implement measures to avert white collar crimes. This takes place in the organisation's own interest and based on respective legal obligations, as well as resulting implementing regulations.

1.1 Objective of the standard

This document describes the ***standard for auditing the anti-fraud-management system.***

The objective is to create a framework based on current scientific and practical findings for auditing the AFM in organisations by the internal audit activity. The standard particularly has the purpose of planning AFM audits to be performed and substantiating the audit mandate. For internal audit employees, the standard is therefore a "red thread", which offers them basic orientation and specifies uniform quality criteria for assessing the AFM. With respect to a necessarily limited scope, the standard takes account of the core elements of a risk-orientated audit approach of the AFM, which is to be aligned with the respective, concrete, organisation-specific circumstances. Therefore, the standard does not claim to be comprehensive.

1.2 Addressees

This standard is operationally aimed at chief audit executives and internal auditors, as well as compliance, risk management, security and anti-fraud officers.

For the organisations' management level, the standard provides information on capture, evaluation and proper handling of fraud risks in respect of the management responsibility and within the context of corporate governance requirements.

It is also intended to form the basis for external third parties dealing with AFM matters, such as external auditors, investigation authorities or regulatory authorities.

1.3 Bindingness of the standard

This audit standard was developed by DIIR – Deutsches Institut für Interne Revision e.V. as local guidance supplementing the International Professional Practice Framework (IPPF) following an appropriate due process. The use of this audit standard is strongly recommended for internal auditors in Germany.

If individual adaptations are necessary in organisations, the standard must be applied analogously.

2. DEFINITIONS AND LEGAL FRAMEWORK CONDITIONS

For the effectiveness of an organisation's AFM, a substantiation of the definition of "fraud" must first take place for this organisation and be documented accordingly. This is necessary because the German jurisdiction does not provide a legal definition of "fraud". Furthermore, the literature also does not contain a conclusive legal opinion regarding which elements are subsumed under the definition of "fraud".

2.1 The definition of "fraud"

In general, "fraud" is regarded as deliberately committed prohibited acts, which can lead directly or indirectly to damaging or jeopardising the assets of an organisation and/or to operational risks in the business processes of the organisation.

In view of this, "fraud" is defined in this standard as an intentional act by one or more individuals – members of management or those charged with governance, (other) employees or third parties – to obtain an unjust or illegal advantage.

Such acts can be committed by members of the organisation (internal fraud), business partners of the organisation and by third parties who are not linked to the organisation (external fraud). They frequently have criminal relevance. Examples to be mentioned here are crimes such as theft (§ 242 German Criminal Code (StGB)) and embezzlement (§ 246 StGB), fraud and breach of trust (§§ 263, 266 StGB), forgery of documents (§ 267 StGB), money and stamp forgery (§ 152 StGB), preferential treatment (§ 257 StGB), money laundering (§ 261 StGB), criminal acts against competition (§§ 298, 299 StGB), malpractice in office (§§ 331 - 334 StGB) and property damage (§ 303 StGB).

The individual version of the definition of fraud in an organisation should be based on the organisation's assets and its operating objectives, the necessary processes for achieving these objectives and internal guidelines. By means of a risk analysis, it should be systematically examined and documented which groups of persons can concretely cause risks or damage to assets by which acts using which resources. The options for acts to the detriment of the organisation, which are determined in this way, as well as the allocation of the acts to individual persons or groups of persons form the content of the individual definition of fraud in the organisation. In the interest of an organisation-wide, consistent understanding, it is therefore necessary to describe the respective AFM in its concrete version.

2.2 The definition of "anti-fraud-management"

Generally, "anti-fraud-management" is regarded as all measures of an organisation, by means of which it

- prevents fraud (fraud prevention),
- detects fraud (fraud detection),
- processes fraud in a structured manner in the event of indications or suspicions, as well as responding appropriately to fraud cases that have become obvious (fraud investigation).

Therefore, the AFM fundamentally contains a preventive, a proactive and a reactive auditing component and is an integral component of organisation-wide compliance management and the internal control system.

The individual structuring of the AFM in an organisation requires the clarification of questions relating to the organisational and operational structure, as well as risk/efficiency considerations. The decision about the concrete structure of the AFM should be made under consideration of the organisational framework and

management's view on the structure. In doing so, the possible detrimental acts determined for the organisation, the groups of persons who can commit these acts and the opportunities that arise for these acts must be taken into consideration.

The considerations on which the structure of the AFM is based (risk and efficiency considerations) should be documented in a verifiable manner. As results of the decision-making process, a description of the tasks and authorities of the AFM and a description of its organisational structure classification should exist, which are bindingly communicated in the organisation.

2.3 Statutory and legal requirements, standards and risks

The requirements for the implementation of an AFM as a significant component of the risk management system result indirectly from the following legal provisions.

2.3.1 General requirements

The provision of § 91 Par. 2 of the German Stock Corporation Act (AktG), introduced during the course of the Corporate Sector Supervision and Transparency Act (KonTraG), specifies, inter alia, that the board of directors must take suitable measures, particularly the establishment of a monitoring system, to ensure that developments which may jeopardize the existence of the company can be recognised at an early stage. In correspondence with this, compliance with the measures in accordance with § 91 Par. 2 AktG with respect to the existence and operation of a risk management system and the related measures in the area of internal audit are subject to the statutory financial statement audit of listed stock corporations in accordance with § 317 Par. 4 of the German Commercial Code (HGB).

The extended obligations that are applicable only to the stock corporation in accordance with the wording of § 91 Par. 2 AktG develops a "radiating effect on the framework of duties of the managing directors of other company forms as well", according to the justification of the government draft to the KonTraG. In addition, the duty of the board of directors for a legality check of the employees working in the company and taking suitable organisational measures is derived from §§ 76 Par. 1 and 93 Par. 1 AktG.

Clause 4.1.3 of the German Corporate Governance Code (DCGK) accordingly envisages that the board of directors must ensure compliance with the legal provisions and the internal company guidelines and must work towards their observance by the group companies (compliance). Furthermore, in accordance with Clause 3.4 Sentence 2 DCGK, the board of directors must inform the supervisory board regularly, timely and comprehensively about all questions relevant to the company regarding the risk situation, risk management and compliance. The DCGK does not develop any direct legal obligation for organisations, as they are free to follow the regulations of the Code. However, the so-called declaration of compliance in accordance with § 161 AktG, which was inserted in the Transparency and Disclosure Act (TransPuG) during the course of further reform of stock corporation law and accounting law, forms the basis for the implementation of the corporate governance principles in stock corporation law. According to this, the board of directors and supervisory board are obligated to annually issue a declaration as to whether the DCGK has been complied with and continues to be complied with. During the course of the new version of § 161 AktG, the further obligation exists for listed companies to justify deviations from the recommendations of the DCGK in the declaration of compliance (so-called "comply or explain" principle).

2.3.2 Specific requirements for credit institutions and financial services institutions, as well as insurance companies

In accordance with § 25a Par. 1 Sentences 2, 3 of the German Banking Act (KWG), for specific divisions, the managing directors of credit institutions and financial services institutions are responsible for a proper business organisation, which must specifically include adequate and effective risk management. In accordance with § 25c Par. 1 KWG, notwithstanding the duties listed in § 25a Paragraph 1 KWG and in § 9 Paragraph 1 and 2 of the German Money Laundering Act (GWG), the institutions must have adequate risk management, as well as procedures and principles that serve the prevention of money laundering, terrorism financing or other criminal acts, which could lead to putting the institute's assets at risk. The minimum requirements for risk management (MaRisk (BA)) substantiating § 25a KWG individually prescribe the framework for the implementation of the institution's internal risk management, particularly the definition of strategies and the establishment of internal control procedures. § 64a Par. 1 of the German Insurance Supervision Act (VAG) contains the regulation for insurance companies that corresponds to § 25a Par. 1 KWG, § 80d Par. 1 VAG, § 25c Par. 1 KWG. § 64a VAG and § 104s VAG are substantiated by the supervisory requirements for risk management (MaRisk (VA)).

The examination of the adequacy and effectiveness of the risk management system to be established in accordance with the aforementioned legal requirements, as well as the assessment of the effectiveness of the measures for the prevention and discovery of fraud, i.e. the assessment of the effectiveness of the AFM, is a major task of the internal audit activity.

2.3.3 Specific requirements for public institutions

For public institutions, there are some specific regulations with respect to fraud. For example, the directive of the federal government (in accordance with Article 86 Sentence 1 GG [Constitutional Law]) on the prevention of corruption in the federal administration dated 7 July 2004 regulates that risk analyses must be performed for areas of work that are particularly at risk of corruption. No. 6 of the directive states that the task of corruption prevention can be transferred to the internal audit activity.

2.3.4 Legal risks with a lack of implementation of an AFM

In addition to the prevention and discovery of fraud, the implementation of an AFM has the purpose of avoiding damages claims by third parties against the organisation (external liability), on the one hand. On the other hand, the objective of the AFM is to avoid claims by the organisation against members of the organisation's management and the supervisory body (internal liability). Furthermore, damages claims by the organisation against third parties are intended to be safeguarded, in order to prevent (reputational) damage to the organisation. In the event of lacking implementation of an AFM, in addition to civil-law damages claims for compliance violations, liability risks under criminal law and administrative offence law also exist for responsible private individuals, as well as for legal entities/organisation. As an overview, the following risks can particularly result from this:

- **Risks under criminal law**
  The liability of responsible persons under criminal law can result from perpetration (§ 25 StGB) or participation in the form of incitement (§ 26 StGB) or aiding and abetting (§ 27 StGB) in conjunction with the respective criminal offence.

- **Risks under administrative offence law**
  In comparison to StGB, in accordance with § 14 Par. 1 Sentence 1 OWiG [Administrative Offence Law], administrative offence law makes no distinction

between perpetration and participation. For reasons of simplification, no assessment is carried out regarding the extent to which the respective contribution to the offence by the participant is regarded as perpetration or participation. In fact, the type and scope of the contribution to the offence form the basis for the assessment of the fine.

The central liabilities for legal entities are §§ 30, 130 OWiG. In accordance with § 130 OWiG, the owner of a business or company acts irregularly if he wilfully or negligently omits the supervisory measures that are necessary for preventing contraventions of duties in the business or company which relate to him and whose violation is threatened with punishment or a fine. § 30 OWiG extends these duties to managing directors, members of the board of directors, management staff and supervisory board members and attributes their breaches of duty to the company (so-called association fine). In the case of a wilful criminal act, the fine imposed on the company in accordance with §§ 30 Par. 2 S. 1, 130 Par. 3 S. 1 OWiG can amount up to one million euro. Furthermore, the profit generated for the company can be skimmed off by way of forfeiture or collection (§§ 73 et seq. StGB, 29a OWiG).

- **Risks under cartel law**

  § 81 Par. 4 Sentence 2 GWB (German Act against Restraints of Competition) also contains a practically important special regulation for cartel fines. With serious breaches of German or European law, a company or association of companies can have a fine imposed on it, which exceeds the basic amount of one million euro. The fine is not permitted to exceed 10% of the company's total turnover generated in the previous year by the company or association of companies. For the calculation of the total turnover, the worldwide turnover of all private individuals and legal entities, which operate as an economic unit, are used as a basis. The amount of the total turnover can be estimated.

3. TASKS OF INTERNAL AUDIT WITHIN THE AFM

The major task of the internal audit activity with regard to the AFM is to audit its accuracy, adequacy and effectiveness and to inform the bodies of the organisation – organisation management and supervisory bodies – about this on a regular basis.

A special feature for the internal audit activity results from performing suspicion-related special investigations on internal and external fraud. In this, the internal audit activity serves as a clarifying instance. Furthermore, based on its audit results, it serves as an impulse provider for the continuous further development of preventative measures in the business processes of the organisation. It uses the experiences gained from this to optimise internal audit-specific auditing approaches. This requires that the AFM audit activities are performed by internal auditors who have respective professional experience as well as AFM-specific expertise and personal skills. With this, the internal audit activity fulfils its preventive as well as clarifying task in the AFM.

For a proper business organisation, the clear allocation of all significant responsibilities is necessary. The aim is non-redundant performance of functions. All organisational units that participate in the AFM must be aware of their tasks, competences, responsibilities and methods of communication; transparency about this must prevail for all participants.

In order to clarify the allocation of functions in the AFM, the "Three Lines of Defence" model is explained as an example:

With this analysis, the AFM is an integral part of the internal control system. Objects for analysis of the AFM can be e.g. the following sub-areas:

- Compliance with legal and regulatory requirements (e.g. regarding money laundering),
- Security of IT systems and processes,
- Effects of personnel changes.

Organisational units that are at risk of fraud must be sufficiently sensitised to fraud risks. The necessary controls must be defined for the business processes and monitored by the business divisions **(1st line of defence)**. This requires a fundamental understanding of the relevant processes and the risks inherent in the process. In particular, the employees involved must be aware which concrete responsibility they have in structuring the business processes, as well as processing and controlling the business transactions.

In order for the implementation and performance of the control measures to be functional and effective, constant monitoring of the existing controls must take place by the monitoring functions. Thus, it must be ensured by a risk control self-assessment within the organisation that required controls with respect to the identified risks are actually performed. In addition to this, the person responsible for the AMF (AFM Officer) must implement and monitor the AFM in a functional manner (**2nd line of defence)**.

The internal audit activity **(3rd line of defence)** audits the task fulfilment of the business divisions and monitoring functions and thus the organisation-wide accuracy, adequacy and effectiveness of the implemented control procedures (system and process audit). Insofar as AFM Officers are appointed, the audit by the internal audit activity extends to their adequate fulfilment of duties. Tests of details and/or analytical procedures can be performed on a sample basis. They are necessary when the monitoring functions are not adequately administered or existing risks have not been covered so far. The internal audit activity can also be called in by the company management to consult on the

structuring and adaptation of the AFM and give recommendations for improving the AFM.

4. AUDIT STRATEGY AND APPROACH

When planning an audit of the AFM, the organisation-specific requirements and the AFM measures and processes based on these must be systematically recorded. These must be analysed under consideration of the inherent fraud risks and the fraud control risks and in respect of their practicability. In particular, the possibilities for the occurrence of fraud or criminal acts, respectively, and the resulting liability and reputational risks for the organisation must be included in the audit strategy.

The objective of the audit is to express an overall statement on the accuracy, adequacy and effectiveness of the implemented AFM and possible weaknesses based on the assessment of the fraud risks and the related AFM measures within the organisation. For this, a comprehensible and consistent documentation must be available which shows the organisational structure and process organisation of the AFM.

4.1 Auditing the organisational structure of the AFM

The basis for each audit is the organigram, which shows the individual organisational units that are involved in the AFM process. From this, the defined functions and responsibilities, as well as reporting channels, can be gathered based on role, position and functional description. These also include the rights and responsibilities of the individual persons involved in the AFM. The prerequisite for the definition is a sufficient allocation of personal and physical resources by the company's management.

The audit must particularly include organisational units besides the internal audit activity that are regularly involved, such as the AFM Officer, legal department, compliance, personnel, security, data protection and risk controlling. Within the organisation, the existing country-specific, product-specific, customer-specific, sales-specific and transaction-specific risks must be traceably allocated, each with respect to the responsibility.

In doing so, it must be checked whether an early interface analysis has been performed between the organisational units to avoid monitoring gaps regarding existing fraud risks and redundancies with the organisation-wide risk recording. The AFM must be integrated into existing risk management systems.

In order to ensure timely and organisation-specific decisions, a committee regarding fraud cases should be formed (e.g. compliance/fraud/steering committee) with the involvement of the relevant decision-makers of the aforementioned organisational units.

The audit criteria for the procedural structuring of an effective AFM is the organisation-specifically defined regulatory framework, which results from the written, fixed framework concepts. The mission statement formulated for the respective organisation and the ethical code of conduct are particularly worth mentioning, as well as the guidelines, manuals, process descriptions and work instructions based on this.

4.2 Auditing the process organisation of the AFM

4.2.1 AFM objectives

The starting point of the audit of the process organisation is initially the structuring of AFM processes as to whether the intended AFM objectives correspond to the objectives that were previously defined in the organisation-specific regulatory framework (e.g. avoidance of conflicts of interest, corruption). This requires that the agreed objectives are aligned with the organisational culture, the understanding of values and the role

model function of the organisation management (e.g. "Tone at the Top" and "Zero-Tolerance-Strategy"). In addition to the acceptance of the establishment of the AFM within the organisation, this includes the existence of an adequate risk culture and a respective control awareness. The audit procedures extend to the analysis of the organisational targets specified by the organisation management and code of conduct, the definition of the functions, competences and responsibilities of the respective organisational units, as well as their interdisciplinary communication and reporting channels. The acceptance within the organisation is promoted through incentive systems for rule-consistent behaviour and through sanctioning of misconduct.

In the following, the implementation of the organisation-wide defined AFM objectives is analysed in the individual organisational units in respect of their respective achievement of the objectives, e.g. on the basis of the so-called SMART criteria (**S**pecific, **M**easurable, **A**chievable, **R**ealistic, **T**imed).

4.2.2 Fraud risk identification and fraud risk assessment

The audit subject matter is the extent to which adequate risk recording is an integral component of the AFM and carried out at defined, regular intervals. The focus of this is the extent to which an organisation-wide, systematic and methodical risk identification has taken place. Relevant audit criteria are the information sources and criteria, e.g. business model, organisational structure, employee and customer structure, corruption index (CPI-Index Transparency International), country-specific and industry-specific information (press, Internet, public databases, etc.), as well as known cases of damage (internal/external) used as a basis within the context of the risk analysis.

Furthermore, it must be assessed to what extent it is ensured that current changes within and outside of the organisation have been/are being properly included in the risk identification (legislative changes, new business fields, patterns of action for loss cases that occur from fraud, employee changes, etc.) in order to continuously develop the AFM.

The methods of identifying the risks must also be included. Interviews, workshops, questionnaires, contract and document inspection, IT-supported data analyses and industry-specific background research on selected fraud risks come into question as such.

After the verification of the risk survey, the assessment of the fraud risks that has been performed by the AFM must be checked. The objective of this is the assessment of the prioritisation of the fraud risks that has taken place. In this respect, the assessment standards applied for the individual risks as well as the weighting criteria between one another and regarding their relevance for the overall organisation must be considered. The basis of the risk classification is a matrix-based presentation of the “loss amount” and “probability of occurrence” parameters. Subsequently, it must be checked to what extent an organisation-relevant risk categorisation has been carried out by the AFM on this basis. The objective should be a prioritisation of possible tangible and intangible liability consequences. On this basis, the organisational allocations of risks as defined by the AFM have to be assessed with regard to their usefulness.

As a result of the audit, the risk map established by the AFM is verified and any procedural and methodological weaknesses in the AFM process are identified.

4.2.3 Fraud risk control and risk limitation

In order to assess the degree of effectiveness of the AFM, the internal audit activity must determine whether and to what extent a systematic comparison has been performed between the identified fraud risks and the already implemented risk-reducing measures and processes (Fraud Performance Assessment). With this, it must be

included how the AFM assesses warning signals (Red Flags) particularly with identified high-risk areas and which measures have subsequently been initiated.

The audit subject matter is whether in the interest of a continuous improvement process, the determined fraud risks (so-called gross risks) have been compared with the existing control environment in the sense of all implemented risk-minimising measures – e.g. guidelines, internal controls system (4 eyes principle, separation of functions), competence regulations, AFM training courses, etc. - to determine the residual risks (so-called net risks).

The auditing of risk control comprises the extent to which a decision has been made regarding handling of the net risk in the form of possible additional risk-reducing and risk-avoiding measures (e.g. additional controls), outsourcing to third parties (e.g. insurance, sub-contractors) or risk acceptance. This decision must be checked with a gap analysis for its organisation-specific adequacy. In order to close identified weaknesses, improvement measures must be initiated on the basis of the recommendations made by the internal audit activity.

4.2.4 AFM communication

Furthermore, it must be determined to what extent the development and implementation of an effective communication concept that is adapted to the organisational requirements is a component of the AFM. This is comprised of target group-orientated and task-orientated training and sensitisation measures in the form of classroom or web-based training courses for the organisation management and the employees – as necessary – including a participation certificate. With this, it must become clear which AFM contents are communicated internally to which persons to what extent.

Furthermore, it must be ensured on a regular basis that the created training concepts and initiated training measures are continuously updated in respect of new employees, employee changes within the organisation or changed functions and organisational changes. In the same way, the updating is comprised of incident-related (current fraud cases) and recurring incidents (e.g. reminder of gift policy at Christmas). The selection of the communication channel (e.g. meetings, newsletters, leaflets, e-mails, intranet) must be defined on an organisation-specific and incident-specific basis.

The external component of the communication comprises the announcement of the specific requirements and rules for third parties, e.g. vis-à-vis customers and suppliers.

4.2.5 Informant system

A supplemental component of the AFM audit is the extent to which an organisation-specific informant system is implemented. A confidential communication system to obtain information is regarded as such, which opens up the opportunity for employees and third parties to report possible violations of internal and external regulations and laws anonymously. IT-supported processes, ombudspersons and internal and external whistleblower hotlines come into question as forms of informant systems to be established. The audit comprises whether the fundamental requirements for an informant system, e.g. anonymity of the informant, achievability, documentation of the report, reaction and initiated measures for incoming reports, are fulfilled.

4.2.6 Forensic special investigations

In the event of an existing initial suspicion in respect of acts that correspond to the organisation-specific definition of fraud, it is the task of the internal audit activity to perform the clarification of facts within the context of a forensic special investigation. During the course of a targeted approach, findings must be obtained that will stand up in court, particularly based on forensic interviews, IT-supported document analyses and

case-related background research. With the intended audit procedures, the requirements in accordance with the Federal Data Protection Act specifically in respect of employee data protection (BDSG) and possible participation rights of the works council/employee committee under the Works Constitution Act (BetrVG) and the Federal Law on staff committees in the public sector (BpersVG), respectively, must be observed.

Furthermore, country-specific legal framework conditions abroad (e.g. Foreign Corrupt Practices Act (FCPA), UK Bribery Act) must already be taken into account with the audit planning. Furthermore, a decision may need to be made about the inclusion of additional internal and external parties (e.g. criminal prosecution/consultation with the investigation authorities in case of pending proceedings, notification of the public relations department, appointment of external lawyers/audit teams, organisation-internal coordinated loss notification with the insurance company). In order to prevent possible additional losses for the organisation, in accordance with the AFM response plan (please refer to 4.2.7 below), incident-related, timely safeguarding measures (e.g. suspension of the suspected employee, initiation of measures for preliminary legal protection, blocking of IT access, distribution of employee-related operating resources (company ID card, PC/laptop, credit card, mobile phone, etc.)) are to be initiated in consultation with the other organisational units involved (particularly personnel, legal, IT).

In addition to investigating the accomplices, the goal is particularly to make a statement regarding the amount of the loss incurred or expected. Furthermore, the audit results have the purpose of continuously improving the AFM and the initiation of additional preventive measures.

4.2.7 AFM response plan

The audit of the internal audit activity relates to the extent to which the AFM comprises an organisation-specific response plan, which describes the systematic general approach in the event of fraud cases occurring or measures initiated by investigation and regulatory authorities. The aim of the response plan is to identify the organisational units to be involved in a fraud case, to ensure a short response time and to define the cooperation with the parties involved. For this purpose, the responsibilities, the time sequence of measures to be initiated, the consultation with the organisation management and possible external offices must be defined in the response plan, as well as the information duties of the organisational units involved in the process.

Furthermore, the adequacy and effectiveness of the response plan, the processes and communication procedures defined in the plan must be analysed and opportunities for improvement must be pointed out. The audit of the adequacy is specifically comprised of the evaluation of the target plan regarding consistency and whether it is known by the organisational units to be involved. The effectiveness should be examined on the basis of an ex post analysis of fraud cases that have occurred using analysable factors (e.g. response time, point in time of forwarding incident-related initial information, inclusion of all units that must be involved).

4.2.8 AFM reporting obligations

Another audit component for the assessment of the AFM is the extent to which the AFM has defined processes within the organisation in order to fulfil existing information and reporting obligations in a regular and timely manner. This is comprised of institutionalised communication to the organisation management and the supervisory boards, as well as the AFM Officer. This way, it is ensured, on the one hand, that they are fulfilling their legal supervisory and monitoring responsibilities and can respond accordingly in the case of AFM violations. On the other hand, the organisation

management and supervisory boards are informed about the condition and effectiveness of the AFM, including any suggestions for improvement, on a regular or incident-related basis.

In order to respond to current influences, internal (e.g. fraud case) and external (e.g. legislative changes) to the organisation, with relevant measures in an appropriate manner, incident-related communication is necessary.

5. REPORTING OF THE INTERNAL AUDIT ACTIVITY

The audit of the AFM is concluded with the preparation of an audit report. The recipients of this report are the organisation management and the management levels of the organisational units involved in the AFM process. The report is comprised of a summary presentation of the audit subject matter, the selected audit methodology and the findings gained on the current status of the AFM. In particular, an assessment of the accuracy, adequacy and effectiveness of the AFM must be made under consideration of the internal organisational and external requirements. In addition to this, necessary measures and recommendations must be formulated. These should be agreed with the respective responsible persons within the organisation in advance. Specific reporting requirements resulting from regulatory provisions must be observed. The timely implementation of improvement measures to be implemented must be monitored within the context of the tracking/follow-up audit.