

1. Systematic investigation approach at SCOPUS

The following article sets out typical phases of any fraud or more specifically, corruption investigations. However, even though the methodology can be applied all over the world, specific legal requirements and obligations must be taken into consideration. In principle, the following article describes our internal proceedings at SCOPUS when performing fraud or corruption investigations. By doing so, we rely on a remote workflow system, guiding us through the different phases and allowing to document all evidence and actions. The audit trail moreover ensures availability and integrity of respective data at any time.

2. Take action and document evidence

It quickly starts with immediate actions. Those measures not only have to be taken at the beginning of a special forensic investigation but can also be relevant during or after the special investigation has been completed. Most important, avoid further financial damage, limit the loss of reputation and to repatriate assets. It is crucial that the investigation team checks whether immediate measures need to be taken not only at the beginning, but also during the execution of the special investigation. The question of immediate measures must therefore be asked at the end of each relevant investigation step or whenever relevant new facts become known or have been finally processed. Even more important is the storage and documentation of the results and evidence in a reliable and safe data environment. Therefore, at SCOPUS we are relying on one of the world's leading providers of respective workflow software, storing all data in a high security data center in Switzerland.

Typical immediate measures are shown in box A Immediate measures after the conclusion of the special investigation and after the presentation of the results are generally no longer the

responsibility of the investigation team. This highly depends on the respective local law where the investigation is conducted. However, it is the task of the leading investigator to inform the recipient of the report of conceivable or necessary immediate measures and corresponding responsibilities and know about local regulatory requirements. Therefore, we at SCOPUS only work in cooperation with local experts, familiar with the respective law.



3. Communication overall

The topic of communication we at SCOPUS consider to be one of the most crucial topics overall. It is therefore necessary that those responsible define certain premises regarding communication before a specific special investigation. Based on a detailed sample case, the following must first be identified: possible internal and external communication partners to be identified; to determine communication responsibilities in the investigation team or in the company; determine the means of communication; to take into account various information content and thus levels of criticism; define rights, obligations and limits in communication; determine the time and frequency of communication.

It is therefore advisable to have a communication concept ready for special forensic investigations that answers essential questions about communication. It is intended to give the members of the investigation team the security they need to obtain and pass on information to

ensure that a special investigation is successful and to minimize the negative consequences of poor communication (we can provide you on request on our communication concept at SCOPUS). Ultimately, it is crucial that everyone involved knows who is allowed or must communicate with whom and when about which content. The communication partners can also be external to the company and may then have to be treated differently from the point of view of communication. Other external communication partners can be, for example, investigative authorities, external specialists, and other external parties such as service providers, suppliers, customers, or the media. Depending on the communication partner, the responsibilities for communication, the means of communication, the rights, obligations, and limits in communication as well as the communication content differ. For example, these points differ considerably when information is passed on to the public prosecutor, your own lawyer or a service provider commissioned to analyze the data. In addition to the persons responsible for the investigation or individual members of the investigation team, e.g., the corporate communications department, the legal department and the management are conceivable as communication officers. In any case, all members of the investigation team or persons otherwise notified of the special forensic investigation must know what their rights, obligations and limits in communication are. Ultimately, the goal must be to avoid communication deficiencies that can be observed again and again. Examples of this are shown in Box 2.

4. Rights and duties of those involved

It is necessary for those responsible for the investigation to identify, legally safeguard and communicate the rights and obligations of those involved in advance, e.g., using a sample case.

For such cases and due to individual legal requirements based on the countries where investigation take place, it is advisable to involve local law support. The specific situation of the company must also be considered. This means that the relevant jurisdiction and current legal practice must be considered as well as the company's internal regulations in the form of guidelines, company agreements and employment contracts, as well as operational practice. To avert negative consequences for those affected, those involved and the company, close and continuous cooperation with your own legal department or external specialists is recommended. The specific investigation situation often gives us rise to further questions about rights and obligations of those involved. In these cases, all members of the investigation team must be sufficiently sensitized to this issue to identify such need for clarification. Moreover, at SCOPUS we file interview notes and evidence and whenever possible, let documents being signed by the counterparty. Furthermore, the investigation team must have appropriate basic knowledge. For further questions, the investigation team must know their contact persons about rights and obligations of those involved. These contact persons, in turn, must be familiar with the subject of special forensic investigations and be ready to work out the optimal solution for the specific special investigation. This means that the contact persons may not go unreflective with an exaggeratedly cautious approach to the supposedly safe side and thus unnecessarily hinder the special forensic investigation, nor may the investigation team, for example, be exposed to the risk of their own criminal liability through frivolous assessments. Mention of relevant subject areas for which standards should be defined in the company.

1. Rights and obligations of those affected by the allegation and of the witnesses:

Obligation of employees to cooperate in clarifying company-related issues (depending on the hierarchy level); Regulation of the involvement of a lawyer in interviews; Duty of confidentiality of employees who become aware of the special investigation; Employee protection in the sense of protecting the suspect from damage to his or her reputation; Protection of the whistleblower (whistleblowing program).

2. Rights and obligations of the company and / or the investigation team:

Unrestricted active and passive right to information; Rights and obligations, e.g. in the context of a forensic data backup, during interviews and with regard to access to assets; Internal coordination and information obligations (among other things defined in a checklist for immediate measures); Obligation to report to supervisory bodies such as the audit committee; Possible reporting obligation to state supervisory authorities; Confidentiality of the members of the investigation team; Duty to protect the company from financial damage or negative reputational effects; Possible legal and regulatory reporting obligations in the case of definitive evidence.

As part of the internal investigations, the investigation team is generally less bound by legal requirements than, for example, the investigating authorities due to their criminal procedural obligations (e.g., no duty to instruct when interviewing the suspect). Against this background, it should be defined in the respective company whether and to what extent in the context of special forensic investigations e.g., the promise of advantages, the announcement of legal steps, deceiving about facts are permissible and wanted and whether the company is, e.g., about instructions The members of the investigation team are under no circumstances allowed to expose themselves to

criminal charges. A violation of rights and obligations by members of the investigation team can lead, among other things, to the following: Effects on the usability of evidence. Financial damage to the company, e.g., through claims for damages and fines; Negative reputation effect for the company in general and for the investigation team in particular; Personal consequences for members of the investigation team who may have committed criminal offenses.



5. Crisis management in white-collar crime

An allegation or suspicion of white-collar crime can trigger a crisis in a company. This is especially the case when critical information becomes public. To avoid or cope with a crisis, it is advisable to implement a crisis management system. This represents a methodical identification, evaluation, control and management or avoidance of crisis situations and thus enables an appropriate reaction to the most varied of crisis scenarios. Such a system includes the initiation of proactive and reactive measures:

Establishing a structure and process organization for crisis management or avoidance in terms of a definition of actors, processes and interfaces;

Implementation of a procedure for the internal preservation of evidence and clarification of the facts; Creation of a catalog of measures with regard to labor, civil and criminal law steps; Development of guidelines for cooperation in the event of official investigative measures; Immediate measures as part of crisis management; Support for the departments that are directly affected by official investigative measures, e.g. searches and interviews; Minimizing potential damage to reputation and loss of trust through appropriate internal and external crisis communication.

A crisis plan should be kept as a minimum component of a crisis management system (ask to see SCOPUS crisis plan for such incidents). In this, inter alia. the procedures and measures mentioned are presented and addressed in a structured manner. The basis of a crisis management system is an inventory of the potential crisis situations, which can be identified using a scenario technique, for example, and the course of which is anticipated. As a result, a crisis plan can be derived that clearly defines the necessary measures, standards of action, competencies, and responsibilities, defines a communication strategy and thereby contributes to a uniform appearance in terms of content and argumentation. Due to the complex and interdisciplinary nature of a crisis, it is recommended that a crisis team be set up depending on the situation. Such a crisis team, like the investigation team, should bring together different, relevant departments of an organization. Relevant departments are the legal department, the data protection officer, the communications department, the compliance officer, corporate security, and internal auditing.

6. Conclusion

The success of a special forensic investigation is shaped, among other things, by many cross-project phase aspects. These include the topics quality assurance, immediate measures, communication, rights, and obligations as well as

crisis management. If too little attention is paid to these issues during project implementation, this can have negative effects both on the project result and on the company, its employees and third parties have: If the possible need to carry out immediate measures is not constantly observed, e.g., at the end of a special investigation, a material claim against a contractual partner can be established, but it is unnecessarily difficult to enforce in the absence of a payment stop. If communication sovereignty is given up, there is a risk that the company will lose actual control over the special forensic investigation. In the most negative case, the content and the speed of the special investigation are then actually determined by the media. If the rights of the data subjects are not observed, this can - in addition to damage to the company's reputation - result in criminal liability for the investigating employees. If there is no crisis management system or at least a crisis plan, it cannot be ruled out that the occasion of a special forensic investigation leads to a crisis for the company, which in the most negative case can take on dimensions that threaten the existence of the company. The same applies if no use is made of an existing contingency plan within the framework of a special investigation. In addition to these few examples, several negative consequences of inadequate consideration of cross-project phase topics are conceivable. Due to the risks, it is the responsibility of the investigator to ensure that these aspects are dealt with comprehensively in a forensic investigation.

BOX1: Immediate action

Blocking access to IT systems, electronic data, paper documents as well as material assets, accounts, etc; Preservation of evidence with regard to IT systems and data as well as paper documents, etc., taking into account possible accomplices; Freeze directives, e.g. payments, assignments to suppliers (black listing); securing information and communication sovereignty; Examination of information and possible reporting obligations Initiation of immediate or precautionary access to the assets of the perpetrator and accomplice, e.g. arrest measures with regard to the suspect's liability.

BOX2: Communication deficiencies

Impairment of the work of the investigation team due to failure to communicate about its rights (e.g. unrestricted active and passive right to information); disclosure of non-coordinated / quality-assured investigation results; Oral communication of complex issues; Failure to take the necessary care when communicating using the fast and informal medium of e-mail; Misdirection of sensitive information; Communication that is not appropriate to the addressee or the context; Waiver of communication sovereignty without there being a need to do so (e.g. information to the media); Disregard of simple communication standards, such as confidentiality, courtesy and objectivity; Not timely communication, communication not taking into account the accomplice hypothesis Unsecured disclosure of information to third parties, e.g. to investigative authorities without a search or confiscation order or failure to anonymize data that may be legally necessary.

Ihr SCOPUS Fachkontakt

THOMAS CHRISTEN



t.christen@scopus-partners.com
info@scopus-partners.com