INguide

INTERNAL INVESTIGATIONS

TEİD
Etik ve İtibar Derneği
Ethics & Reputation Society

TEİD

Etik ve İtibar Derneği

Ethics & Reputation Society

teid.org
Mor Sümbül Street. Varyap Meridian
Business I Blok No: 1 D: 66
34746 Batı Ataşehir, Istanbul

INTERNAL INVESTIGATIONS GUIDE

TEİD Etik ve İtibar Derneği Ethics & Reputation Society

TICE Turkish Integrity Center of Excellence by @TEİD

ÖSKEM Özel Sektör Kolektif Eylem Merkezi

Internal Investigations Guide
INguide

Ethics and Reputation Society
Mor Sümbül Street. Varyap Meridian Business I Blok No: 1 D: 66
34746 Batı Ataşehir, Istanbul
0 (216) 580 90 34

Writers

Av. Altuğ Özgün	*Partner*
Av. Barış Kalaycı	*Partner*
Av. Begüm Biçer İlikay	*Lawyer*
Av. Birtürk Aydın	*Partner*
Av. Asena Aytuğ Keser	*Lawyer*
Cem Çelebi	*Data Analytics and Technology Consultant*
Av. Cihan Altuntuğ	*In-House Lawyer*
Dilek Çilingir Köstem	*Global Assurance Talent Leader & Turkey Assurance Leader*
Emre Çolak	*Ethics and Compliance Cluster Head*
Dr. Emre Doğru	*Founding Partner*
Av. Emre Kotil	*Lawyer*
Fikret Sebilcioğlu	*Managing Partner*
Av. Filiz Toprak Esin	*Partner*
Gizem Taştemel Dinçkan	*Assistant Manager*
Av. Gökçe Serez	*Lawyer*
Dr. Gökhan Yılmaz	*Head of Forensics, Compliance and Crisis Management Services*
İdil Gürdil	*Partner*
Merve Gündoğar	*Senior Consultant, Forensic Services*
Av. Merve Tüzmen	*Lawyer*
Av. Okan Demirkan	*Partner*
Senem Dal	*Internal Investigations Manager*
Sinan Çamlık	*Forensic and Compliance Director*
Av. Togan Turan	*Partner*
Av. Uğur Değirmenci	*Partner*
Umut Turan	*Ethics and Compliance Manager*

With the support and participation of:

Ali Cem Gülmen	*Research and Publications Director*
Dr. Bahar Karacar	*Project and Training Coordinator*
Gülçin Turasay	*Corporate Governance, Risk and Compliance Director*
Neslihan Yakal	*Secretary General*
Yiğit Bulutlar	*Forensic & Integrity Services Director*

Astellas Pharma

Cerebra CPAs & Advisors

Coca-Cola İçecek

CORPERA Consulting

Esin Attorney Partnership

EY Turkey

Gün + Partners

HDİ Sigorta

Keskin – Değirmenci Lawyerlık Ortaklığı

Kolcuoğlu Demirkan Koçaklı Attorneys at Law

KPMG Türkiye

Paksoy

Philip Morris Sabancı

PwC

Zorlu Holding

Letter from Chairman

Dear Stakeholders, September 2020

As the Ethics and Reputation Society, we are happy, proud, and excited to present the “INguide” Internal Investigations Guide to our esteemed companions.

It is safe to say that our association, founded in 2010, has reached a new stage in our journey, with more than 150 members now conducting work in the field of business ethics. We always feel the support and contribution of our TEID companions in our association activities, whose impact is getting stronger and expanding more each day.

We aim to continue our activities with an understanding based on scientific methods and data, with practical and applicable tools that are necessary for the world of business. In this respect, it is one of our most important goals to share the experiences of our stakeholders, each of whom are valuable in their own sectors, with all levels of our business world. In this direction, our new guide has been prepared with the efforts of the Internal Investigations Working Group, one of the working groups we have established under the structure of our Association. We see this guide as one of the tools that will turn the Ethics and Reputation Association into a reference and training point in our country.

We further hope that our guide will become a guiding light for employees working in the fields of ethics and compliance, in companies throughout today’s business world, where awareness is always growing of the issues of effective management of ethics and compliance risks, honesty, accountability, and transparency.

While presenting our guide for your appreciation and evaluation, we salute you with love and respect.

Yours respectfully,

Ertuğrul Onur
Chairman of the Board
Ethics and Reputation Society

FOREWORD

Internal investigations are often difficult and complex for companies. The non-routine process, privacy concerns, possible legal processes, internal problems due to actual or alleged unethical or illegal violations, possible loss of reputation are just a few of the factors causing the process to be challenging and complex.

Internal investigations, by their very nature, involve accusations or allegations against employees in the institution. Unless these investigations are carried out meticulously, legal problems and unexpected complications may arise for the institution. Moreover, internal investigations are often initiated without prior notice, and they are often conducted during periods of high stress at the institution. Internal investigations may require a crisis management process, especially when action is taken immediately after detecting abuses or allegations of violations.

Despite these many challenges, an internal investigation is a necessary and healthy process, especially for the institutions that have an ethics and compliance program and make these topics their priority. A well-conducted internal investigation identifies the sources of the loss of the institution, addresses the damage, and prevents any damage that may be faced in the future through the elimination of the control and process issues that have caused the abuse. In addition, it helps the institution defend itself successfully against legal processes initiated by any employees whose employment is terminated.

The Internal Investigations Guide was prepared by the “Internal Investigations Working Group” established under the roof of the “Ethics and Reputation Society” in line with long-standing activities and professional experience. With this guide, our aim is to share practical information on the issues that need to be taken into account in order to carry out effective and efficient internal investigations. These processes constitute one of the most critical stages in the ethics and compliance initiatives of institutions.

We would like to thank the members of the Internal Investigations Working Group for their great commitment in the preparation of the guide, and we hope that this guide will serve you well.

Fikret Sebilcioğlu, Executive Board Member at TEID
Av. Filiz Toprak Esin, Executive Board Member at TEID

Table of Content

NOTES

Section 1
PLANNING OF THE INTERNAL INVESTIGATION

1.1 Definition

One of the main steps in the process of detecting actual or suspected legal or business ethics violations in organizations is internal investigation. Internal investigations are critical for determining the outcome of the violation as well as being a process that must be managed with due diligence in terms of the balances it involves.

Today, many definitions have been made which highlight common aspects of internal/occupational frauds but also reveal different aspects of these. According to the Association of Certified Fraud Examiners (ACFE), internal fraud is defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets". It should not be forgotten that internal frauds that result in detriment of the employer is a risk that threatens organizations to a great extent.

Organizations conduct internal investigations in order to determine actual or potential loss and damage or to investigate the reality of an allegation. Internal investigations are conducted in order to determine whether the actions and behaviors defined as misconducts in their internal documents are present, to determine the dimension of the misconduct (if any), and to identify the ways to eliminate these loss and damage by taking suitable measures or by determining actual or potential loss and damage. In addition, internal investigations can be defined as a set of processes, which include collecting information and documents from relevant sources within the scope of examinations and researches conducted in order to prevent reoccurrence of these acts, and preparing reports to inform the relevant units about the conclusions and results reached.

Investigation process mainly consists of the following steps:

- Receiving and analyzing the notice,
- Planning the investigation,
- Collecting evidence,
- Analyzing and documenting the evidence,
- Conducting investigations,
- Preparing investigation report,
- Conducting disciplinary process and identifying corrective actions.

Upon making the decision to conduct an investigation as a result of receiving and analyzing a notice, the organization focuses on how to conduct the investigation in the most effective and efficient way. At this point, planning stage is a highly critical process. Investigation team is formed during planning stage, and factors for investigation strategy are determined. Afterwards, the interviews conducted in order to collect evidence, obtain information or confessions and the evidence obtained as a result of the investigation process are analyzed, these evidences are documented, and an investigation report is prepared. In the event that the misconduct is proven after the final stage, disciplinary process is initiated and corrective actions are identified.

Two Sides of Internal Investigations	
Not routine.	Increases trust.
Requires cost and time.	Improves Speak Up culture.
May cause damage to the organization.	Enhances the efficiency of ethics and compliance program.
May cause employee dissatisfaction.	Conveys powerful messages to employees.

1.2 Planning of the Internal Investigation

Carrying out the internal investigation planning using a standard document containing necessary details would be useful in terms format, guidance and fictional tracking. In this context, it can be recommended to conduct an internal investigation plan including but not limited to the following matters:

- The date on which the case is notified
- The first person to whom the case is notified
- Planned completion date for the investigation
- Source person for the notice (name, title, relation to the organization.)
- Confidentiality and conflict-dispute conditions required by the case
- How the whistleblower knew about the misconduct and the evidence possessed by them
- Case category
- Persons to be notified in the organization's management
- Immediate measures and action plan (Especially in the event of threat, physical damage, critical data and evidence that must be protected, and explicit risks.)
- Investigation team
- List of documents and evidence to be examined (Their responsible persons and relations to the case must be specified.)
- Digital forensics or electronic investigation needs
- List of people to be interviewed
- Key questions to be asked during interviews
- Determination of the country laws to be implemented
- Evaluation of the legal privilege to be subjected to based on the nature of the organization/case

However, investigation planning must reveal an "action" plan with details meticulously considered beyond a standard documentation. For this, the contents listed above must be based on experience in a conscious way.

It would not be wrong to say that even though the breaches subject to investigations are the same or similar, each investigation is unique. The reason for this can be listed as conditions of breach, root causes and people involved in the action. Therefore, each planning requires a work specific to the case. This requires care and diligence in terms of method.

1.3 Matters to be Considered during Planning of the Internal Investigation

1.3.1 Duration

The duration between the notification of the case and the commencement date of the investigation must not be long. It would be suitable if it is long enough for planning and assuring key evidence and/or evidence that may be destroyed.

The allegation subject to the investigation must be examined in detail. Sometimes, examination in multiple categories can be required. In such cases, required resources may also vary.

1.3.2 Subject

Accurate legal characterization of the investigation's subject will play an important role for determining the investigation strategy accurately as well as determining and implementing the urgent actions to be taken. In this sense, it must also be considered whether the allegation subject to the investigation has a scope to create liability to notify the crime as well as the necessity to take action in order to take internal measures such as discharge and limitation of powers as well as external measures such as determination of evidence, temporary legal protection applications, seizing assets, etc. immediately.

Conducting the investigation with or without announcement must be decided based on assessment on the nature of the case, persons involved and destruction possibility of evidence.

1.3.3 Legal Status

When a notice that may expose the organization to internal investigation process is received, legal consultancy service is received from in-house or independent attorneys in general when determining an action plan, the attorneys prepare their opinions on the investigation subject in this sense, and therefore can exchange correspondence. Such communications and exchanges between the attorney and their client are under "attorney-client" confidentiality protection as a rule, and "attorney-client confidentiality" includes not only the investigation process, but also the legal consultancy provided before the investigation.

The importance of this protection becomes evident especially when judicial or administrative authorities are involved. As a matter of fact, documents, opinions and correspondences under attorney-client confidentiality may fall outside the scope of search and seizure decisions within the scope of the right to defense. However, it should be noted that this protection is not an absolute protection. Communications such as opinions, correspondences, etc. that are prepared by company lawyers or independent lawyers, but are created for the purpose of continuing or hiding the breach subject to the notice and not covered by the right of defense will not benefit from attorney-client privacy.[1]

1.3.4 Investigation Team

Conflict of interest examination should be conducted while forming the investigation team. Regardless of their seniority, one of the elements that lies at the basis of the relationship between the employee and the employer is "trust", which is based on the fact that the employee will only protect the interests of the employer and avoid all kinds of processes and relations that aims to or may result with personal benefit and would be against the employer's interests. In cases where this factor is violated by the employee and there is a suspicion that such a violation may occur, a conflict of interest would be present.

As a consequence, the interest that needs to be protected in an internal investigation is not the interests of the investigator, directors, or those with whom they are associated, but the interest of the company/organization. In order to conduct a healthy and reliable internal investigation process, all factors that may cause conflict of interest must be taken into account and prevented at the very beginning of the investigation process.

Leader of the investigation team must be a good coordinator who is competent in investigation field. Qualification of the team leader is also important in terms of guidance since not everyone in the investigation team is an expert investigator.

When forming an investigation team, number and profile of investigators must be planned based on the needs of the case. However, the quality of investigators is also important.

Following matters must be considered when identifying the investigators:

- Investigators must be experts in the subjects to be examined under the case (finance, company systems and field knowledge, etc.).

- While forming the investigation team, care must be exercised in order to not select people who may have a direct or indirect relationship with the events under investigation, or who have close relationships with those to be involved in the investigation scope. For this, first of all the scope of the investigation must be carefully determined, the actions and activities that will be subject to the investigation and the people who may be related to them must be determined completely and accurately. In this sense, there must be no subordinate relationship between the team members and the persons to be interviewed during the investigation.

- If necessary, outsourcing needs must be determined for the team (attorney, translator, forensic accountant, forensic IT specialist, etc.). Receiving support from external consultants may be the healthiest method to minimize the possibility of conflict of interest. However, when making this choice, the relationship and closeness of the chosen consultant person or company with the company must be taken into consideration; for instance, care must be exercised in order to make sure that the external consultant to be chosen has not previously provided services, opinions, etc. on the case subject to the investigation.

- Measures to prevent conflict of interest must be taken at the very beginning of the investigation, and necessary steps must be taken to ensure continuous surveillance and elimination of conflict (if arises) throughout the investigation. tespiti hâlinde ortadan kaldırılması için gerekli adımların atılması gereklidir.

[1] See Section 9.1 Attorney and Client Confidentiality for detailed information about the subject.

Definition and scope of powers is important for the ones who join the investigation team externally. In this way, access can be provided to required information and documents. This authorization can be provided with methods such as board decision or approval of international companies for investigations to be conducted with their participation pursuant to laws and company rules.

1.3.5 Analyzing the Data

During an internal investigation, actions which result in processing personal data such as examining company computers, phones and e-mails or recording audio or video during interviews conducted within the scope of the investigation can be performed. Therefore, during the planning stage of such an investigation, it must also be evaluated how to process these data within legal limitations and how to secure the processed data as well as taking required measures.

If the company has already adapted its personal data policies in line with its obligations within the scope of "Law on Protection of Personal Data (LPPD)" and completed relevant clarification and receiving approval obligations, no additional obligation for providing clarification or receiving approval would be necessary for the data to be processed only for the investigation to be conducted in most cases. However, if this adaptation has not been completed, it is important to determine the obligations to be fulfilled within the scope of LPPD and to make relevant preparations during the planning stage.

In the event of receiving services from independent consultants during internal investigation processes, it will be important for the company to sign protocols with these consultants as the data controllers which determine the limitations of data processing and ensure security in terms of fulfilling this obligation as the party having the responsibility to ensure safety of personal data to be processed

1.3.6 Planning of Interviews

Following matters can be discussed about the interviews to be conducted during the investigation process:

- First of all, current organizational chart of the organization must be examined and the people to be interviewed based on the allegations must be identified based on their positions in the organization as well as case/evidence outcomes.

- It must be determined who should be included in each interview.

- It is ideal to have two investigators present during interview.

- Special conditions must be known and cultural differences must be taken into consideration, especially based on the geography in which the investigation takes place.

- Some employees (especially the whistleblower) may request confidentiality in relation to the file. Therefore, interviews may be conducted outside the organization.

- Some cases can require interviews with third parties. An appointment must be made to meet with these organizations/persons and the meeting place must be determined in advance.

1.3.7 Collecting Evidence

Collecting evidence is one of the most critical stages of internal investigations. Effectiveness of this process can only be possible through healthy and thorough planning of the procedures to be implemented at the beginning of the work. Following issues regarding the evidence collection process must be considered at the planning stage:

- It must be ensured that evidences and other required information are collected. These are as follows:
  Bunlar:
  - In-house documents
  - Forensic informatics and other electronic investigations (e-mail, hard disk images, company entry-exit records, phone records, camera records, GPS reports etc. of suspects)
  - Public information including social media
  - Information and documents obtained from third parties

- Required legal opinions must be obtained in advance in order to avoid legal violations during the evidence collecting process, even if it is involuntary.

- It can be inconvenient to use the originals of the information and/or documents since these may be damaged. Therefore, it is recommended to prepare copies (electronic or physical) during planning stage.

1.3.8 Measures

There are certain important measures to be taken at the beginning of the work in order to conduct health internal investigations. Some of these include the following:

- If there are people who are required to be removed from the organization at the beginning of the investigation, these people must be determined, required preliminary works must be conducted with Human Resources, Legal and Data Processing departments, and measures must be taken.

- Logistic planning must be conducted independently from the department to be investigated.

- An internal and (if required) external communication plan must be prepared in relation to the investigation. If necessary, employees must be informed about the process -without details- and asked to assist to the process.

NOTES

Section 2
COLLECTING THE EVIDENCE

2.1 Organizational Policy and Procedures Required to Collect Employee Data

Internal investigations can be triggered by different reasons such as a notice on the violation of laws or business ethics rules, risk assessment processes or internal audits. Organizations generally carry out internal investigations when they encounter "unusual problems".

In order for the whole process to be conducted in a lawful and fair manner, organizations must be proactively prepared for this process and inform their employees about these processes in advance, provided that they do not violate the confidentiality of the investigation. Senior management to assign the internal investigation duty to a department in the organizational structure as well as the department employees who are authorized and competent to conduct these internal investigations must determine in which geography and which sector the organizations carry out activities and which covenants are given by other organs of the organization to employees, society and environment as a point of origin.

Adapting national and international regulations as well as sector and work branch-based regulations would be helpful to overcome many problems during internal investigations. In addition, it is also of critical importance to assess the legal acceptability of all evidences collected throughout the investigation process in the.

The employment contract regulating the liabilities and obligations between the employee and organization must include policies sorted and enforced as subjects clarifying the rules to be adhered by the employee and the employer organization throughout the employment term of the employee. The documents to be signed between the employee and employer organization according to these policies as well as their properties will be described in the next section.

As described above, each organization will vary based on their areas of activity, targets based on their vision and the preferred corporate identity, however, essential policies are as follows:

- Confidentiality, storage and destruction of personal data policy,
- Anti-bribery and anti-corruption policy,
- Fair competition policy,
- Code of conduct policy,
- Conflict of interest policy,
- Data security policy,
- Gift and hospitality policy.

All of these policies will bring the opportunity to act on the constitutional and international human rights level for employer deputies in the daily workflow and those conducting the investigation during the internal investigation phase as well as an obligation to comply with all these.

These statistical data also provide us with the reason why policies that are emphasized are essential. When the 7 most frequently used methods for hiding fraud are examined, the most common ones are as follows;

- Creating forged documents,
- Altering physical documents,
- Establishing fraudulent transactions in the accounting system,
- Altering electronic documents and files,
- Destruction of physical documents,
- Creating forged electronic documents and files,
- Creating forged journal entries,

In this context, the sources from which data can be collected as well as collection methods and integrity of data will be detailed in following sections of the guide.

Regardless of the level, when an employee joins an organization, their duties and responsibilities as well as company policies and procedures must be explained to them. This integration can be done in a conventional way firstly, with an accurately determined orientation process in terms of contents. Afterwards, compliance must be maintained with special trainings designed according to their duties.

2.2 Documents to be Signed Between the Workplace and the Employee in order to Collect Employee Data

During internal investigations, various data of employees can be collected and examined in order to better understand the issue and to use it as evidence in a potential case. Considering that today's written communication is mostly done by e-mail and instant messaging, the information on the company's laptops, tablets, computers and phones must be collected during the internal investigation. These collected devices are processed by the forensic IT teams by the methods described below and made ready for examination. Also, physical documents such as employee notes, agendas, etc. can be collected and examined, as they may contain elements that may constitute evidence or illuminate the subject. Before these documents or devices are collected, the most important question that must be asked to the authorization persons managing the investigation is whether there is personal data in the document or devices. Because, after the LPPD entered our lives in 2016, organizations were accepted as data controllers because they process their employees' personal data and therefore faced many obligations. In the usual flow of life, it is very likely that there is personal data of the employees in the laptops, tablets computers and phones used in the daily working environment.

First of all, it must be stated that personal data cannot be examined without explicit consent of relevant persons pursuant to the general rule of our current legal system. However, there are some exceptions to this rule. These exceptions are listed in article 5 of LPPD. In general, to the extent that conducting an internal investigation is required for legitimate interests of the data controller, "It is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed" according to clause (f) of article 5 can be an exception. Alternatively, if the organization must conduct an investigation within the scope of certain liabilities, this can also be under the exception stated in clause (ç): "It is necessary for compliance with a legal obligation which the controller is subject to". In the event of these conditions, the data controller organization can process personal data without obtaining explicit consent of the relevant employee.

Even though it is possible to conduct an internal investigation without requiring explicit consent due to the conditions of the process – if certain actual conditions allow – it is also compulsory to fulfill other liabilities of LPPD before collecting documents and devices containing personal data.

2.2.1 Providing Clarification Text[2]

Pursuant to article 10 of LPPD, data controller or the person it authorized is obligated to inform the data subjects about for what purpose and how to process the data. Clarification text must include the following factors:

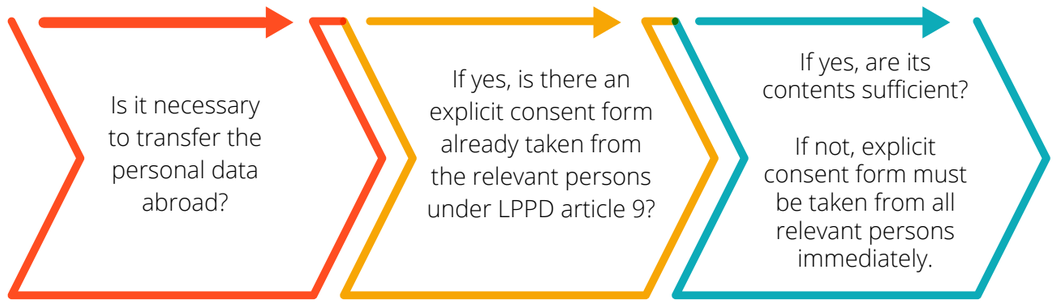
- The identity of the data controller and if any, its representative,
- The purposes for which personal data will be processed,
- The persons to whom processed personal data might be transferred and the purposes for the same (In this context, it is not necessary to specifically name a person. It can be sufficient to understand who are meant in general. For instance; Shareholders, suppliers, third persons from whom we receive legal services, etc.)
- The method (For instance, examination of physical files, examination of electronic records or automatic and manual examination) and legal cause of collection of personal data (for this, an appropriate legal reason from the ones listed in article 5 of LPPD must be written.)
- Other rights set forth under article 11 of LPPD (A general reference to article 11 of LPPD can be provided without listing all rights in the article 11, and "The person has the right to apply" can be expressed in relation to the rights here.)

Organizations which examine personal data without providing their relevant employees with a clarification text will be imposed an administrative fine between 5.0000 TRY and 100.000 TRY.[3]

To summarize, before starting an investigation, it must be investigated whether the organization has previously provided a clarification text within the scope of LPPD. If so, it must be determined whether the content of this text complies with the criteria specified in LPPD. If the no clarification text is provided, a text must be prepared in the abovementioned content and this text must be presented to the employees. These texts must be provided to the employees in return for signature in order to prove that the text is provided to the employees when necessary in the future.

2.2.2 Obtaining Explicit Consent Form for Transferring the Data Abroad

Particularly international organizations may have to transfer data to the country where their headquarters is located during an investigation, or their service provider to process the data may be in a foreign country. Therefore, the personal data to be examined may need to be exported abroad. In order for personal data to be transferred abroad, the explicit consent of the person concerned is required in accordance with Article 9 of the LPPD. In this consent text, the country to which the data will be transferred must be specified. There is no need to obtain consent form from all employees. It will be sufficient to obtain a consent form only from the relevant persons whose personal data will be transferred abroad. In the event that the internal investigation expands, it will be necessary to obtain explicit consent from those employees if the data of other employees must be transferred abroad.



[2] See section 9.2 Protection of Personal Data for detailed information.
[3] These amounts are applicable for 2020. Fines vary depending on annual revaluation rate

2.3 Resources to Collect Data

Today, there are many different data sources due to the digital processing of data. For an examination to be carried out, determining the data sources completely and completely, including them in a format suitable for the examination and performing the examination in accordance with the law are among the most important issues.

Main data sources are listed below:

- Corporate computers that employees have access to (desktop, laptop, server)
- Mobile phone/smartphone
- Portable data storage devices (USB disc, external disc)
- Financial records
- E-mail server
- Internal and external company applications
- Active directory logs
- Firewall logs
- İnternet logs (5651, proxy)
- Application logs
- Common corporate areas
- Cloud storage areas
- Login-logout logs
- Camera images
- Telephone call records
- GPRS
- Personal files
- Social media posts

Data sources may differ depending on factors such as workplaces of the organizations, the information systems, software and the technological infrastructures they use.

2.4 Data Collection Methods

Before the digital data is collected, data sources that are under the responsibility/control/access of relevant persons must be determined. Otherwise, the data to be processed may include information independent from the subject and certain data may be left out.

The method to be applied when collecting the data must be determined according to the type of data. The first step suggested for collecting the data is determining whether a hard disk image will be acquired. Acquiring the hard disk image is important for the acceptance of the user's computer by the Prosecutor's Office and its recognition as unaltered evidence.

The data is written on the disk surface in binary bit order (0-1). For this, the polarity of the molecules on the disc surface is altered by using magnetism. Disk image acquisition means transferring the same bit sequence on the disk into a disk/medium.

2.4.1 Main Data Collection Methods

Acquiring Static Images

The primary method that can be applied for copying the information on the internal and external disks of devices such as computers and laptop is to acquire a "static image". If the device to be imaged is an internal disk, it must be disassembled and used with data writing protection software/hardware, or data writing to the disk must be prevented by using certain software during the boot-up phase when turning on the computer. Volatile data (memory, certain network logs, etc.) cannot be accessed in this image type. The aim is to acquire the exact image of the disc. It is also possible to restore the deleted files in the images acquired with this method under certain technical conditions.

Acquiring Live Images

In this image acquisition type, a copy of all data, including volatile data at the operating system level, is taken since the image is taken while the computer is on. Live image acquisition must be preferred in cases where it is not possible to obtain a static image since it is acquired through the computer's operating system.

Storage Area

In order to collect the data in storage areas, the type of storage area and its structure must be determined first. Specific examples of storage areas are listed below:

- Physical-Portable discs, DVDs/CDs, etc.
- Digital-Common areas, file servers, cloud systems, etc.

The critical issue for the data to be acquired from these areas is whether there is only data related to the relevant person in the area. Data on portable devices that are used by a single person can be copied using image acquisition methods. For other data, related files can be copied by applications such as robocopy etc. In this case, it is recommended to keep the originals of the files unaltered, if possible.

Logs

One of the resources that may be used for examinations are log files. These files are:

- Windows - Event, audit, security
- İnternet - Firewall, proxy
- Active directory/Exchange

Log files must be stored in a way that cannot be altered, and the examination must be made on the copies of files or through the interfaces of the systems where the files are stored in order to preserve the originality of the records.

2.5 Ensuring the Integrity of the Collected Data

The first thing to do after collecting the data is to ensure the integrity of the data collected. At this point, it must be ensured that:

- All data are included in the examination,
- Data which is not relevant to the investigation are not included,
- Data obtained from data resources are collected with suitable methods,
- Collection steps are appropriately recorded when collecting data (Evidence chain is recorded and preserved),
- Copied data and data at source are compared and verified in terms of consistency when collecting the data (Hash control, etc.).

2.6 Making the Collected Data Ready for Examination

During the preparation process, preparation must be made in accordance with the type of data collected and the examination to be carried out on the data. Examination methods to be applied for structured data such as financial records, log records and examination methods to be applied for unstructured data such as word, excel, etc. documents or e-mail correspondence will be different.

For this reason, the first thing to do is to separate the data according to the examination method. In the next step, it must be ensured that the environments suitable for the analysis of the separated data (software, hardware) are ready to use or can be installed as needed.

Key issues to be considered here can be listed as follows:

- While analyzing the data, the storage space needed must be available,
- Licenses of software to be used in the examination process must be active,
- Appropriate number of licenses for examination must be available,
- The data to be used in the examination process are must be backed up,
- No alterations must be made to the data.

If the data will be obtained by acquiring physical images of computers or telephones, the chain of evidence must be established in a healthy and appropriate manner when these computers and telephones are taken from the employees. Otherwise, claims can be encountered before the court, such as the data obtained by the organization has been changed to be against the employee by the organization. Acts that could violate personal privacy during the examination process must be avoided.

2.7 Data Analysis Methods and Applications That Can be Used for Analysis

2.7.1 Structured Data

Different methods can be applied according to the data type in the analysis of structured data. Main analysis methods can be listed as;

- Qualitative data analysis
- Quantitative data analysis
- Relationship analyses
- Parametric analyses

Analysis method must be determined depending on the type of data and the conclusion to be reached.

For these analyses, many different licensed and open-source software can be used such as MsSQL, Postgre SQL, MS Excel, SAS, SPSS, Knime.

2.7.2. Unstructured Data

The current examination software that can be used in the process of unstructured data analysis enables the creation of keywords using smart operators (AND, OR, etc.) and examination of the data by filtering with keywords. In this way, it will be possible both to exclude the issues outside the allegations and to filter the relevant data among millions of data. Software such as Intella, Relativity and Nuix can be mentioned in relation to the issue as well as many other products that can be preferred. It is recommended to use demo versions of the software be tested or to conduct POC (Proof of Concept – testing of the software by the user before purchasing) in order to select the most appropriate software according to the infrastructure of the organization.

2.8 Issues to be Considered by Employer and Employees During Relevant Processes

If the findings obtained as a result of the internal investigation constitute a suspicion of crime, the subject will turn into a criminal complaint, and therefore a criminal case. If it violates the workplace rules and the provisions of Labor Law, it can be transformed into certain legal processes, especially termination of the employment contract by the employer and the reemployment claim filed by the employee whose employment contract is terminated. On the other hand, attacks on personal rights and/or interventions to privacy would also be the subject of lawsuits before judicial authorities. Although it is anticipated that all of this can happen, it will result depending on whether the person or persons conducting the internal investigation are acting with these steps in mind, as mentioned in the previous section. Therefore, there are certain rights "that expect respect". These rights can be listed briefly as follows:

Bu haklar kısaca şu şekilde sıralanabilir:

Thus, pursuant to article 132 of Penal Code of Turkey, "Disclosing the contents of the communication to only one person is sufficient for the disclosure."

In the very first lines of this section, we have mentioned that internal investigations are not routine, are high cost and will create certain internal damages. In this case, the person or persons conducting the internal investigation must also be asking themselves the following questions:

- Considering there is a right to be forgotten in the law, will the reputation of the persons concerned be damaged in the organizational examples?

- Can we apply similar sanctions for the same case?

- What did we commit to at recruitment, what are we doing now?

- Aside from the commitments made to the employee, will our publicly announced corporate identity and our corporate goals determined accordingly make our current actions appropriate?

Whether or not these questions are asked, potential business cases, commitments made, policies enforced, and subsequent internal investigations and decisions made are subject to supervision of the Supreme Court.

Section 3
Interviewing Techniques

3.1 Interviewing Principles

It is possible to summarize questioning principles under six main headings:

- Having a good command of the subject
- Complete review
- Confidentiality
- Impartiality
- Effectiveness, and
- No involvement in management

In accordance with these principles, it is necessary to detect violations by minimizing the depreciation of the person interviewed without suspicion. Having knowledge as wide as possible during the interviewing phaseis important for the investigation. It is highly necessary to have complete documents and information to be obtained from the individuals to be interviewed, to obtain the findings to resolve the case as well as their accurate evaluation. Investigators must maintain their impartiality and try not to prove the allegations or defend the suspects during the investigation. During the investigation, the principle of confidentiality must be preserved. Since efficiency is one of the important principles, it is essential to have a good command of the subject during the interview process with a serious, authoritative personality.

The investigator's self-confident and severe attitude will have a psychological effect on the interviewee and also increase his/her respect to himself/herself and the subject. Again, one of the important points is that the management of the related unit or process must not be interfered with throughout the task.

During the interview, it should be noted that the relationship between the employee and the organization, which is based on mutual trust should not be damaged. It is critical to protect and preserve the legitimate interests of the organization and employees while applying interviewing techniques.

In order to achieve the most accurate method in the process, a scenario that includes the stages of the case from investigation of the scene, obtaining preliminary information from witnesses to review the current documents as of the beginning of the act should be created. It is necessary to try revealing the results and evaluate the situation by drawing conclusions from the scenario created about the occurrence of the case.

3.2 Interview Process

An investigator should take into account the following items throughout the interview.

•Being a good listener and focus on the conversation.

- Not being accusative and tough.
- Speaking confidently without hesitating.
- Asking questions with a clear and understanding language, adapting a kind and patient attitude.
- Applying technical methods such as follow-up questions, cross-examination in order to clarify the issues subject to the interview.

During the interview, the person should be allowed to meet his/her personal needs (water, food, toilet, air, etc.), and it should be noted that restriction of such needs in the interview may lead to unlawfulness and negatively affect the results to be obtained from the interview. It should be stated that the person can end the interview whenever he/she wants, and if requested, the process can be carried out with a legal consultant to allow the interviewee to provide answers with support of a legal consultant.

The interview should be completed within a reasonable time and, if possible, recorded in written. During the interview, actions that may constitute legal contradiction such as physical and psychological violence, psychological pressure, harassment and discrimination should be avoided.

Another issue to be considered during the interview process is the venue, that is, the physical area where the interview will be conducted. It must be ensured that the area is quiet and has adequate privacy, meets the minimum conditions (sufficient light, sufficient ambient temperature, sufficient ventilation, no physical deficiencies such as odor, humidity, etc.) to conduct the interview in a healthy way. It should be ensured that all the participants sit at the same level with each other and that there is no long distance between them.

3.3 Main Issues to be Considered During the Interview

It is appropriate not to start the interview directly on the subject of dispute but rather conducting a short preliminary interview in order to reduce the stress of parties will be adequate in order to proceed the communication in a healthier way.

Although it is convenient to use the cross-examination technique in order to clarify the event that is the subject of the dispute, the interview should be conducted on the principle of confidentiality in general. In case of choosing the cross-examination method, the people participating in the interview should be enabled to answer only the questions asked by the interviewer, mutual dialogue or discussion of unrelated issues should be avoided. In this regard, in case of conducting interviews with different parties of the dispute at the same time, it would be appropriate to limit the issues to be discussed with each individual to a specific purpose and scope. It should be ensured that interviewees explain the subjects they directly witnessed, and avoid discussing information that are irrelevant or obtained only from third parties based on rumors. In this process, reactive discourses should be avoided and the interview should be kept under control in terms of emotions.

3.4 Techniques

3.4.1 Determining Strategies

In the event that the existing evidence is not based on concrete and material foundations, it would be more appropriate not to direct the interview to admission. Because, additional information and evidence to be obtained as a result of these interviews may cause the investigation to evolve in different directions. In this regard, it is of great importance that the characteristics of each case are discussed differently and that the concrete information and evidence available are pre-evaluated by the interviewer and the interview strategy is shaped accordingly.

3.4.2 Admission/Confession

The interviewer should ensure that as many explanations as possible are provided by the other party. In this respect, the active party should be the party to whom the questions are asked during the interview. The interviewer should listen to the explanations and should share the information that he/she obtained before starting to the interview and ask the other party to confirm or disclose.

It is noted that the evidence at hand is based on concrete and material findings will play an important role in admitting the dispute. The interviewer should always has an objective attitude when asking questions, not diverge from the evidence obtained before the interview and avoid asking questions that he/she does not know the answers.

In this process, the method of asking repetitive and follow-up questions can be preferred in general, as well as clarification of the subject in dispute with the cross-examination method. In case of acceptance of the subject in dispute by admission/confession during the interview process, additional questions should not be asked, interview should be ended, and the replies should be documented in written.

3.4.3 Psychological Advantage

If suspicion intensifies during the interview, it is possible for the interviewer to divert the attention of the other party to a different direction by explaining the side factors and other details that are not directly related to the event, rather than the issues related to the subject of the case. In this regard, it is important that the interviewer acts in a way to gain the trust of the other party by establishing a certain and reasonable closeness. It will be easier for the interviewer, who has a psychological advantage, to detect contradictions in the statements; thus, it will be effortless to clarify the case subject to dispute.

3.4.4 Body Language

It is admitted that appearance has implications for getting the impression of suspicion. Likewise, making this impression felt by the other party may lead to psychological advantage. In this context, it can be used as an effective method if the interviewer closely follows the body language of the other party and especially observes radical changes (such as dryness of mouth, blushing, sweating, trembling of limbs, tongue slips, avoiding eye contact) in order to lead the interview.

3.5 Ending and Reporting the Process

At the end of the interview process, it is essential to summarize the case and the issues discussed and to review the important points.

In order to document the interview, it is recommended that the statements are written down. In this context, it is necessary that statements are expressed objectively and reflect the material truth completely with a formal style. It will be useful to include information about how and from whom the annexes on the details of the event or information obtained from third parties as well as place and date of the interview.

It will also be useful to mutually sign the minutes of the interview including the identity details of the interviewer and the interviewee, without being subjected to any pressure.

NOTES

Section 4
REPORTING

4.1 Importance of Investigation Report

The investigation report is the final stage of an investigation process, and perhaps the most critical part. A thorough and effective investigation may not provide the expected result if it does not contain the information that must be provided in writing. Therefore, the long and hard work carried out may be unrequited in a sense.

Investigation reports need to be written with a flexible technique, often due to the special circumstances and considering the needs of the parties requesting the report. In addition, elements such as accuracy, clarity, and relation with the subject are universal characteristics expected from a good investigation report.

The investigator must prepare the internal investigation report, taking into account that the it will not only be read internally, but by external parties. For instance; this report can be seen by the defendant, supervisory bodies of government agencies or other stakeholders. Therefore, contents of the report and how to protect the privacy of the report are important issues to be considered by the investigator. The investigation report must be designed in a structure that makes all rational explanations to the reader with its content in order to clarify the issues and must be sufficient to answer facts such as “who, what, when, where, why, how”. The reader of the report must not have the need to apply to another document or source of information in order to understand the issues in the report.

4.2 Characteristics of a Good Investigation Report

A well-written investigation report has the following characteristics:

4.2.1 Accuracy

The report must be accurate because an inaccurate report damages the reliability of both the report and the author. The report must include all the facts. The investigator must confirm all dates and supporting information in the report with those providing the information before the report is published. If there will be an annex to the report, these annexes must be fully explained. Inaccuracies and reckless errors can turn the report into a useless document.

4.2.2 Clarity

Reports prepared as a result of internal investigations must convey all relevant information in the clearest language. The report must only provide objective facts, and contain unbiased evidence that is unaffected by personal feelings, interpretations or prejudices. It is not appropriate to judge or comment on the report. If complex or technical terms need to be used, the investigator must ensure that these terms are used in appropriate contexts and, where necessary, explain the meaning of complex terms. In general, professional jargon must be avoided. Because the report can be read by people who are not familiar with technical terminology.

4.2.3. Impartiality and Relation Level

In the report, all facts must be presented without prejudice and all information related to the subject must be included in the report, regardless of which side it favors or what it proves or disproves. At the beginning of the investigation, the investigator must carefully determine what information will be required to prove the allegation and try to include only that information in the report. The report must include only issues related to the investigation.

4.2.4 Timeliness

The investigator must prepare the written report in a timely manner. It is critical to prepare the reports in a timely manner, especially in order to strengthen the accuracy of the statements taken for interviews aiming to obtain information or confession and to protect the investigator’s memory of the interviews. In particular, interviews must be documented on the day of the interview preferably.

NOTES

Section 5
DATA ANALYTICS IN INTERNAL INVESTIGATIONS

5.1 What are Data Analytics?

Data analytics means achieving implications from the entire data by extracting the raw data from the source, making it usable by cleaning and analyzing it using various techniques . Data analytics techniques can be used in many sectors and businesses. In this sense, the term "data analytics" covers a wide variety of data analyses. Today, data analytics is effective in a wide range, from machine automations in factories of organizations operating in the manufacturing sector to strategies shaped by sales algorithms in the retail industry.

In determination of fraud within the scope of internal investigations, methods based on the use of technology are encountered increasingly. With data analytics, it is possible to test all of the data and scenarios previously defined by the person who will perform the analysis on the entire data as well as commanding the entire data in determination of the fraud. On the other hand, continuous surveillance and predictive analysis can be performed with the help of artificial intelligence algorithms. At this point, unlike the term "data science", which is more generally used for a kind of discovery and aims to find the right questions to ask, "data analytics" aims to respond and mobilize certain questions with the help of available information. "Data science" is a broader term that includes "data analytics." [5]

Fraud is such a widespread problem all over the world that it is not possible to say that any country or institution can be completely protected from fraud[6] . Since data analytics methods provide full command of the data, it provides a proactive approach by revealing both preventive and detective controls in the fight against fraud.

Combating abuse is a cyclical process consisting of successive steps rather than linear. In this sense, data analytics can be used in the preventive, detective, remedial and supervisory steps of fight against fraud. The following sections will focus primarily on the determinative role of data analytics, and afterwards on the areas of continuous surveillance and predictive analytics.

5.2 Identifying Unusual Scenarios and Related Risks

Detecting unusual scenarios and identifying relevant risks using data analytics in internal investigations is carried out with the help of a methodology that includes the following steps[7]:

5.2.1 Detecting the Questions: What is Unusual?

Although the notification letter received from an organization gives some clues to the internal investigator on the subject to be investigated, it is necessary to first understand what the usual course of work is to determine exactly what the problem is. The definition of "ordinary" for certain processes may differ on the basis of countries' legal regulations, sector's practices or corporate internal policies. Therefore, the conditions of the country, the functioning of the sector and the processes of the business must be understood in a multidimensional way in the first place. For example, the level of approval limit for offers received from suppliers, standard duration between sales orders and invoicing, or access authorizations to information technology systems are only a few examples specific to each business.

Afterwards, within the scope of the process to be examined, a scenario pool is created which includes the contradictory practices and risks that may arise as can be defined as "unusual" on the basis of the organization's processes and sub-processes. This unusual scenario pool is the first step towards identifying the risks of fraud in each layer by making a complete dive into the processes covered by the internal investigation. The conclusions to arise in the event of occurrence of each fraud level and the data analytics scenario to be applied to determine this conclusion are determined.

5.2.2 Are All Data Suitable for Analytic Operation?

As the technologies of the infrastructure programs used in data analytics studies progress, any form of data can be included in the data analytics study in some way. On the other hand, the quality of the data (by looking at the characteristics such as how continuous it is, how old it is, how modular it is) directly affects how it will contribute to the internal investigation.

Once appropriate data sources are identified, the source to be used for the relevant internal investigation must be selected. During the selection of the data source, a result-oriented approach must be taken primarily. In case of predetermined fraud scenarios, questions such as what kind of traces may be left in which forms will direct the person who will conduct the investigation to the right data source.

5.2.3 Clearing, Organizing and Converting the Data by Easy Methods

Data cleaning methods are based on filling missing qualities and values on data obtained from different sources, organizing, grouping and leveling data in disorganized form, eliminating discrepancies and analyzing inconsistencies.[8][9]

Software such as Alteryx provide a very user-friendly method to observe the discrepancies in each column of data to be used in internal investigations. Such software are very fast and useful not only for detecting and clearing inconsistencies, but also for editing and converting the data into tables in a flat file format for the analysis phase that is the subsequent process.

On the other hand, technologies integrated directly into the Microsoft Excel program, such as Microsoft Power Query, help users to easily clean, organize and convert data. Power Query is a data link technology for discovering, linking, merging and organizing data sources for analysis.

The common feature of Alteryx and Power Query is that unlike systems that require technical language proficiency, such as "structured query language (SQL)", they are designed in a way suitable to be used by people who are not trained in the software and

[4] Fisher, D., Deline, R., Czerwinski, M., &Drucker, S. (2012). Interactions with big data analytics. Interactions, 19 (3)
[5] Aasheim, C.L., Gardiner, A., Rutner, P., Williams, S. (2015). Data Analytics vs. Data Science: A Study of Similarities and Differences in Undergraduate Programs Based on Course Descriptions. Journal of Information Systems Education, 26 (2)
[6] Abdullahi,R., & Mansor, N. (2015). Forensic accounting and fraud risk factors: The Influence of fraud diamond theory. The American Journal of Innovative Research and Applied Sciences,1(5)
[7] Baesens, B. (2015). Fraud analytics usingdescriptive, predictive, andsocial network techniques: A guideto data science forfrauddetection. Hoboken, NJ: Wiley.
[8] Fatima, A., Nazir, N., &Khan, M. G. (2017). Data CleaningIn Data Warehouse: A Survey of Data Pre-processing Techniquesand Tools. International Journal of Information Technologyand Computer Science, 9 (3)
[9] Wells, J. T. (2017). Corporate Fraud Handbook.

work all kinds of functions of the organization for cleaning data and detecting contradictions upon certain guidance to be provided by data analytics experts.

Today, many organizations prefer to have data analytics experts in their internal audit teams. In cases where it is not possible to meet this increasing demand with internal resources, external consultancy supports can be obtained by the experts of the subject. In any case, the fact that the organization meets the demand in question with its own internal resources with the help of the technological investment deemed appropriate, reveals at what stage and what kind of support will be needed thanks to the preliminary analyses that can be made..

5.2.4 Analysis of Data

Data sources selected, cleaned, organized and converted to be used within the scope of internal investigations are ready to be tested for pre-determined unusual scenarios after all these stages.

The unusual scenarios, which consist of hypotheses about the emergence of the case, where the data will be compared during the analysis, can manifest themselves in a wide variety of ways. While some of these scenarios are manifested as missing or contradicting values that have been deliberately applied in financial statements or reports, in another scenario, it can be detected by unusual change of the position of the process or data in the data table. After the scenario in question is determined on the source data with the help of relevant commands, the processes that fit this scenario are filtered from the data and a result table is created to verify the hypothesis or the question we ask the data.

While the scenario sample to be tested against the source data is shaped according to the scope of the internal investigation, the scenarios must be short, clear and equally understandable to everyone. Following scenario examples demonstrate a few standard examples that can be used in many internal investigations:

- On supplier main data; Suppliers with the same bank account number,
- On purchasing data; purchases made without receiving demand for needs,
- On stock data; repeating stock movements,
- On personnel expense data; divided expense transactions on the same date, under approval limit,
- On sales data; refund transactions showing an increase compared to annual average return at the beginnings of the following term in return for the sales showing an increase compared to annual average sales,
- On payment data; transactions with payment dates on weekend,
- On purchase approval data; purchases exceeding the approval limit of the employee.

5.2.5 Creating Visual Data Model and Interpreting Analysis Outputs

The fact that the investigation expert applies to visualization with the help of graphics while interpreting the results of the data provides ease to read and interpret the contradictions in the data for both them and the addressees of the study report. After the data tables confirming the scenario are found and modeled as associative tables, the model is reported by visualization. At this stage, a dynamic reporting and visualization method can be used that automatically renews itself according to new sources that will change or linked to the main data sources throughout the internal investigation. There are various technologies used in this sense, and the best known ones are Power BI and Tableau.

For representation of the resulting data model, the appropriate visualization method is selected depending on the area the analysis wants to focus on and the question it asks the data. Visualization methods can include area chart, map chart showing color density, linear and divided column chart, and tree map visual. The visual to be used is the one that can show the analysis outputs reached in the internal investigation in the most understandable way and will guide the internal investigator in the interpretation. In the reporting pages dynamically created thanks to the modern visualization technologies used today, for instance, while city-based sales and return figures can be tracked instantly on the map, on the other hand, a report can be designed that displays the horizontal analysis results of these figures on a monthly basis.

After presenting the data tables containing the findings with the help of the appropriate visuals, high, medium and low-risk areas can be highlighted and the addressee's action can be sorted out. This risk rating is made according to various predetermined criteria and is categorized. For example, the high or low financial risk is often measured by the ratio of estimated loss to earnings before interest and tax (EBITDA), while the methods used to measure the impact of a legal risk are much different. Risk rating is considered as a multiplier of the effect of risk and its frequency in the generally accepted methodology. Although this method is generally used in fraud risk assessments, it guides process owners during the recovery stages following internal investigations.

[10] Rettig L., Khayati M., Cudré-Mauroux P., Piorkówski M. (2019) Online Anomaly Detectionover Big Data Streams. In: Braschler M., Stadelmann T., Stockinger K. (eds) Applied Data Science.

5.3 Continuous Surveillance with Big Data

5.3.1 About Big Data

"Big Data" and "Continuous Surveillance" emerge as issues of increasing importance in the world of internal audit or internal investigation.

"Big Data" is a term used for data that are difficult to store, transfer and process with traditional database systems considering the volume and growth rate. When looking at each data source within an organization, it can be seen that the data that can be called "big data" can start at terabytes (1,000 GB) level and reach up to petabytes (1,000,000 GB).

When big data, data analytics, continuous surveillance and continuous audit are applied together or partially together, they provide businesses with significant gains and new perspectives for directors. Thanks to big data, organizations are making their operations more and more effective with their next generation decision making mechanisms and controls.

Big data that can be used in the field of continuous surveillance and audit varies characteristically. In general, these data are classified under two groups: structured and unstructured data.

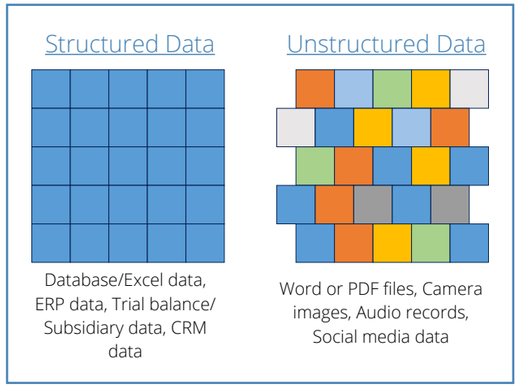
Structured Data: It is stored in a modular form, consisting of rows and columns, and can be analyzed with database analysis languages such as SQL. To summarize, these data:

- Can have data contents such as date, name, number, character, address,
- Are grouped as rows and columns,
- Can be processed on SQL and similar systems,
- Can be associated based on tables.

Unstructured Data: : It is the general name given to the data in the style that has no row-column relation. Video, Microsoft Word, PDF, image or audio files are examples of unstructured data..[13]

The difference between structured and unstructured data is described below:

Diagram 1: Structured and Unstructured Data



In this big data, which is rapidly diversifying and expanding, organizations have started to seek new insights and facts on themselves that they have not noticed before by using advanced statistical models as well as the latest developments in the computer science. This trend increasingly continues in the fields of continuous surveillance and control audit.

[11] Nada Elgendy, Ahmed Elragal (2014) Big Data Analytics: A Literature Review Paper
[12] Hugh J. Watson (2013) Big Data Analytics: Concepts, Technologies, and Applications.
[13] Chandra, P., &Praveen, S. (2017). Influence of Structured, Semi Structured, Unstructured data on various data models. International Journal of Scientific & Engineering Research,8(12)

5.3.2 Continuous Surveillance and Continuous Audit

Continuous audit is a type of audit using special computer-aided audit programs that allows the audit of information produced in the real-time accounting information system, without requiring for physical documents. In this approach, possible errors and frauds can be detected before they happen with the help of scenarios integrated with the programs.

With the effective use of continuous surveillance, corporate directors can better grasp on which areas resources must be allocated for improving processes, implementing new actions, issues to focus on while addressing risks, and risk priorities. Thanks to all these, they can present a more suitable image for their corporate objectives.

Continuous surveillance can be considered as a set of automated and continuous processes. Thanks to continuous surveillance:

- Risky issues and efficiency of controls are determined,
- Business processes and flows are improved in line with ethics and compliance principles,
- Better decisions can be made quantitatively and qualitatively by right timing,
- More cost-effective controls can be created with the help of various information technology systems.

Unlike continuous surveillance, continuous audit provides more efficient use of limited resources of the management within the audit process and better performance of audit in qualitative and quantitative terms. Thanks to the continuous audit, internal audit teams can perform the following during their audits:

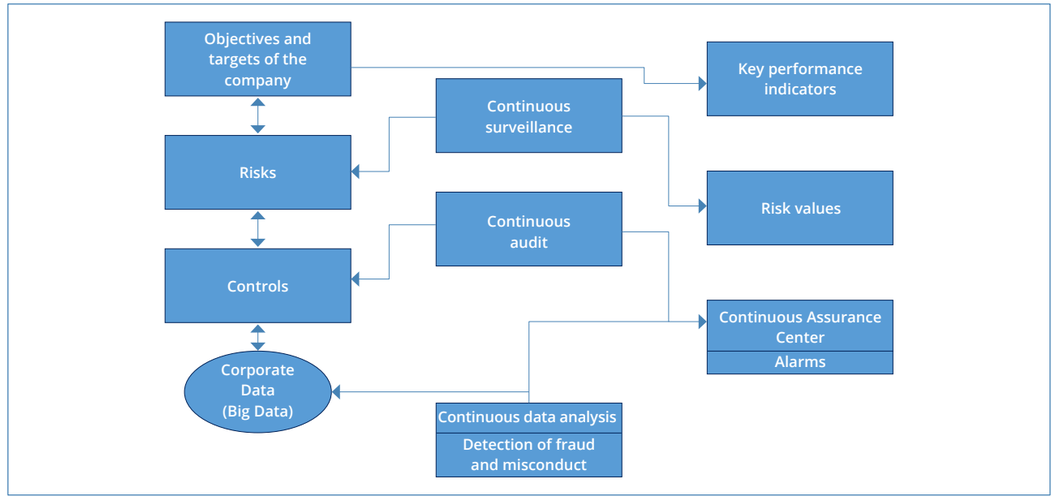
- Turning audit activities from periodical to continuous, providing more proactive solutions by internal-external audit teams with a broader perspective,
- Transferring to a more dynamic and solution-oriented audit approach from annual audit plans,
- Reducing audit costs by effective use of information technologies,
- Storing critical data to be used in internal-external audit activities such as information on processes, bookkeeping accounts, transaction information in a continuous and automatic way.

[14] Murat Serçemeli, M. Suphi Orhan, (2016) Journal of Turkish Court of Accounts Issue: 101, A Study On Bist-100 Firms With Respect To Continuous Auditing And The Future Of Auditing

5.3.3 Big Data and Possible Surveillance Areas in Organizations

Operational and financial data that the organizations possess are data with highly convenient form for continuous surveillance and audit. How the continuous audit and continuous surveillance processes can be implemented in the organizations is explained in the diagram below:

Diagram 2: A Sample Continuous Audit and Continuous Surveillance Application [15]



Identifying the right controls and data sources will greatly increase the success of automated risk surveillance and risk audit. In addition to this, considering the operations of the organizations and implementing sector-specific controls as much as possible will improve the quality of continuous surveillance and audit outputs. In addition, it is of vital importance for the system that the big data of the corporate to ensure operation of continuous surveillance and audit systems is complete, consistent, compliant, accurate and valid for the institution's big data that will enable continuous surveillance and control systems to operate.[16]

Matching the right roles with the right employees within the entire system to be established, strengthening the reports to be generated automatically with key performance values that will facilitate the decision-making of the directors will trigger a stronger internal audit structure in the organizations.

Continuous surveillance and audit are also important for organizations operating in sectors that are subject to high and complex legal regulations (e.g. finance, energy, medicine, etc.). Considering the reputation and financial losses of criminal sanctions imposed by the regulators in the past, it has been observed that it may be more beneficial for organizations to allocate resources for the establishment of continuous surveillance and control systems to be used for this purpose. After the installation, testing the system with various trials will increase the reliability of the system. Also, it is possible to continuously improve the system with the new rules to be added.

[15] Continuoustestingandmonitoring of IT controls (2017) https://www.pwc.com/us/en/risk-assurance/publications/assets/continuous-testing-monitoring-it-controls.pdf
[16] Continuoustestingandmonitoring of IT controls (2017) https://www.pwc.com/us/en/risk-assurance/publications/assets/continuous-testing-monitoring-it-controls.pdf

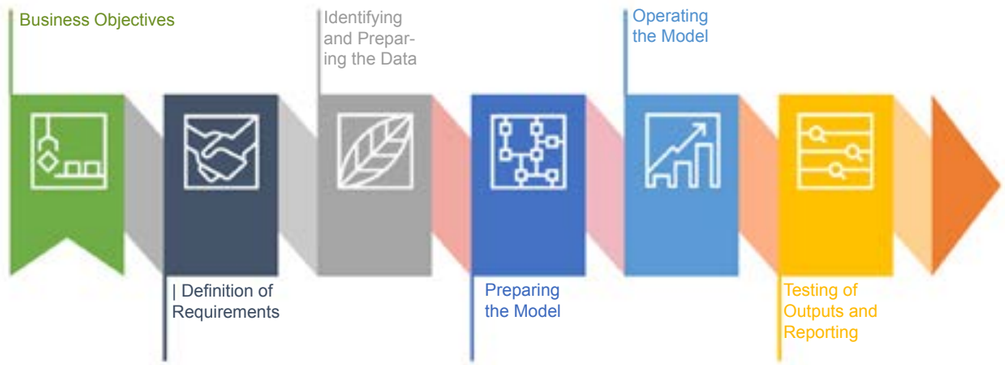
5.4 Predictive Analytics

5.4.1 Definition of Predictive Analytics

Predictive analytics can be defined as applying advanced analyzing techniques such as data mining, predictive modelling, artificial intelligence on current and past data, and therefore predicting the potential future events.

A standard predictive analytics process is shown in the diagram below:

Diagram 3: A Sample Predictive Analytics Process



Determining the business objectives, which is the first step of the process, enables identifying the target to be reached within the scope of the organization's objectives and activities. Contribution of directors is important in defining the appropriate requirements for this. In the identification and preparation of the data step, analytical work has started, and works are carried out in areas such as relationships between tables and cleaning of the data. Preparing the model with the right parameters is an issue that requires experience. Because, meeting the right data with the right model will increase the accuracy of the predictive work performed. It is essential that the types of algorithms to be used in creating the model (e.g. regression, classification, clustering, etc.) are selected in accordance with the desired output and available data. The outputs of the model must be compared with the historical data that have taken place. While the management is able to take action with these values if the outputs are in line with the requirements determined in the beginning, it is required to prepare the model again and run it with a different data set if it is not in line with requirements.

5.4.2 Using Predictive Analytics in Internal Audit and Examination Activities

It has been seen that the directors of organizations use predictive analyses to improve the existing business strategies and to apply new strategies. It has been observed that the benefits of predictive analysis techniques for the world of internal audit and examination are very comprehensive in every sense.

It is a certain fact that in the world of internal audit, predictive analytics will have great benefits in determining risks before they occur and designing relevant detective controls. On the other hand, the use of predictive analytics in the world of internal investigation and examination appears in the stages following the realization of the internal investigation, that is in determining preventive controls. In addition, artificial intelligence technologies are run on current or historical data to help predict future fraud events even before they occur and to enable businesses to position themselves strategically.

Section 6
SPEAK UP CULTURE AND MECHANISM

"Speak up" means that violations of legislations, in-company rules and ethical principles can be freely expressed and reported on the basis of confidentiality. The power that enables the notification or reporting mechanisms foreseen by the companies in compliance programs is the notification and speak up culture of company employees in terms of suspicious compliance violations. For this reason, speak up culture and mechanisms are an important part of the ethics and compliance cultures of companies, and are considered as one of the basic elements of compliance programs.

It can be said that there is an advanced "speak up" culture in a workplace where employees can report any discrepancies they encounter or suspect without being concerned about confidentiality or retaliation, relying on the fact that it will be investigated fairly and effectively. Employees in these workplaces report more frequently and do not remain silent against any disputes they encounter or suspect.

6.1 Why Are Speak Up Mechanisms Important?

Importance of speak up mechanisms are felt deeply by companies due to the fact that incompliances from acting against in-company rules to violation of ethical values are one of the biggest obstacles that hinder corporate productivity or legislation compliance sensitivities of companies has increased as a result of penalties imposed by various authorities.

In most cases, it is sufficient to damage the reputation of companies if there is an incident pointing to fraud, any rumors or an allegation spread in the social media. It is possible to detect and solve such problems without being spread inside and outside the company thanks to effective and structured speak up mechanisms based on confidentiality principles.

Notices are the most important methods to detect nonconformities. Such that, according to 2018 Global Study on Occupational Fraud and Abuse prepared by ACFE, business frauds were discovered by notice method by far with a rate of 40%.
In a work environment where speak up culture is not developed, settled or ineffective, the effectiveness of one of the most important methods that can ensure detection of incompliance decreases or disappears. This situation in itself poses a risk for companies.

First of all, the ethical code or speak up policy must clearly and explicitly reveal the company's approach in this regard, the mechanisms it envisages, their operating principles, how to evaluate and finalize the notices. In addition, employees must be encouraged to use these mechanisms, and the benefits of this situation for themselves and the company must be explained. Otherwise, hesitation to notice or being afraid of their result block the way to the detection of the incompliance as well as discouraging the employees in terms of their motivation and confidence to act for honest operation of the company. In cases where the company sincerely prefers open communication and transparency and can prove it through in-house practices, employees can understand what kind of work culture they are expected to adapt to and adopt the company culture more easily.

6.2 Speak Up Mechanisms and Common Practices

In order to fight fraud and other incompliances, the most natural method is of course the assignment of a competent person or team within the company to conduct these reporting processes. Therefore, every company expects any notice to be directed directly to this person or team.

The expectation of confidentiality in these whistleblowing processes is natural, based on reasons such as the concern that any notice they make may have a negative effect on them, and the possibility of damaging inter-company relations. By creating a team that fulfills these expectations, it must be ensured that all employees are aware of whom they can report an incompliance they have observed or suspected. For this purpose, memorable tools suitable for the human resource demography of the company must be used such as trainings, posters and information cards.

Notice lines (hotlines, weblines) are the most common notification tools. Many international companies use whistleblowing lines with different language options open to continuous (24/7) whistleblowing. This line is sometimes designated as an online messaging, e-mail or sometimes call service. It is also observed that some companies use more than one speak up mechanism at the same time, considering whether the sector in which the company operates is more open to fraud and other incompatibilities or the workload of its international offices.

The said whistleblowing lines must provide a secure communication channel between the company and the whistleblower. This platform must provide the opportunity for the investigating team to share with the whistleblower the need for additional information and documents, and also for the whistleblower to request information about investigation phases and outputs.

Considering the employee structure, physical structure of the workplaces and their business forms, companies with multiple employees or workplaces utilize multiple mechanisms such as hotlines, websites, e-mail accounts allocated for whistleblowing, and consultants outside the company. In any case, it is ideal to envision multiple mechanisms that employees can choose from to express themselves.

Companies frequently and explicitly express the fact to their employees in words and writing that confidentiality will be ensured and retaliation will be prevented in order to describe the usualness of these mechanisms and to spread its use. As a matter of fact, in addition to the accessibility and convenience of the whistleblowing mechanisms, the effort to create a comfort area that will enable employees to apply for this method and to make it embraced is reflected in the ethical codes created by companies, offered to or accessed by each employee.

6.3 Embracing the Speak Up Culture

Effectiveness of whistleblowing mechanisms depends on the establishment of speak up culture within the company. In this respect, it is important for the employees to learn that whistleblowing, speaking up and open communication are part of the corporate culture, by the people who have the title of manager with the method known as “tone at the top” in the literature. In cases where feasibility or ultimately audit and/or sanction processes are not present or a determined attitude in this direction is not displayed at the executive level, whistleblowing mechanisms would lose their meaning.

One of the most important issues in the adoption of whistleblowing processes is to ensure confidentiality. So much so that practices that oblige any employee to report their identity explicitly will have the opposite effect and create the idea across the company that reporting may be against the interest of employees. In order to prevent such situations, the proposed mechanisms must be tested, and their functionality should be ensured. For example, the reporting practices placed at the points that can be seen by everyone, such as “complaint boxes”, will not be preferred. In fact, in some cases where employees are allowed to report face-to-face, it is expected that the room of the person to whom the employee will consult to is not visible to everyone. It is essential for the establishment of speak up culture throughout the company that the employee who will initiate the whistleblowing process to continue working as if any such whistleblowing never happened after conveying information about the relevant case.

It is necessary to assure whistleblowing employees that there will be no retaliations in order to establish speak up culture and improve ethical culture of the company in the long run. Otherwise, it would be very difficult to convince the employees that the company has adapted speak up culture and encourages them to freely notice incompliances.

Ultimately, main objective of whistleblowing mechanisms is to take preventive measures and/or to resolve the outcomes by investigating the incompliances that continue by themselves or by their effects, and then work on their causes. In this context, taking into account the realities of human nature and the position of the employees against their companies, the development of speak up culture as well as appropriate and favorable notification mechanisms will undoubtedly contribute to the investigation processes and ethical cultures of the companies.

Section 7
PERSPECTIVE FOR COMMUNICATION FOR MEDIA CRISES AND WITH EXTERNAL STAKEHOLDERS

One of the most essential stages of crisis management is thought to be the management of communication with the media and external stakeholders. It can even be said that many directors realize that the problems that arise in their organizations have turned into a crisis only when they see it on the news. When we look at it from the perspective of internal investigations, it turns out that this case is valid. Protection of corporate reputation depends on proper and sound management of communication with both the media and external stakeholders. However, we are faced with the conditions in which we need to review communication routines regarding how this can be done. Because we are going through a period when the methods used in communication and the meanings attributed to the concepts are changing. It is possible for us to understand this transformation, which is of great importance for the sound execution of internal investigation processes, in three main pillars.

The first of these is the fact that the separation between the stakeholders inside and outside the organization has almost been almost eliminated. The opportunities for media and external stakeholders to get information from within the organizations have increased, and the ways for corporate employees to knowingly or unknowingly export information have increased. Therefore, those who manage the internal investigation process need to reconsider the assumption that the information will not leave the organization.

Second step is the fact that communication channels have increased with digitalization and mainstream media has lost its sole determination unlike the past. A claim suggested or information shared on social media can attract the attention of media channels in a short period of time, causing activists (artists, athletes, etc.) who have influences in the society to get involved in the issue and thus increase social awareness.

Third pillar of the transformation is that reputation can be established as a result of sustainable and sincere relationships formed with external stakeholders. In the past, when communication channels were under control, while advertisement-based, polished image campaigns were sufficient to create a positive perception about companies and organizations, today, in an age of transparent communication, media and external stakeholders can now closely follow the compliance or incompliance between what organizations say and do. In other words, expectations of stakeholders of organizations (clients, society, employees, investors, etc.) have increased compared to the past, and channels have been created where they can observe whether these expectations have been met. If the official discourses of the organizations are not supported by their actions, it may even result in new crises.

In order to be free from this whirlpool and prevent crises, companies must adopt a new perspective towards the management of their relations with media and external stakeholders. Some works that can be conducted in this regard are described below.

7.1. Does the Crisis Knock Before Entering?

Crisis is defined as an unpredictable event that creates an effect that will radically change the existing situation due to its magnitude. However, one of the many assessments about the crises is the thought that it is retrospectively predictable as expressed Nassim Nicholas Taleb in his “Black Swan” theory. It is not possible to say that all crises are predictable and preventable. As its name implies, if crises are known before they happen, all actors get position accordingly and there would be no crisis. However, organizations can take more effective steps to prevent or be prepared for potential crises by using certain methods.

- The most important of these is that each organization identifies its “Black Swans” and works on possible scenarios that may occur with them. In other words, situations that are unlikely to happen but potentially damaging must be listed by the teams in the organization and must be handled in different dimensions such as nominal, financial, operational, life and property-related security.

- How the decision-making mechanism will occur in crisis situations and who will be responsible must be determined in advance. Accordingly, roles must be distributed and communication channels must be defined in advance.

- In every crisis, especially media and external stakeholders need accurate and continuous information flow by the leader of the organization. For this reason, the people who will work as spokespersons in the organization must be trained in advance and be informed about the messages to be provided to the public.

- Primary stakeholders of the organization must be identified in advance as well as how to contact with them in the event of a crisis. It must be known to the stakeholders how to initiate support mechanisms when necessary.

However, the most effective way to predict and prevent a crisis is the directors to listen to the signals coming from the organization. Directors who have developed their senses within the organization can determine whether there is a systemic disruption by considering the slightest signs. Unfortunately, many directors believe that the problems are “isolated” and hope that they will pass by themselves. Ignoring failing situations or anomalies often results in disaster. For example, after the crisis in 2019 that resulted with the two crashes of new model planes of a plane manufacturer company, hundreds of people losing their lives and stopping of planes; it was revealed that five pilots have written reports on “problems they encountered in critical moments” during flights.

7.2 What to Do During a Crisis

When a crisis reflects to the media and external stakeholders, the first thing to do might be to reach them and give our messages. Of course, this step needs to be taken. However, what needs to be done first of all is to make sure that the organization is running flawlessly and calmly. As we explained in the first section, we live in a period where communication between internal and external stakeholders is increased and the flow of information is accelerated through digital channels. In crisis situations, consequences such as problems arising within the organization, increased stress and emotional reactions can be reflected to external stakeholders and make the crisis worse. Therefore, the first step to be taken is to ensure that the organization going through the crisis understands the matter correctly and clearly.

When this phase is over, the information obtained to the media and external stakeholders must be clearly communicated as soon as possible. The important point here is not to hide any topic, but also to indicate what are not currently available or clear. Otherwise, it may be possible to increase the doubts and decrease the trust in the organization that is already going through the crisis. When communicating with internal and external stakeholders, it is vital that the messages are provided from the most authoritative position. Because leadership would be important exactly at this time. In fact, the leader is not the one who manages the crisis, but the person who gives confidence to the parties affected by the crisis. If the leader tries to solve the situation that caused the crisis from the very first moment, confidence inspiring messages that are expected from them would be delayed. This may cause stakeholders who are the parties to the crisis to take wrong actions. Delegating these messages to less senior directors is an attitude to be avoided.

If there is an operational or technical problem that caused the crisis, the pressure on the relevant teams must be reduced in order to reveal and resolve the causes. If urgent action is taken to solve the problem as soon as possible with the temperature of the crisis, it may be possible to make mistakes that will deepen the crisis. As with any emergency, the first principle must be not to worsen the current situation.

7.3. Post-Crisis Restoration

In fact, every crisis fosters an opportunity in itself. It is an opportunity for organizations to renew themselves when they examine the conditions and root causes of the crisis with great clarity and take necessary measures. But linking the problem other factors (personal issues, external causes, etc.) rather than seeing the systematic aspects of it allows the organization to only save time until the next crisis. In such cases, image work is mostly useless. However, the structures that come out stronger from crises increase their resilience and become more prepared for the crisis-like situations that may occur in the future.

Institutions that have experienced the crisis need to explain how they have found the opportunity to compensate after this crisis in order to both renew themselves and establish trust of their stakeholders. Of course, the people who lead the organization must make some difficult choices here and make sincere decisions in order to avoid similar situations in the future. Some systematic interventions may be required after root causes are identified. These often occur in ways such as governance, committee structures, and decision-making mechanisms. Especially organizational culture and values need to be revised, and the invisible spiritual values leading to the crisis must be reconsidered. People who lead the organization take a leading role in the restoration of values and reflect it on their actions. Because only in this way the right value sets can transform into the culture of an organization, manifest themselves in behaviors of employees and thus prevent possible crises. This transformation must be explained both internally and externally and must be communicated to stakeholders with a campaign and message that can be easily understood, if possible.

NOTES

Section 8
LEGAL ISSUES TO BE CONSIDERED IN INVESTIGATION PROCESS

8.1 Attorney and Client Confidentiality

Attorney-client relationship is a confidential relationship that must include concessions and confidentiality in many ways. In order to protect their rights and freedoms in the most accurate way, individuals must be ensured that the information they provide to their attorneys will remain confidential. Attorney-client confidentiality is based on the right to legal remedies, which is a constitutional right. Accordingly, in order to ensure fair trial, the client's relationship with the attorney must be carried out in an atmosphere of trust. In order to establish this atmosphere of trust, attorney-client confidentiality, which is protected by many regulations in the international platform, is mainly regulated under the Code of Criminal Procedure ("CCP") and Attorneys' Law No. 5271 in our country:

CCP art. 130:
"...If the judge with venue establishes that the seized items are under the privilege of attorney client relationship, the seized object shall be promptly returned to the attorney and the transcripts of the interactions shall be destroyed."

Attorneys' Law art. 36:
"Attorneys are prohibited to disclose the information entrusted to them and they learn due to their attorney duties or their duties at Turkish Bar Association and bar organs."

Constitutional Court also highlighted the importance of the confidentiality of the attorney-client relationship in the light of legal regulations and decided that the documents belonging to the attorney-client relationship must be returned to the attorneys :

"If the judge with venue establishes that the seized items are under the privilege of attorney client relationship, the seized object shall be promptly returned to the attorney and the transcripts of the interactions shall be destroyed."

Whether or not the correspondence with the attorneys in the examinations made before the relevant organization can be accepted as evidence has been a matter of dispute, especially in the examinations and investigations made by the Competition Authority in accordance with the relevant legislation. The reason for this is the article 15 of the Law No. 4054 on the Protection of Competition, which gives the Competition Board the right to conduct audit on-site and is open to broad interpretation:

"The board may conduct audits at enterprises and enterprise associations if deemed necessary while carrying out the duties granted by this law..."

What would be the limit of on-site audit authority? Competition Board decisions made in this regard are striking. Dow Decision of Competition Board draws the limits of attorney-client confidentiality in terms of the board's own practices and states in which cases it is a legal interest worth protecting:

"...This protection includes the correspondences made with the aim to exercise the right of defense with the independent attorney and the paperwork prepared for obtaining legal advice from the independent attorney. On the contrary, correspondences which are not directly related to the use of the right to defense, made to help with any violation or to conceal an ongoing or future violation, cannot benefit from protection, even if they concern preliminary research, investigation or examination."

Pursuant to Dow Decision, in order to refer to attorney-client confidentiality in documents to be examined within the scope of a competition investigation, (i) there must be an independent relationship between the client and the attorney, and (ii) the documents which are alleged to be under confidentiality liability must be for the right of defense. Accordingly, it will not be possible for attorneys working at the organization (i.e. attorneys working at the organization's own legal department) to benefit from attorney-client confidentiality. In addition, correspondences which are not directly related to the use of the right to defense, made to help with any violation or to conceal an ongoing or future violation, cannot benefit from protection provided by attorney-client confidentiality.

This approach of the Competition Board has been subject to serious criticism. First of all, Competition Board interprets the right of defense quite broadly. Legal counseling services received from an independent attorney during the investigation are interpreted within the scope of the right to defense, and legal counseling services received to defend personal rights in the organization, not during the investigation, are also interpreted for the right to defense by the Competition Board. Even if the Competition Board interprets the right of defense broadly, how appropriate is it for the Competition Board to make this interpretation? While the correspondences with an independent attorney and the documents regarding the legal counseling services received must not be examined, it will be arbitrary in practice since these documents are examined and assessed by the Competition Board in terms of whether they are for the right to defense.

In another remarkable decision of the Competition Board, the attorney-client confidentiality principles mentioned in the Dow Decision were repeated and the documents requested to be returned were not assessed within the scope of the attorney-client privacy principle, with the explanation that they were not directly related to the exercise of the right to defense. In the annulment case filed against this decision by the Competition Board, it is understood that the document requested by the organization from the relevant administrative court decision is a report regarding the conditions in which the competition legislation may be violated. The administrative court did not find the Competition Board's decision in accordance with the law. The administrative court also ruled that the regulation compliance report was "in the form of a document prepared for obtaining legal advice from an independent attorney" [17].

In this case, it must be accepted that regulation compliance reports must also benefit from attorney-client confidentiality. As of the publication date of this guide, the Council of State decision regarding the administrative court decision has not been published yet; following this decision will be important in terms of seeing the Council of State approach to the issue.

In addition to knowing the rules, rights and liabilities to be applied and during the investigation, it is also of great importance to be informed about the steps to be taken and legal processes to be initiated after the investigation is completed, and to know relevant legislations and legal possibilities in order to make decisions which protect organizational interest in the best way possible.

[17] Constitutional Court Decision, GK, D. 17.12.2015B. 2013/1631,
[18] Competition Board Decision, D. 02.12.2015, D. 2015-1-54, K. 15-42/690-259

8.2 Protection of Personal Data in Internal Investigations

Law on Protection of Personal Data ("LPPD") discusses the concept of personal data very broad and defines personal data as any information related to a specific or identifiable natural person in its article 3. In accordance with LPPD, the explicit consent of the data subject is required for the personal data to be processed lawfully as a rule. However, some cases constitute exceptions for open consent. First of all, the first question that comes to mind in internal investigations is whether the employee e-mails can be reviewed by the employer and whether this can be assessed within the scope of LPPD. In addition, this issue is not limited to LPPD, but was also the subject of the decisions of the European Court of Human Rights ("ECHR") and the Constitutional Court ("CC"). With the Barbulescu decision dated 5 September 2017, ECHR has adjudged that employers are entitled and have control over the computers allocated to the use of employees, however, certain conditions must be fulfilled in order not to violate the privacy of personal life in the examination of personal conversations/e-mails. These conditions are mainly as follows:

- The employer must inform the employees about the fact that their computers can be inspected and appropriate measures can be taken.
- In case of examination of personal conversations of employees; examination of the communication flow and examination of the communication contents must be separated from each other.
- If the employer is examining personal documents, they must provide a justified reason for this examination.
- Before examining the contents of personal files of employees, it must be researched whether there are methods that would cause less harm than violation of personal privacy.

With its decision published in the Official Gazette dated 10 May 2016, CC authorizes the employer to examine the correspondences of employees. In the incident that CC assessed in reaching this result, it has been seen that the employees has signed an applicable Internal Regulation and Information Security Covenant on the rules to be complied with at the workplace, they made a covenant that they will not use the computers, e-mails, internet connection, telephones, communication software, other IT resources and communication tools allocated to them by their employers for work for personal purposes exceeding basic needs, for entertainment purposes, against public ethics, customs and traditions; in addition, they have declared and undertaken that the IT and communication resources they use can be kept under surveillance by organization directors without informing and notifying the applicants, the correspondence and communication records can be backed up, reported, examined in detail, seized and limited in terms of use when necessary. While making its decision, CC explicitly stated and evaluated all these issues in its justification. In this context, the following justification of CC is important for the prevention of possible personal data violations during internal investigation:

"In addition to the fact that it is not possible to accept under articles 11 and 12 of the Constitution the regulations which allow the employers to interfere with privacies and communication freedoms of their employees arbitrarily and without any limitation, in cases where there are regulations that explicitly contain the rules determined pursuant to commercial requirements and disciplinary approach of the enterprises provided that it is not against the assurances, laws, international contracts provided by constitutional rights and freedoms and where the employees are informed and warned about these regulations in advance, it may be reasonable to take measures in order to restrict certain rights of employees and force them not to break the rules with predetermined scope, especially during working hours. In this context, in cases where no information or warning is provided, it must be accepted that employees will have a reasonable expectation that no intervention will be made to their rights and freedoms and will benefit from the assurances provided by such rights and freedoms."

Supreme Court decisions also confirm the examination authority conferred by CC to employers:

"The employer has the authority to control their computers and e-mail addresses as well as e-mails sent to these addresses at all times. Moreover, it is unacceptable for the complainant employee to use the computer for personal works without the employer's permission. For these reasons, there is no contradiction of law if the defendant employer uses computer data as evidence..."

In this context, although LPPD accepts all kinds of information about a specific or identifiable natural person as personal data, relevant CC and Supreme Court decisions express that the employer has the authority to control their computers and e-mail addresses as well as e-mails sent to these addresses at all times during working hours provided that the employee is informed in advance. However, while conducting internal investigation processes, it must be noted that the data processing that will be carried out by the employer is a purposeful, limited and measured data processing, especially if there will be data processing process other than the corporate computers and e-mail addresses.

A decision that would constitute a case law discussing this subject has not been published within the scope of LPPD. However, as the initial option to eliminate the possible risks, it may be required for employers to obtain written explicit consents of employees about the fact that their personal data may be processed before initiating an investigation. However, due to usual flow of life, obtaining explicit consent of relevant persons may not be possible due to the structure of these investigations. Therefore, it would be appropriate for organizations to publish a policy on how internal investigations will be carried out while conducting such processes, to convey it to all of their employees, and even obtain a written confirmation that they have read and understood these if possible. Thus, employees will be able to learn what personal data will be processed, to whom this data can be transferred, what methods will be used to collect this data, the legal reasons behind them and their rights on this matter, and the obligation to clarify will also be fulfilled within this scope.

In addition, it is necessary to investigate whether the internal investigations conducted

[19] Constitutional Court Decision, Application No. 2013/4825, D. 24.3.2016

[20] Yargıtay 22. Hukuk Dairesi, T. 3.5.2016, E. 2016/6321, K. 2016/13143

at the organization will provide one of the exceptions envisaged in the LPPC in each case. One of these exceptions is a perspective adopted in the doctrine that "the fact that data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the person concerned" can be applied on case basis. Pursuant to this opinion, an internal investigation carried out to protect the legitimate interests of the organization may create a situation where the explicit consent of the employee is not sought for deliberate and purposeful data processing, provided that the fundamental rights and freedoms of employee whose personal data is processed is not harmed. However, even if the data controller has a legitimate interest in the case, the obligation of the organization to fulfill the personal data processing rules and principles in LPPD will continue.

In the light of the clarifications above, care must be exercised to process personal data during internal investigations. In cases where explicit consent of employees is no obtained, each case must be thoroughly assessed whether it is within the scope of an exception pursuant to LPPD. Because, if a personal data other than exceptions is processed by the organization without explicit consent, Personal Data Protection Board ("Board") will be authorized to impose the relevant organization with an administrative fine between 37.000 Turkish Liras and 1.400.000 Turkish Liras.[21]

8.3 Legal Processes Following the Internal Investigations and Developments in Turkish Jurisdiction

It is possible for the employer to apply to various legal remedies, including criminal complaint, according to the requirements of the situation and conditions about the employee whose misconduct was detected as a result of an internal investigation.

8.3.1 Business Law Sanctions and Remedial Responsibility

As a result of the relevant internal investigation, it is possible to terminate the employee's employment contract based on the nature of the evidence possessed by the employer for a justified or valid reason. It is also possible to terminate the employment contract through mutual rescission if the available evidence is not deemed sufficient, there is no evidence, or mutual agreement is preferred. Depending on the circumstances of the situation, it may be preferred to remove the relevant employee from the workplace immediately after notice or serious suspicion from time to time. In this way, it is aimed to conduct investigations and collect evidences within the organization in a healthier way. In such cases, the organization called "garden leave" can be used in order to remove the employee from the workplace before the internal investigation begins or while it continues. Although this application, which can be considered as a form of paid leave, does not have an exact equivalent in Turkish law, it may be ensured that the employee does not come to the workplace during the investigation process by obtaining the consent of the worker. During this period, the worker continues to receive her/his salary, but does not actively come to the workplace.

If unlawful operations and actions of the employee are judged as a result of the investigation, it may be required to rightfully terminate or terminate with a valid reason based on the force of the evidence available. Supreme Court has recently made decisions about acceptance of termination with valid reason in the event that the employer has strong suspicions that the relevant employee conducts unlawful acts within objective facts and indications as a result of examinations performed. This called "termination for suspicion" (for instance changing lifestyle of the employee, current statements of colleagues, etc.). However, if the employment relation would be terminated since the trust in the relevant employee is damaged even though the examination reveals that there exist no conclusions beyond an abstract suspicion, employment contract can be terminated by mutual rescission. Because, the main purpose of internal investigation processes is to reestablish the organizational order by conducting an effective and healthy internal investigation. Steps to be taken in terms of labor law will also allow efficient finalization of internal investigation processes.

In addition, it is possible to request the remedy of the financial and reputation loss caused by the relevant employee pursuant to relevant articles of the Turkish Code of Obligations. In the event that the relevant employee is in the capacity of an executive pursuant to the Turkish Commercial Code ("TCC"), it is also possible to discuss the possibility of remedial liability of the director who directly caused harm or who is considered responsible due to the fact that they do not show the due diligence despite being obliged pursuant to provisions of TCC.

8.3.2 Penal Sanctions of Behaviors Performed Against the Organization

Crimes that cause in-house investigations are so-called "white collar crimes" and are often encountered as misappropriation or fraud in practice. These crimes are regulated in the Turkish Criminal Code of Procedure ("CCP"). The major nature of the crime of misappropriation is regulated in article 155/2 of CCP.[22]

"Any person who denies the transfer to himself of moveable property belonging to another, or who enjoys the use of such property for a purpose not specified at the time of the transfer for the benefit of himself or another, where such property had been transferred for the purpose of protection or for a specified usage, shall be sentenced to a penalty of imprisonment from six months to two years and a judicial fine, upon complaint.

Where the offence is committed in relation to property, which was submitted and delivered as a requirement to confer authority to administer such property, and this authority is derived from a professional, trade, commercial, or service relationship or any other reason the offender shall be sentenced to a penalty of imprisonment for a term of one to seven years and a judicial fine of up to three thousand days."

According to article 155 second paragraph of TCC as mentioned above, it will be possible to discuss the possibility the that directors who commit the crime of misappropriation would be punished due to major nature of the crime since there is a commercial relationship between them and the organization.

Until recently, Turkish courts considered

[21] As of the publication date of the guide (2020).

[22] CCP art. 155; taken under the reconciliation scope with the judicial package with the regulation enforced in 2019.

the responsibility of the directors due to the damages inflicted by the organization's directors as "commercial incompliances" and made decisions based on the fact that a criminal sanction could not be imposed accordingly. However, it is seen in the recent court decisions that criminal dimension of the executives who have committed "white collar crimes" has been accepted and the criminal responsibility of these executives has been examined in detail. For instance, the Supreme Court in a decision made in 2014 ruled that the organization's director had committed the crime of white collar fraud because he worked as a director within the organization while he committed the crime and therefore accepted that the conduct of the director constituted a crime exceeding the nature of commercial dispute, and thus decided for the conviction of the director:

"Considering the fact that the defendant works as director at the participant organization on the date of the crime ... he/she held the check amounts collected within the frame of service relationship and did not return it to the participant organization, it is hereby decided for conviction of the defendant pursuant to article 155/2 of TCC no. 5237..." [23]

In the event of committing misappropriation crime more than once, successive offence provisions will be imposed and the penalty will be increased proportionally. The Supreme Court has decided that a director who received money from the organization more than once would be imposed with increased penalty pursuant to successive offence provisions:

"Considering the fact that the defendant received money from the participant organization more than once on different dates, it has been understood that the defendant violated the same provision of the law multiple times by the same offence within the scope of article 43/1 of TCC no. 5237, and it has been decided to impose partial penalties by not implementing successive offence provisions when imposing penalties on the defendant..." [24]

To summarize, with the new approach of the Supreme Court, it would be possible for employees to be obliged with paying compensation to the organization in the event they harm the organization with their unlawful acts and at the same time to be sentenced to prison sentence and punitive fines within the scope of TCC.

[23] Supreme Court 15th Penal Department, D. 24.2.2014, E. 2012/17443, K. 2014/3288

[24] Supreme Court 23rd Penal Department, D. 28.3.2016, E. 2016/3683, K. 2016/3454

TEİD

Etik ve İtibar Derneği

Ethics & Reputation Society

teid.org
Ethics and Reputation Society
Mor Sümbül Street. Varyap
Meridian Business I Blok No: 1 D: 66
34746 Batı Ataşehir, Istanbul