

Report on the  
Voluntary Special Audit at  
ThyssenKrupp AG, Essen

November 12, 2013

# TABLE OF CONTENTS

---

A. AUDIT ASSIGNMENT AND BASIS OF INFORMATION .....	1
B. MANAGEMENT SUMMARY .....	5
C. SUBJECT OF AUDIT .....	11
I. Further development of Internal Control System (audit subject 1).....	11
II. Further development of Compliance Management System (audit subject 2).....	59
III. Investment controlling as part of future large investment projects (audit subject 3).....	66
IV. Follow-up reporting by the Board to the Supervisory Board (audit subject 4).....	73
D. CLOSING REMARKS .....	78

## LIST OF ILLUSTRATIONS

---

Illustration 1: Overview of the Structure of the Compliance Organization at ThyssenKrupp, As at October 1, 2013.....	30
---	----

---

## LIST OF ABBREVIATIONS

---

Abbreviation	Meaning
a. M.	am Main
par.	paragraph
ACT	Group program ("Achieve Change@ThyssenKrupp")
AG	Aktiengesellschaft (stock company)
AktG	Aktiengesetz (German Stock Corporation Act)
AMI	ThyssenKrup investment database
Art.	Article
BA	Business Area
BDO / BDO AG	BDO AG Wirtschaftsprüfungsgesellschaft (auditing company)
BKMS®	Business Keeper Monitoring System web portal software
e.g.	for example
BT-Drs.	Bundestag printed paper
Business Keeper	Business Keeper AG
BWL	Business Administration
reg.	regarding
resp.	respectively
approx.	approximately
CC CT	Corporate Center Controlling & Risk

---

Abbreviation	Meaning
CC IA	Corporate Center Internal Auditing
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIS	Commonwealth of Independent States
CMS	Compliance Management System
CO/AUD	Corporate Function Internal Auditing
CO/CAR	Corporate Function Controlling, Accounting & Risk
CO/CPL	Corporate Function Compliance
CO/CPL-AP	Corporate Function Compliance, Department Awareness & Prevention
CO/CPL-INV	Corporate Function Compliance, Department Compliance Investigations
CO/CPL-PRP	Corporate Function Compliance, Department Projects, Reporting & Processes
CO/PSM	Corporate Function Procurement & Supply Management
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPI	Corruption Perceptions Index
CT	Components Technology
i.e.	id est
daproh	data and process harmonization
DAX	Deutscher Aktienindex (German share index)

Abbreviation	Meaning
DCGK	German Corporate Governance Code
Dr.	Doctor
e.V.	registered association
EAT	E-Learning Administration Tool from ThyssenKrupp
ERP	Enterprise Resource Planning
ET	Elevator Technology
etc.	et cetera
EUR	Euro
poss.	possible, possibly
FAQ	Frequently Asked Questions
FTE	Full-time equivalent
acc.	in accordance with, as per
GET	Global Engagement Tool
if appl.	if applicable
FY	Financial year
GmbH	Gesellschaft mit beschränkter Haftung (limited corporation)
RP	Rules of Procedure
HFM	Consolidation software
HQ	Headquarters

---

Abbreviation	Meaning
IDW PS	Auditing standard from the German Institute of Public Auditors
ICS	Internal Control System
ILO	International Labour Organization
InCo	Investment database
incl.	Including
spec.	specifically
IS	Industrial Solutions
KonTraG	German Law on Control and Transparency in the Corporate Sector
KPI	Key Performance Indicator
KPMG	KPMG AG (auditing company)
KWG	German Banking Act
LiNet	E-Learning Platform from ThyssenKrupp
MER	Monthly Executive Report
mill.	million
bill.	billion
MX	Material Services
No.	Number

---

Abbreviation	Meaning
Prof.	Professor
RACI	Competence, Responsibility, and Reporting Matrix
pg.	page
SAP	SAP AG
SE	Steel Europe
ThyssenKrupp	ThyssenKrupp Group
ThyssenKrupp AG	ThyssenKrupp Aktiengesellschaft (Essen)
TransPuG	German Transparency and Disclosure Act
incl.	including
USA	United States of America
cf.	confer (compare)
VIP	Very Important Person
Board	Board of ThyssenKrupp AG
e.g.	exempli gratia (for example)
ZGV	business transactions subject to approval

---

# ATTACHMENT

---

General Engagement Terms for Wirtschaftsprüfer  
and Wirtschaftsprüfungsgesellschaften  
[German Public Auditors and Public Audit Firms]  
including Special Conditions  
(as at January 1, 2002)

Attachment 1  
page 1 - 4



# A. AUDIT ASSIGNMENT AND BASIS OF INFORMATION

---

## I. Audit Assignment

Following the agreement of July 16, 2013 between ThyssenKrupp AG, the Deutsche Schutzvereinigung für Wertpapierbesitz e.V. (German association for private investors), and Christian Strenger, the auditing company BDO AG (hereafter referred to as "BDO" or "BDO AG") and Prof. Dr. Hans-Joachim Böcking, Professor of Business Administration, specifically Auditing and Corporate Governance, Goethe University, have both been appointed by the Board of

### ThyssenKrupp AG, Essen

to carry out a voluntary special audit. Following various significant incidents in recent years, the voluntary special audit should help to create sustainable value for the whole ThyssenKrupp Group and for the shareholders of ThyssenKrupp AG.

We carried out the audit during the period from August 2013 to November 2013 at the business premises of ThyssenKrupp AG in Essen, Germany, and our business premises in Hamburg and Düsseldorf with Prof. Dr. Böcking in Essen, Frankfurt a. M., and Heusenstamm.

The subject of this assignment is a joint audit of the following issues:

1. The suitability of the basic structure of the developed Internal Monitoring System within the Internal Control System (ICS) at ThyssenKrupp AG to prevent compliance breaches and its implementation in selected areas, if this has taken place, in accordance with auditing standard IDW PS 261 of the Deutsches Institut der Wirtschaftsprüfer (German Institute for Public Auditors).
2. The extent to which the recommendations declared in the audit report for the audit of the Compliance Management System (CMS) on the prevention of anti-trust and corruption breaches as per IDW PS 980 from September 30, 2011, have already been implemented.
3. The process of investment controlling for future large investment projects in accordance with the current Investment Guidelines and the process-independent auditing activity of the Internal Auditing department in projects of this type.
4. The provisions of the current information rules relating to follow-up reporting by the Board to the Supervisory Board as per section 90 (1) of the Stock Corporation Act (AktG) with the aim of checking that the Supervisory Board is guaranteed to receive due notice of significant budget overruns or other significant misdevelopments in future large investment projects.

The term "compliance" used in the report refers to the areas of anti-trust legislation and anti-corruption focused on by ThyssenKrupp and the shareholders (compliance in the narrower sense).

In accordance with this audit assignment for ThyssenKrupp AG, BDO carried out the audit for audit subject 1, which accounted for the major part of the audit. The audit subjects described in items 2 to 4 were audited by Prof. Dr. Böcking. The report for the audit subject 1 was created by BDO accordingly. The report relating to items 2 to 4 was created by Prof. Dr. Böcking.

The present report is based on our knowledge as at November 12, 2013. No investigations were carried out after this date. All statements made in this report relating to legal questions should be interpreted as pointers for legal monitoring. They do not represent legal advice.

The forwarding of the joint audit report or extracts thereof to a third party is prohibited without our prior written agreement. This excludes distribution to shareholders of the ThyssenKrupp AG before the next Annual General Meeting. There is of course nothing to prevent the audit report being forwarded if this is required by law.

The General Engagement Terms for Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften [German Public Auditors and Public Audit Firms] from January 1, 2002 and the Special Conditions for the Increase of the Liability under the General Engagement Terms as of January 1, 2002, which are included with this report, are valid for execution of the audit assignment and the liability of BDO AG - also with regard to third parties. The increase in liability is not applicable if a lower liability sum has been determined by law for a professional performance, in particular, for an audit required by law. The statutory liability rule applies in this case. Within the scope of the assignment, a special liability rule has been agreed for the execution of the audit assignment and the liability of Prof. Dr. Böcking. BDO and Prof. Dr. Böcking have been employed on the basis of separate assignments and do not have joint liability for the results represented in this joint report. It must also be pointed out that BDO and Prof. Dr. Böcking are only responsible and liable for the parts of the report that they have each created.

## II. Basis of information

Our knowledge and statements are exclusively based on information imparted verbally and on the data and documents provided to us. For the provision of information for the audit assignment, a data room was set up by ThyssenKrupp AG in which we reviewed all information.

During the audit we received and analyzed documentation from ThyssenKrupp, including the following:

- Guidelines and clarifying information leaflets
- Training materials
- Organizational instructions
- Operating procedures
- Internal notes (instructions)
- Company presentations
- Clarifying and explanatory company information
- Minutes
- Expert reports
- Written responses to questions

We documented the individual data and documents in detail in our working papers. All documents requested by us were made available promptly and - as far as we could judge - in full; we were also not hindered in our work.

During the audit we also spoke with employees from the following functional areas, amongst others

- Accounts Receivable
- Invoice Processing Deliveries
- Master Data

from ThyssenKrupp Business Services as well as with employees from the functional areas

- Corporate Function Controlling, Accounting & Risk
  - Department Performance Management & Controlling
  - Department Controlling Processes & Risk Management
  - Department Group Standards
- Corporate Function Internal Auditing
- Corporate Function Legal
- Corporate Function Compliance
  - Department Awareness & Prevention
  - Department Projects, Reporting & Processes
  - Department Investigations

from ThyssenKrupp AG, and with external consultants. In addition, a meeting took place with the Chief Financial Officer from ThyssenKrupp AG.

In our working papers, we documented the names of the employees from ThyssenKrupp and the external consultants with whom we held meetings.

ThyssenKrupp has also signed a declaration of completeness which confirms that, to the best of their knowledge, the documents required for carrying out the Special Audit were made available in full. In addition, it also confirms that all respondents have, to the best of their knowledge, informed us in full and truthfully of all facts in the documents provided that could have been relevant within the scope of the Special Audit but not evident.

## B. MANAGEMENT SUMMARY

---

### On audit subject 1

The subject of the first audit extends to the audit of the suitability of the basic structure of the developed Internal Monitoring System within the Internal Control System (ICS) of ThyssenKrupp to prevent compliance breaches and the implementation in selected areas, if this has taken place, in accordance with the auditing standard IDW PS 261 from the Deutsches Institut der Wirtschaftsprüfer (German Institute of Public Auditors).

### Internal control system - daproh

As part of the ICS, the Internal Monitoring System at ThyssenKrupp has been subject to an extensive revision process since 2012, known as the data and process harmonization (daproh) project. The aim of the project is to achieve globally consistent, standardized business, accounting and controlling processes across the entire ThyssenKrupp Group. At the time of our audit, the implementation phase had already started across five companies, however, it was not complete at any of the companies, and so, given the current status, we cannot make a conclusive statement on the implementation capacity. Therefore we recommend that the implementation is audited using a single company as a test case after successful completion of full implementation. In our opinion, companies in other countries which place both cultural and legal demands on an ICS would be appropriate for this purpose.

As planned, the completion of the daproh project should take place within three to five years after the Go Live of the pilot companies in September 2012. An estimate of whether this schedule can be considered realistic is currently only possible with some reservations. After looking through the project plan and the current status of implementation, we recommend a critical review of the schedule and, if applicable, modification.

The basis of the daproh project is a risk assessment for which ThyssenKrupp has decided on the Best Practice approach. In doing this, risks are only included if they have already been identified in similar companies. As a result of this approach, no systematic documented recording of risks has taken place yet. Therefore it has not been systematically established whether all relevant risks have been identified. In view of this, we consider the decision taken on the part of ThyssenKrupp, in short to carry out several self-assessments to complete the risk inventory, to be sensible and necessary.

At the time of our audit, the risk inventory included a total of 110 risks, two of which were assigned to the Compliance risk category by ThyssenKrupp. On the risk category all compliance-relevant risks basically belong to Compliance. Other risk categories are Operations and Financial Reporting.

According to our assessment, in addition to the two risks recorded during the risk assessment, other risks should be classified as compliance-relevant. As a result, we carried out a supplementary review and categorization of the risks and took into account all risks that we classified as compliance-relevant.

When auditing the controls assigned to the risks, we established that the control descriptions exhibited very different qualities due to the lack of defined minimum standards and sometimes did not fit the risks. In addition, there were risks that have been identified but which were not addressed by any controls. We recommend that for these cases, the design is further improved in spite of imminent implementation.

After consultation with ThyssenKrupp, ThyssenKrupp Business Services was suggested as the subject for the audit as, according to ThyssenKrupp, it was already advanced in the implementation process and was thus ready for an audit. During the audit of controls already implemented at ThyssenKrupp Business Services, we identified in random tests that the SAP authorization concept redesigned as part of the daproh project had been implemented according to specifications. The implementation of individual controls was partly executed. This was due to both the business model for ThyssenKrupp Business Services as well as technical difficulties in implementation.

#### **Internal Control System - Risk Management**

In its current form, the Risk Management System at ThyssenKrupp is to be viewed as a suitably arranged system which formulates group-wide standardized guidelines for the risk management process. In the risk inventory, which is carried out regularly, in addition to corruption and anti-trust breaches, other compliance-relevant information is also reported in the centrally specified risk categories and are thus integrated in the Risk Management System. The recording of individual risks using the bottom-up approach, which is carried out using a risk management tool, enables the appropriate consideration of individual compliance risks. At the time of the audit, a total of five compliance risks (anti-trust and corruption risks) considered at ThyssenKrupp to be significant were reported to the Risk Committee. Of these, three compliance risks were taken into account without a valuation as valuation-relevant information (e.g. the exercising of claims for damages) for drawing conclusions of the possible damages amount was not available. Adjustments relating to possible damages are continually reviewed at ThyssenKrupp and are arranged as soon as there are suitable information bases for this. To reinforce the link between the systems as intended by ThyssenKrupp, compliance risks identified during the further development of the ICS are also taken into account in Risk Management.

## Internal Control System - Compliance

As a result of breaches of anti-corruption and anti-trust legislation in the past, ThyssenKrupp have made the areas of anti-corruption and anti-trust the focus of their Compliance program. This is also reflected in the top-down risk assessment carried out in 2011. The systematic recording of the compliance risks from the bottom up has not yet taken place, however this is planned for 2014. We recommend that the systematic risk analysis planned by ThyssenKrupp for 2014 is carried out as planned.

Overall, it must be noted that there have been a variety of compliance-relevant measures in the area of Compliance since the breaches of anti-corruption and anti-trust legislation at ThyssenKrupp, and that these measures are, in principle, suitable for minimizing the risks in the areas of corruption and anti-trust legislation. Examples of these measures are the restructuring in the area of Compliance, which came into effect on October 1, 2013, the guidelines and leaflets in the areas of anti-corruption and anti-trust legislation, as well as the E-Learning and on-site training, which are obligatory for the relevant ThyssenKrupp employees according to risk.

Timely actions for improvement in the area of Compliance exist, in particular, with regard to the monitoring of the Compliance Managers employed in the individual group companies whose task it is, amongst other things, to publicize the Compliance Program and make it known at their local site. We also recommend that the positions of Regional Compliance Officer that are currently vacant should be filled. We also recommend the planned implementation of a web-based tool to carry out and check the prompt auditing of consultants/intermediaries and the expansion of the application area of the tools to other business partners, if applicable.

Overall, the Compliance function at ThyssenKrupp is organized correctly and has appropriate staffing. This finding was based on, amongst other things, a benchmark carried out in January 2013 to assess the compliance systems of several DAX 30 companies.

## On audit subject 2

An audit of the Compliance Management System (CMS) to prevent breaches of anti-trust and corruption legislation as per IDW PS 980 took place on September 30, 2011. As a result, the investigation relating to audit subject 2 should exclusively refer to the extent to which the recommendations made in the audit report relating to the CMS audit from September 30, 2011 have already been implemented.

Recommendations that can be rapidly implemented have been implemented since the completion of the KPMG audit as per IDW PS 980 on November 14, 2011. The implementation of more in-depth recommendations has started. The actions already implemented and those that have begun appear to be suitable for meeting the recommendations of KPMG and to be a suitable reaction to the two observations made by KPMG.

It must be noted that the restriction of the Corporation Function Compliance (CO/CPL) to the prevention of anti-trust and corruption infringements could result in questions and/or risks relating to differentiation and assignment as there is not always a clear distinction from other compliance questions. As compliance has played a major role in the context of preventing anti-trust and corruption infringements in the past, an additional recommendation may be appropriate in addition to those in the original audit subject 2 relating to the corresponding reproduction of the rules in the German Corporate Governance Code (DCGK) subitem 5.3.2 for the creation of reports for a Supervisory Board committee, e.g. to formally document the Audit Committee, for example, in the Rules of Procedure for the Audit Committee.

### On audit subject 3

Audit object 3 is the process of investment controlling of large investment projects in accordance with the current Investment Guidelines as well as the process-independent auditing activity carried out by the Internal Auditing department in projects of this type.

The process for the application and approval of large investment investments appears suitable. In the Investment Guidelines, a relatively low value threshold of EUR 25 million is applied for (large) investment projects, after which the investment must be approved by the full board. During the voluntary special audit, there were no circumstances found that indicated non-compliance with the investment guidelines. Sensitivity and scenario analyses are obligatory in the investment application, and an ex post audit of planning assumptions by means of an investment recalculation is also carried out if applicable. This is to be considered positive. During the execution of the investment, the regular revision of the effects of changes to the planning assumptions (e.g. market environment, market prices) on the efficiency of the investment project is essentially the responsibility of the Business Area; any possible depreciation requirement should also be identified.

Irrespective of the suitability of the controlling process, continual monitoring may be appropriate as a preventative measure for large investments with an application volume in excess of EUR 150 million - also taking into account technical issues - under the responsibility of the Corporate Function Controlling, Accounting & Risk (in other words, at the group level), as well as regular reporting of this to the Board and Supervisory Board and inclusion in the Investment Guidelines. From this investment level, in individual cases, external assessments of the technical feasibility or other specific aspects should be included and, if required, updated in specific time intervals. We were informed that the existing investment guidelines were currently being expanded to include a separate regulation for large investment projects in which the above-mentioned recommendations were being included.

The process-independent auditing activity carried out by Internal Auditing appears to be suitable. However, the status of Internal Auditing should be further reinforced. The corresponding guidelines should formally specify that budget overruns must be reported to Internal Auditing and that Internal Auditing receives immediate access to the investment database. The staffing levels for Internal Auditing should also be reviewed, specifically regarding the ratio to staffing levels in CO/CPL who concentrate on the prevention of anti-trust and corruption breaches at ThyssenKrupp. The differentiation between the areas of responsibility for the group functions Internal Auditing and Compliance should be more clearly represented in the Internal Auditing Guidelines. To upgrade the status of Internal Auditing within the framework of company-internal monitoring, a quarterly report by Internal Auditing to the Audit Committee of the Supervisory Board and the inclusion of the Audit Committee in the audit planning could be included in the Rules of Procedure for the Audit Committee.

## On audit subject 4

Audit object 4 refers to the provisions of the current rules of information for follow-up reporting by the Board to the Supervisory Board in accordance with section 90 (1) of the German Stock Corporation Act (AktG) with the aim of checking whether it can be guaranteed that the Supervisory Board will receive timely knowledge of budget overruns or other significant misdevelopments in future large investment projects.

With the "Monthly Executive Report (MER)", the Board provides the Chair of the Supervisory Board with an information base that enables a suitable target/actual analysis and which is suitable for identifying significant misdevelopments at the group level or at the Business Area level and/or give the Chair of the Supervisory Board cause to investigate the developments and request additional information.

The MER that has only been provided to the Chair of the Supervisory Board up until now could also be made available to members of the Audit Committee on a monthly basis as a step towards increasing monitoring efficiency. In addition, based on the follow-up report as per section 90 (1) of the German Stock Corporation Act (AktG) to guarantee the flow of information, it is worth considering that the Chair of the Audit Committee should also be a member of the Strategy, Finance, and Investment Committee so that accounting risks can be identified early.

In accordance with the recommendation for audit subject 3, it may be appropriate to include an additional investment level in the investment guidelines for large investments with an investment volume in excess of EUR 150 million. For investments at this level, regular reporting to the Supervisory Board, in particular in the case of budget overruns and other misdevelopments (e.g. technical problems) should also be included. This can take place via information to the relevant committees (e.g. Strategy, Finance, and Investment Committee and the Audit Committee). We were informed that the existing investment guidelines were currently being expanded to include a separate regulation for large investment projects.

## C. SUBJECT OF AUDIT

---

### I. Further development of Internal Control System (Audit subject 1)

#### 1. Audit assignment

The subject of the first audit extends to the audit of the suitability of the basic structure of the developed Internal Monitoring System within the Internal Control System (ICS) of ThyssenKrupp to prevent compliance breaches and the implementation in selected areas, if this has taken place, in accordance with the auditing standard IDW PS 261 from the Deutsches Institut der Wirtschaftsprüfer (German Institute of Public Auditors).

#### 2. Individual Audit Results

##### 2.1. Internal Control System - daproh

###### 2.1.1. Execution of audit

The Internal Monitoring System is a fundamental part of the ICS, as defined in IDW PS 261, which consists of process-integrated and process-independent monitoring measures. The process-integrated measures can be split into organizational safeguarding measures and controls.

Both types of process-integrated measure are undergoing an extensive revision process at the time of the audit at ThyssenKrupp, known as the data and process harmonization (daproh) project. The daproh project is scheduled for a period of three to five years and has implications for almost all areas of the ICS at ThyssenKrupp as well as on the processes and controls implemented. The documentation on the redeveloped Internal Monitoring System is also being revised and modified accordingly. Therefore, our audit took place within an on-going project with the focus on its design. It is envisaged that individual measures in the daproh project will be modified in turn to comply with the design. The recommendations resulting from our audit can thus be taken into account here.

When carrying out the audit we first viewed and evaluated the documentation provided to us by ThyssenKrupp. This documentation basically dealt with the design of the ThyssenKrupp "Richtlinie Internes Kontrollsystem" (Internal Control System Guidelines) together with an attachment from August 30, 2013, the Risk-Control Matrix from August 30, 2013, the SAP authorization concept "Authorization Concept for TK Group SAP ERP Template Production Systems" from August 2013, as well as several presentations on the status of the daproh project. To supplement this, we also held meetings with employees from ThyssenKrupp as well as with external consultants employed by ThyssenKrupp as part of the daproh project.

To check the actual implementation of the control mechanisms in a selected pilot company, on the suggestion of ThyssenKrupp, we agreed to use ThyssenKrupp Business Services GmbH (ThyssenKrupp Business Services), Essen as the subject of the audit. For this part of the audit, we held meetings with employees from ThyssenKrupp Business Services as well as audit meetings on site in the company premises. To test the implementation of individual controls in the SAP system, we, together with external consultants, were given an overview into the SAP productive system. For the results of our audit of actual implementation, please see item 2.1.5.2. of this report.

Finally we assessed the status quo and gave recommendations for the improvement of the existing risk-minimizing controls.

## **2.1.2. Fundamentals of the Internal Control System**

### **2.1.2.1. Actual situation at the time of audit**

The ThyssenKrupp "Richtlinie Internes Kontrollsystem" (Internal Control System Guidelines), the attachment to these guidelines and a Risk-Control Matrix form the basis for the ICS at ThyssenKrupp. At the time of the audit, these had not yet been released and were still in the draft stage ("draft guidelines").

The draft guidelines should regulate the framework conditions for fulfillment with the requirements for a proper ICS throughout the whole of ThyssenKrupp that is consistent across the group, and serve as a guide for handling the inherent risks of basic business processes. The draft guidelines define the ICS as all principles, processes, and measures introduced by ThyssenKrupp that target the organizational implementation of Management decisions for achieving the following categories of objective:

- business objectives, such as securing the effectiveness and efficiency of the business processes,
- reporting (the accuracy and reliability of internal and external reporting) and
- rule compliance (compliance with the legislation and regulations relevant to ThyssenKrupp).

The attachment to the ICS Guidelines specifies the target groups and the validity area of the ICS. The implementation of the requirements of a daproh system in the operating units is also described here (see also item 2.1.4.4). The main features of other authorizations in extraordinary situations are also shown. In the Risk-Control Matrix, all identified risks are listed with their corresponding control actions (see also item 2.1.4.2).

### **2.1.2.2. Assessment and recommendation**

The draft guidelines represent an essential base for the ICS at ThyssenKrupp. Therefore we recommend that it is approved by the Board soon and communicated to all employees.

The draft guidelines are deliberately very short and only contain a description of the general objectives and validity area. There is also a short explanation of the aim of the Risk-Control Matrix and a reference to it. References to further applicable guidelines and process instructions, for example, the attachment to the ICS guidelines are not yet included. We recommend that the content of the guidelines is expanded. In particular, references to all relevant ICS documents, and thus the conceptual bases that are a fixed component of the ICS, should be included.

### **2.1.3. Principles and aims of the daproh project**

#### **2.1.3.1. Actual situation at the time of audit**

Within the daproh project, standardized business process that are consistent around the world, together with consistent accounting and controlling processes, should be defined and implemented for the entire ThyssenKrupp Group. This should lead to increased transparency and a reduction in complexity and costs. The aim of the daproh project is that all ThyssenKrupp companies within the group achieve the daproh standard.

Essential milestones within the daproh project are the introduction of the SAP/ERP template for ThyssenKrupp, which should take place in February 2014, as well as the completion of the entire daproh project which was originally planned to take place within three to five years after the Go Live for the pilot companies in September 2012.

Key elements in the daproh project are the automatic, standardized processing of orders with integrated finance and controlling processes, the guarantee of compliance, the minimizing of risks in company processes as well as automatic, efficient accounting and reporting processes.

At the time of our audit, the further development of the ICS as part of the daproh project is partly implemented. The SAP ERP template has already been implemented at five companies in Germany and the USA. The roll-out at these companies began in October 2012. However some elements are still in the test phase (cf. also item 2.1.5.2.). A further essential roll-out began in October 2013 at a Chinese group company. Several analyses are currently running in parallel in all areas of the group with the aim of driving through the implementation of daproh requirements across the group.

The ICS-relevant elements are represented as follows within the daproh project at ThyssenKrupp:

- Process Controls
- Segregation of Duties
- Controls for the Authorization of Critical Transactions
- IT Security of ERP Systems

Within the daproh project, the area of Process Controls represents the monitoring of the effectiveness of essential controls in business processes. This is carried out integrated within the process and also through downstream function tests.

In this context, the subarea Segregation of Duties regulates the requirements for the separation of incompatible functions and tasks in the SAP system.

The Key Group Requirements form the basis of the ICS. These are basic standards and rules that every group company must fulfill and comply with to conform with daproh and thus, by definition, provide a proper and appropriate ICS. The Key Group Requirements were formulated as part of the daproh project and they are based on the information provided from the experience of proven methods.

In addition to the daproh subareas, the ICS at ThyssenKrupp also consists of other upstream and downstream systems containing control elements. However, these are not the subject of our audit assignment.

#### **2.1.3.2. Assessment and recommendation**

The worldwide implementation of a revised ICS represents a complex task in which delays and difficulties in individual project phases cannot be avoided. As a result, a final audit of the project status could also not be carried out. With regard to the implementation capability in particular, an audit today would still only be possible with certain restrictions due to the on-going implementation. This implies in particular that both risks as well as controls were still changed during the course of the audit. We basically recommend that the structured project retrospective already taking place is continued consistently and that the knowledge from completed roll-outs is taken into account to a greater extent. We also recommend that the audit of the implementation capability, for example, in other countries, is carried out as soon as this appears feasible.

In doing this, the different cultural and legal requirements of an ICS should also be taken into account.

## 2.1.4. Elements in the daproh project

### 2.1.4.1. Risk assessment

#### 2.1.4.1.1. Actual situation at the time of audit

A Risk Assessment represents the first phase and thus the basis for the daproh project. In doing this, a Best Practice approach is selected. This is based on the experience of proven methods, whereby the risks recorded are those risks that are generally to be expected at comparable companies with similar business processes. The completion of the Risk Assessment is supported by external consultants. Recorded risks are classified in a second step according to the categories of the COSO framework. The framework concept supports companies in developing, implementing, and monitoring the effectiveness of internal controls. The three following categories are identified:

- "Financial Reporting",
- "Operations" and
- "Compliance"

At ThyssenKrupp, there was a further differentiation of the categories into "Financial Reporting" and "Non-Financial Reporting" at the start of the audit and some risks were assigned to the latter category. However, during our audit, ThyssenKrupp decided to merge these categories into one category and thus fully comply with the categories of the COSO framework.

Overall, during the Risk Assessment, 110 risks were documented by ThyssenKrupp for the processes Order to Cash, Purchase to Pay, Asset Accounting, Cash & Banking and Period End Closing. As this process is still on-going, the number of risks is subject to change. Of these 110 risks, two were assigned to the COSO category Compliance at the time of our audit. However, compliance-relevant risks are also included in other categories. We also selected all risks classified by us as compliance-relevant from other categories and the accompanying controls as the bases for our audit.

The identified risks and their classification are represented in a Risk-Control Matrix. An explanation of the structure of the Risk-Control Matrix can be found below under item 2.1.4.2.

#### **2.1.4.1.2. Assessment and recommendation**

As a result of the Best Practice approach selected by ThyssenKrupp for the Risk Assessment, no systematic recording and evaluation of the risks has yet been carried out and documented. Therefore at the time of the audit we could not make a final assessment of whether all relevant risks that should be taken into account in a centrally designed ICS had been fully recorded. To ensure complete compilation of the risks, we recommend including relevant risks by means of a run-through of the different company processes to be taken into account and structuring them according to the process flow. In addition, Risk Assessments from other corporate functions, for example, the Corporate Function Compliance (CO/CPL) could also be used to identify compliance-relevant risks. In the course of our audit, ThyssenKrupp had already decided to carry out several self assessments in the short term to test, and if necessary complete, the existing risk inventory which will, in our opinion, contribute to a quantitative and qualitative improvement in the recorded risks.

According to our assessment, in addition to the two risks recorded during the risk assessment, other risks should be classified as compliance-relevant. We recommend that the classification of the risks in the COSO categories is critically reviewed once more to identify other compliance-risks as such. We also recommend, if applicable, close coordination with CO/CPL. There are also risks that primarily address other objectives (e.g. Financial Reporting), but which also include compliance risks. We recommend that these risks are also classified as compliance-relevant by the creation of a sub-category to make the user of the Risk-Control Matrix more sensitive to compliance-relevant issues.

The risk descriptions formulated as part of the Risk Assessment are deliberately very general and broad. With a view to clarifying the definition and implementation of specific control activities, we recommend - where possible and necessary - that the risks are described in more detail and that a precise restriction to one specific risk set is made to enable a precise link between the risk and control.

#### **2.1.4.2. Risk-Control Matrix**

##### **2.1.4.2.1. Actual situation at the time of audit**

The Risk-Control Matrix contains all risks identified during the Risk Assessment and represents a central component of the ICS. In total at the time of the audit there are 110 risks in the Risk-Control Matrix.

In the Risk-Control Matrix, a control objective is first assigned to the risks. Furthermore, controls are also assigned to each risk which should minimize the respective risk. There are two different control descriptions for each risk, the "control description (general)" and also the "control description (daproh)". The control description (general) should represent a corresponding "system-neutral" formulation of the daproh control which can be developed individually by a group company (see also item 2.1.4.4.1).

The included daproh controls can be split into Process Controls and Group Rules. One or more Process Controls and/or Group Rules can be assigned to one risk so that there is not necessarily a one-to-one relationship between risks and controls.

### Process Controls

With regard to the concept of Process Controls, this is a system that should automatically uncover weaknesses and deficiencies in the work processes and business processes. For this purpose, reports displaying the results of a control are generated from SAP at defined intervals and processed by employees with responsibility for it.

There are two types of Process Control; fully automatic Process Controls and semi-automatic Process Controls. Both types of Process Control are carried out automatically by the SAP system at regular intervals. Differences between the fully automatic and semi-automatic Process Controls arise with regard to the requirement for a review by an employee from the operating unit in question, the so-called Review Party. With semi-automatic controls, the Review Party must review the hits displayed in the report to determine the causes of the hits. With the fully-automatic controls, each of the hits identified by the control is a deficiency for which further processing is coordinated by the Company Control Officer and cleaned up by the Remediator.

Furthermore in attachment 6 to the Risk-Control Matrix, a control frequency is specified for each Process Control which determines how frequently it is carried out. The control frequency can be daily, weekly or monthly. It is also defined here whether the Process Control is a detective or preventative control. In addition to the "control description (general)" and the "control description (daproh)", the Process Controls are also defined by the technical and content descriptions of the individual controls which are, however, not part of the Risk-Control Matrix and are also not specified here.

### Group Rules

Group Rules are basic specifications that apply across the group and must be observed by all companies to enable a proper ICS. The Group Rules are divided into different categories such as Accounting/Controlling, IT and Group Master Data.

As part of the daproh project, specifications in the SAP ERP system should ensure that the Group Rules are observed in the respective operating units. For operating units that do not use a SAP system, please see the remarks under item 2.1.4.4.1.

#### **2.1.4.2.2. Assessment and recommendation**

The version of the Risk-Control Matrix available to us at the time of audit includes five risks for which no control descriptions (daproh) have yet been defined. Here we recommend that a formulated control description (daproh) is documented for all identified risks included in the Risk-Control Matrix to ensure completeness of the Risk-Control Matrix and thus reduce the corresponding risks due to controls.

Furthermore we have established that both the control description (general) and the control description (daproh) are only briefly recorded in the Risk-Control Matrix and that the content has a different structure. We were told that ThyssenKrupp deliberately decided on the short formulation and has provided more detailed descriptions in other documents. In our opinion, however, the short descriptions could make it more difficult for the addressee of the Risk-Control Matrix to understand the risks and corresponding controls. We recommend that the control descriptions are expanded. In particular, minimum requirements should be defined for the description of controls to achieve a consistently high quality standard for the control descriptions. In principle, as a minimum requirement, the control description should include the performer (role description), specific control activity, time of control, aim of the control, as well as the procedure to follow if deviations are identified.

When looking at the Process Controls we also established that both the fully automatic and semi-automatic Process Controls are downstream controls that check in retrospect whether breaches have occurred. All Process Controls thus have a detective nature. However, sometimes in the Risk-Control Matrix, they are flagged as preventative controls. We recommend that Risk-Control Matrix is subject to a critical review in this regard.

We also found that the Group Rules were sometimes more like basic specifications. We recommend that these are included in process instructions, guidelines, or similar instead.

In individual cases, the link between the content of the Group Rules and the risk it should address was not clear. In these cases we recommend that the Group Rules are modified to this effect and the formulations clarified to better emphasize the link between the risk and the Group Rule.

#### **2.1.4.3. Authorization Concept / Segregation of Duties**

##### **2.1.4.3.1. Actual situation at the time of audit**

A significant part of the ICS redesigned as part of the daproh project is the "Authorization Concept for TK Group SAP ERP Template Production Systems", which is available to us in the version from "August 2013". The aim of the document is to define and describe the daproh authorization concept for the "TK Group SAP ERP Template".

The document describes a four-stage authorization concept. Each user is assigned four roles which each have different authorizations according to the department and position. This should enable employees to carry out their tasks. The individual roles are:

- the "System Common Role" (level 1) includes basic authorizations and is assigned to all users;
- the "Process Common Role" (level 2) only contains read authorizations assigned to all employees in a specific SAP module;
- the "Job Function Role" (level 3) includes the authorizations that allow an employee to carry out specific tasks and is only assigned to individual employees, and
- the "Hierarchy Role" (level 4), which is basically used to allocate authorizations according to profit and cost centers and also segments.

"Supplemental Roles" can also be assigned. These include authorizations for very specific transactions that require specific controls and which only individual employees should have access to.

There is also Emergency User Management. Fire Fighter roles are created in the system and they contain extensive authorizations and, if employees with specific authorizations are absent, this ensures that there is no interruption to the business process. We were told that the Fire Fighter role should only be allocated with significant restrictions. All transactions carried out using this role are also logged.

There are also areas outside of the SAP system in which segregation of duties is necessary. These areas are subject to decentralized regulation and are not included in a central concept. The segregation of duties between the different responsibilities in the area of Process Control should be mentioned here whereby the functions of the Company Control Officer, Reviewer, and Remediator are differentiated. The responsibilities of the positions are specified and differentiated from each other in the attachment to the ICS Guidelines.

#### 2.1.4.3.2. Assessment and recommendation

The four-stage "Authorization Concept for TK Group SAP ERP Template Production Systems" enables the transparent assignment of authorizations in the SAP system. The concept basically ensures that employees cannot have a critical combination of authorizations or authorizations that do not correspond to their tasks. To guarantee all authorizations within a global implementation, exceptions and the corresponding assignment of separate authorizations may occur. Therefore, with a view to the current status of implementation at the time of the audit, naturally no statement can be made regarding the time of complete implementation of the authorization concept.

There is not yet a central document on the segregation of duties for the area of the ICS which addresses, for example, roles both in the system as well as in the context of Process Control and also in other areas in which segregation of duties is necessary. We recommend that all rules relating to segregation of duties are summarized in a central document as the segregation of duties is an important criterion for safeguarding against compliance risks.

#### 2.1.4.4. The procedure for practical implementation

##### 2.1.4.4.1. Actual situation at the time of audit

Due to the different development statuses and specifications of the different ICSs, as well as the ERP systems in the individual ThyssenKrupp group companies, the implementation of the daproh project requires a differentiated procedure. In the attachment to the ICS Guidelines, there is, therefore, a distinction in the way in which the requirements are implemented. This is dependent on the respective development status with reference to the connection of the respective companies to a daproh system.

There are three different procedures:

##### Connection to a daproh system:

If the company is connected to a daproh system, it is called a daproh company. In these cases, the special SAP authorization concept is used in the companies together with the SAP Process Controls. This means that the following points must be guaranteed for the area of segregation of duties in SAP:

- Only standardized global SAP roles may be used.
- There must be no conflicts in the segregation of duties at the user level and/or these must be approved and be subject to compensating controls (mitigation).
- All requirements relating to Emergency User Management specified in the attachment to the ICS Guidelines must be observed.

Partial connection to a daproh system:

If the company is only partly connected to a daproh system, it is called a non-daproh company. With regard to the SAP authorization concept, at these companies the Group Standards department decides individually for each company whether there is a need to implement and/or expand the following requirements until a daproh system is connected. The specific requirements are:

- The ERP system must be connected to the central SAP system for the allocation of authorizations.
- After connection, all breaches of rules relating to the segregation of duties in the SAP Basis and Purchasing regulation sets must be resolved.
- The operating units are obliged to record risks from their own developments in additional Segregation of Duties regulation sets.
- Emergency User Management must be set up in compliance with all requirements specified in the attachment to the ICS Guidelines.

No connection to a daproh system:

Companies who are not connected to any daproh system are also known as non-daproh companies. These companies do not use the SAP Process Controls. Instead, a decentralized approach is followed. This approach intends for the companies to carry out a self-assessment against the Risk-Control Matrix. In doing this, it is within the area of responsibility of the respective management teams for the operating units to introduce appropriate control measures and to ensure that the control objectives specified in the Risk-Control Matrix are achieved.

#### 2.1.4.4.2. Assessment and recommendation

The different methods of implementing a daproh-compliant ICS at the various ThyssenKrupp group companies take into account the heterogeneous current situation in the area of the existing ICS and ERP systems to an appropriate extent. They also enable the companies to achieve the objective of the daproh project in different ways.

## **2.1.5. Review of the practical implementation at a selected pilot company**

### **2.1.5.1. Actual situation at the time of audit**

Due to the fact that the implementation process was not yet complete at the time of the audit, the audit could only be carried out in one of the five companies at which the daproh roll-out had already started. As a result, with the agreement of ThyssenKrupp AG, the audit of the daproh implementation was carried out at ThyssenKrupp Business Services in Essen.

ThyssenKrupp Business Services basically carries out selected administrative services in the areas of Finance and Human Resources for domestic ThyssenKrupp companies. This includes support processes. These are batch and competence-based processes that do not belong to the core activities of the ThyssenKrupp group companies.

### **2.1.5.2. Assessment and recommendation**

With regard to the implementation of Process Controls in the company audited by us, ThyssenKrupp Business Services, we established that the majority of the Process Controls have been implemented. These non-implemented controls exist for one of the following reasons: these controls have been initially deactivated following the generation of incorrect reports, they cannot be implemented due to technical difficulties in the implementation, or they are still in the test phase. We recommend that implementation of these Process Controls is completed soon and in full. This applies in particular to companies such as ThyssenKrupp Business Services, which has already been in the introductory phase for one year.

All Process Controls included in our random test are currently only carried out on a weekly basis at ThyssenKrupp Business Services, irrespective of the intended control frequency for the respective control that is specified in the Risk-Control Matrix. We recommend that the controls are carried out in the frequency defined for each Process Control to generate maximum protection from the implemented controls.

In addition, during our audit we established that no hits were generally expected for some of the implemented Process Controls. In these cases, we were told that control activities had already been carried out by the preliminary system, however, they are not specified in the Risk-Control Matrix. It was not possible to audit the suitability of the implemented controls within existing preliminary systems within the framework of the time-limited special audit.

Our random review of the implementation of the manual part of the semi-automatic Process Control by the Review Party at ThyssenKrupp Business Services showed that the actual implementation of the manual control actions did not follow any standard specifications for execution and documentation. The type and manner in which the audit activities carried out are documented is also dependent on the employee of ThyssenKrupp Business Services who is carrying out the activity. In our opinion, this is due to the fact that the daproh control descriptions describe the manual part of the controls only in general terms or not at all. To achieve a consistent procedure in these cases, we recommend that each control description should contain at least the following information:

- Specification of the position of the person carrying out the activity  
Here there should be a clear reference to the underlying concept or the underlying role description.
- Execution procedure  
A clear procedure should be defined for carrying out the individual control activities.
- Documentation of controls  
The type and scope of documentation should be defined.
- Deadlines for processing  
Specific deadlines for processing a list should be defined and documented.
- Escalation  
Clear specifications should be defined for escalation following violation of a rule.

To carry out the semi-automatic Process Controls we have identified that there is not always segregation of duties between the administrator and the Review Party. As a result, it is possible for employees to review their own processes as a Review Party. In the context of the Double-Verification Principle, this is considered to be inappropriate. Therefore we recommend that the strict separation between the Administrator and the Review Party is critically reviewed and assured.

Our review of the implementation of the Group Rules at ThyssenKrupp Business Services showed that not all Group Rules have been implemented there. This is because some have not yet been technically implemented, they are not intended for implementation due to the business model of ThyssenKrupp Business Services, or they are not yet in the test phase. Like our recommendation for the Process Controls, we also recommend in this case that the implementation of the Group Rules is completed in full in the near future. With regard to the Group Rules already implemented, in a random test we were able to establish that they correspond to the concept with regard to their function.

We were told that the SAP authorization concept in the company audited by us had been rolled out according to the specifications. Following a random review in the area of master data changes, we did not find any evidence to contradict this statement.

## 2.2. Internal Control System - Risk Management

### 2.2.1. Execution of audit

At the time of the audit, the Risk Management System at ThyssenKrupp was represented in the "Konzernrichtlinie Risikomanagement" (Risk Management Group Guidelines). Version 2.0 of the Guidelines has been released since July 10, 2012, and was used by us as the basis for the audit. Meetings were also held with employees and we were given an overview of the tool implemented at ThyssenKrupp for recording risks.

### 2.2.2. Actual situation at the time of audit

#### 2.2.2.1. Design of Risk Management System

The Guidelines represent the policies implemented at ThyssenKrupp relating to risk policy. They describe a risk as a threatening event or threatening development that has a significant effect on an organization achieving its objectives and thus achieving its overall objectives. Risk Management is viewed as the set of all measures that correspond to the systematic and transparent handling of risks. At ThyssenKrupp, Risk Management is implemented with an integrated controlling approach. Therefore it is also used as a control instrument in Controlling and value-oriented company management.

The Risk Management System at ThyssenKrupp is positioned in the area of Controlling, Processes & Risk Management. The Risk Management System is designed as a combined top-down and bottom-up approach. With this approach, binding specifications are formulated as part of the top-down approach, however, the responsibility basically lies with the specialist person responsible for the operating units. The operating units also name Board or Management members as persons responsible for Risk Management. Responsibility at the group level lies with the Chief Financial Officer (CFO).

The Risk Management System for ThyssenKrupp consists of five separate elements shown individually below:

- Opportunities and risks in projection:

The identification and evaluation of opportunities and risks with reference to Earnings Before Interest and Taxes (EBIT) and Business Cash Flow (BCF) for the current reporting month.

- Opportunities and risks in budgeting:

Identification and evaluation of opportunities and risks with reference to EBIT and BCF that have not already been included in the budget.

- Risk inventory:

Within the Risk Inventory, all risks are identified with the aim of recording all significant risks. The result should be the identification and evaluation of risks with reference to EBIT and BCF that have not already been included in the projection or planning. In addition, the risk cause (internal/external) and risk category (implication/relevance for ThyssenKrupp) are determined and the risk effect forecast. Finally, the risks are clustered according to common group threshold values and materiality thresholds with regard to the probability of occurrence and amount of damage. The Risk Inventory is compiled at least twice a year.

The risks are identified using a cross-group Risk Cockpit (RMS Tool) introduced in 2010, whereby all individual risks are entered and compiled. The user must enter information relevant to the risk, category and cause, a risk description, and a person responsible. The information required for the risk evaluation includes the expected net damages and the probability of occurrence. The risk class, which is classified both at the Business Unit level and at the Group level, is calculated automatically by the system. In addition to explanations on the derivation of the damage, qualitative risk effects in the case of a possible realization of the risk are recorded and arranged into predefined effect groups. In addition, planned, on-going, and implemented actions can be recorded and any relevant insurances can be included in the description of risk minimization. Additional descriptions, possible attachments and early warning indicators complete the entry screen.

- Risk scenarios:

Within the risk analysis, portfolio risks should be determined on the basis of predefined risk scenarios. Possible risk scenarios are recorded on a quarterly basis using a standardized process. In doing this, the main activities, results, and specific responsibilities are assigned to each process step. Macroeconomic risk scenarios are shown in country-specific matrices to determine any required measures. Risk scenarios are carried out at least once per year.

- Risk reserves:

Risk reserves contain accounting risks. These should be identified and recorded as individual circumstances by the filter logic. The consideration of accounting risks flanks the risks already identified in the risk assessment and should help the analysis of important reserves for risks as well as monitoring of measures. Analyses of risk reserves are carried out four times each year.

#### **2.2.2.2. Reporting and monitoring**

The elements "Opportunities and risks in projection", reporting interval once per month, and "Opportunities and risks in budgeting", reporting interval once per year, are part of standard reporting. Reporting of the "Risk inventory" element, "Risk scenarios" and "Risk reserves" is carried out four times each year for both the separate Risk Committee and the Audit Committee. The Risk Committee evaluates the material group risks from the risk inventory process, the risk reserves and risk scenarios, and assesses the suitability and implementation status of the measures taken.

#### **2.2.2.3. Compliance interfaces**

The Risk Committee forms the interface to Compliance as part of the organization of the Risk Management System at ThyssenKrupp. There, as a result of the top-down perspective, changes to the significant group risks can be dealt with over time by listing the significant risks and monitoring them across a defined period of time. Compliance risks should be recorded by the line managers of the ThyssenKrupp Group during input via the Risk Cockpit. There are four predefined categories for recording compliance risks: Anti-trust legislation, Anti-corruption, Other legislation, and Group guidelines. At the time of audit, there were a total of 49 risks in the four categories. Of these, five compliance risks were reported as significant group risks in the Risk Committee. Three compliance risks cover existing risks from possible breaches of anti-trust legislation, the fourth risk comprises downstream legal disputes as a consequence of breaches of anti-trust legislation. The fifth risk contains general risks from breaches of anti-trust legislation as well as breaches caused by corrupting behavior, together with breaches of valid anti-trust and corruption legislation. In the context of compliance and the group guidelines, the risk control measures taken into account here relate, in particular, to compliance with anti-trust legislation, to fighting corruption in business transactions, and on personal conduct when dealing with business partners, as well as the integration of intermediaries, consultants, and other persons commissioned for sales support.

The release of the risks in the RMS Tool should be carried out using the Double-Verification Principle. Corresponding procedures were presented to 400 line managers and users in web and on-site training.

#### **2.2.3. Assessment and recommendation**

Within the Risk Management System at ThyssenKrupp, a clear risk organization with corresponding responsibilities is defined in writing and communicated. The responsibility lies with the person responsible for the operating unit and with the CFO at group level.

The identification of risks is carried out across the group using a Risk Cockpit, which appears to be appropriate for the adequate recording of risks. The risks can be evaluated using predefined classifications. At the time of the audit, a total of five compliance risks, which are currently considered by ThyssenKrupp to be significant, were reported in the Risk Committee. Of these, there are three compliance risks that could not be evaluated with regard to the amount of damages due to the lack of details or relevant information at the time of compilation. These were initially included without a specific amount stated and modified according over time. In the case of the reported compliance risks, there was a focus of the areas of anti-trust breaches and corruption. To reinforce the link between the systems as intended by ThyssenKrupp, compliance risks identified during the further development of the ICS are also taken into account in Risk Management.

## 2.3. Internal Control System - Compliance

### 2.3.1. Execution of audit

The Internal Monitoring System is a fundamental part of the ICS, as defined in IDW PS 261, which consists of process-integrated and process-independent monitoring measures. We have defined the area of Compliance as part of the process-independent monitoring measures. At ThyssenKrupp, Compliance focuses on the areas of anti-trust legislation and anti-corruption (compliance in the narrower sense).

Building upon this, we identified six Compliance-relevant areas which we included in the audit of the ICS - Compliance Management System (CMS). The following areas were included in the scope of the audit:

- Training program: E-Learning and on-site training;
- Concept and suitability of Business Partner Checks/Business Partner Screenings;
- Compliance-relevant guidelines;
- Compliance Case Management, Compliance Reporting including the whistleblowing concept, and the follow-up process and Compliance Audit;
- Functionality of Compliance Consulting;
- Structure of Compliance Organization.

The objective of the analysis of these areas is to depict the risk-minimizing measures at ThyssenKrupp in the area of ICS - Compliance that have been implemented for the individual areas.

To establish this, in the first step we captured and represented the actual situation in the specified areas. To do this, we evaluated the documents provided to us by ThyssenKrupp and held meetings with employees from ThyssenKrupp who are responsible for the individual areas. During the audit, the focus of consideration was the audit of the processes. An in-depth audit of the content of the measures to reduce risks in the areas of anti-trust legislation and anti-corruption was not the primary concern here.

In a second step, we assessed the actual situation we had found and, where applicable, made recommendations for the further improvement of the existing risk-minimizing measures and/or for possible additional measures that have not yet been implemented.

As a result of breaches of anti-corruption and anti-trust legislation in the past, ThyssenKrupp have made the areas of anti-corruption and anti-trust the focus of their Compliance program. This is also reflected in the top-down risk assessment carried out in 2011. No systematic bottom-up risk analysis has yet taken place, however, this is planned for the calendar year 2014.

We consider the planned bottom-up risk analysis to be necessary. We are told that this will take into account the following points:

- Recording of objective risk indicators;
- Recording of business-model-specific risk indicators/Red Flags;
- Self-assessment of defined corruption and anti-trust legislation risks.

Hereafter we always use the term "group-wide" with reference to the entire ThyssenKrupp Group with the exception of the North America region (USA and Canada). This region has its own Compliance Program. However, we were told that the Compliance Program at ThyssenKrupp will soon also include the North America region.

## **2.3.2. Compliance Organization**

### **2.3.2.1. Actual situation at the time of audit**

The Corporate Compliance Office is located at the group headquarters in Essen.

In accordance with the Compliance Organization valid since October 1, 2013, CO/CPL is split into three areas (Corporate, Business Areas, Regions) that are subordinate to the Chief Compliance Officer.

- Area: Corporate  
From an organizational viewpoint, at ThyssenKrupp there are four Corporate Departments: "Awareness & Prevention", "Projects, Reporting, Processes", "Investigations" and "Regions". A Compliance Officer heads each of the departments. In the future, "Investigations" should be supported in its activities by two Regional Hubs currently under construction in China and North America.
- Area: Business Areas  
ThyssenKrupp has divided up its business into a total of five Business Areas (Business Area Components Technology, Business Area Elevator Technologies, Business Area Industrial Solutions, Business Area Material Services, and Business Areas Steel Europe). There is also the Business Area Steel America (discontinued) and the Corporate area, incl. the Corporate companies. A Business Area Compliance Officer and up to six further Compliance Officers (all full-time) are responsible for each of the specified Business Areas. Currently two of the five Business Area positions are vacant, however, we were told that they will soon be filled. Substitution rules exist for the vacant positions.
- Area: Regions  
Geographically, for the purposes of the Compliance Program, ThyssenKrupp is split into twelve regions. One or more Regional Compliance Officers are responsible for each region. The regional subdivision is shown below: Spain/Portugal, Italy, Russia/CIS, China, India, Asia/Pacific, North America, Middle East/North Africa, Eastern Europe, Brazil, France, and Turkey. With regard to the organization, the Regional Compliance Officer is subordinate to the Department Regions within the CO/CPL/ Within the scope of responsibilities, ThyssenKrupp follows a "First point of contact" approach. In accordance with this, a contact person (Regional Compliance Officer) is specified for each of the above regions. Countries to which no Regional Compliance Officer is assigned are looked after by the respective Business Area Compliance Officer. Criteria for the responsibility of a Regional Compliance Officer for a region and/or country include cultural conditions and regional aspects. There is no mathematical approach for the measurement of the number of Compliance employees in the individual regions. Criteria include the turnover in the country, the CPI, a White-Spot analysis, and the number of group companies in the region in question.

The Compliance Officers are supported by the Compliance Manager employed at the individual group companies. The Compliance Manager is generally the CFO of the group company. We were told that there are currently 320 Compliance Managers (as at September 30, 2013) in around 420 positions which is due to the fact that a Compliance Manager can also be responsible for several group companies. The centrally devised Compliance specifications are implemented on-site by the Compliance Managers.

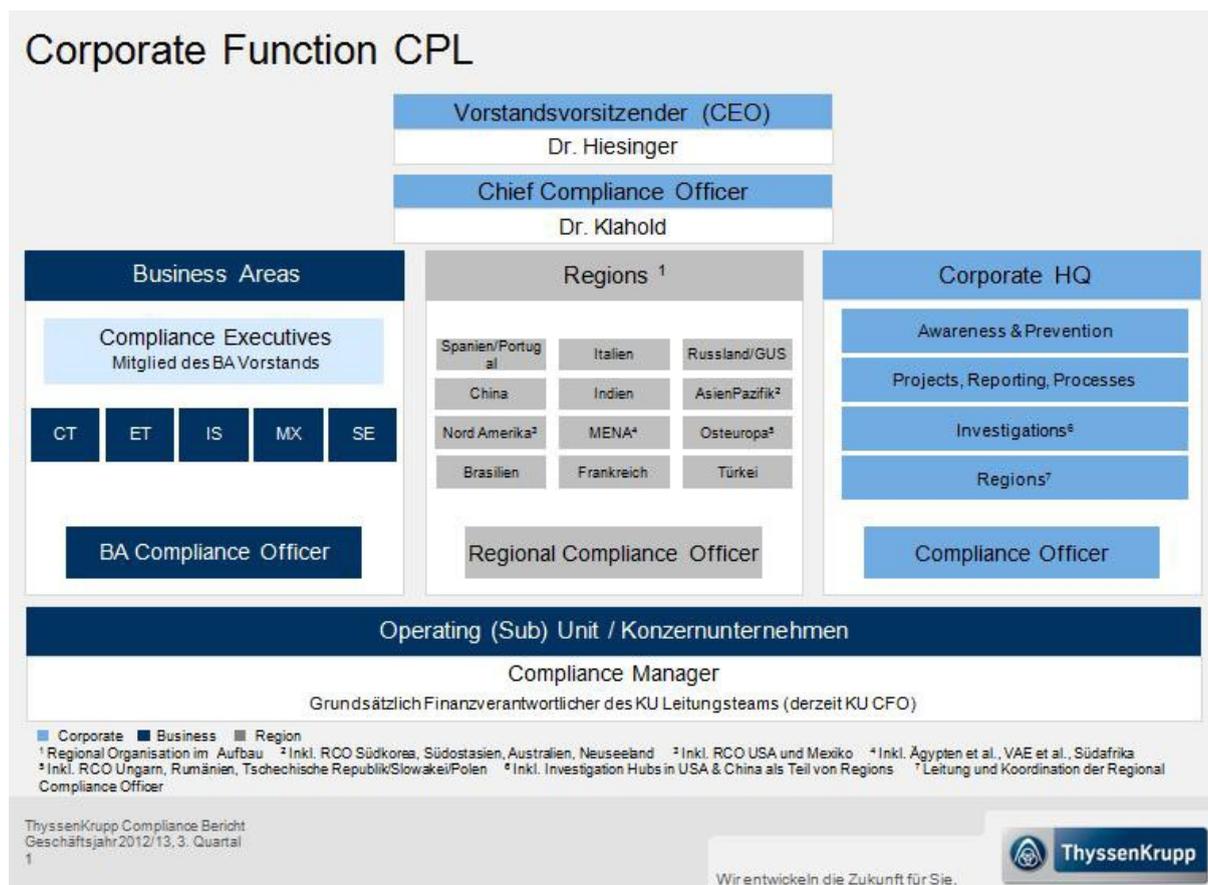


Illustration 1: Overview of the Structure of the Compliance Organization at ThyssenKrupp, as at October 1 2013

We were told that the Compliance Managers are appointed as follows: For each active group company, a Compliance Manager is nominated in consultation with the responsible Compliance Executive of the respective Business Area and the Compliance Officer. This person is often a member of the Executive Board, preferably the Chief Financial Officer, who is responsible for the area of Compliance in addition to their other tasks. In individual cases, the Compliance Manager is responsible for several group companies. If, in exceptional cases, no explicit nomination has (yet) taken place, the CEO will take on the position of Compliance Manager for the respective group company in the interim.

When the Compliance Manager for a group company is appointed, the employee in question receives a "Welcome Package" containing general information on the function and range of tasks of the Compliance Manager. At the same time they are informed via e-mail that they will soon be invited to participate in the E-Learning offering "Role and function of Compliance Managers".

According to the benchmark analysis for Compliance Staffing Levels carried out in January 2013 for several DAX 30 companies, ThyssenKrupp is above the DAX 30 average of 28.5 with regard to the absolute number of Compliance Officers with its planned target of 51 employees which should be achieved after the ACT restructuring on October 1, 2013. As a result of the Compliance Organization, ThyssenKrupp also has over 337 Compliance Representatives who have secondary responsibility for compliance (as at January 2013). In this case, the average for the DAX companies participating in the Benchmark test during the survey period was 77.2. In terms of turnover, this gives a figure of 51 Compliance Officers 12.7 Compliance Officers per EUR 10 billion (planned target after ACT restructuring). This value is below the average for the benchmark participants, which was 16.5.

ThyssenKrupp plans to have 33.5 Compliance Officers per 100,000 employees after the ACT restructuring. Here the average for the benchmark is 25.8.

#### 2.3.2.2. Assessment and recommendation

The Compliance Function also appears to be focused on best practices and properly organized. All compliance elements and subjects addressed in IDW PS 980 are logically assigned in the context of a mutually exclusive development and process organization in the Compliance function. The separation between the areas of Consulting/Prevention (basically anchored at the Business Levels area) and Detection/Investigation (as governance tasks at the ThyssenKrupp AG level) is clear and consistently implemented. The regional organization under development is required to embed local compliance structures from an organizational and content viewpoint. The basis for compliance consulting that is independent of everyday business interests is created correctly via the reporting lines, both at the level of the Compliance Officer for the Business Area and the Regional Compliance Officer (each in a direct reporting line to the Chief Compliance Officer).

Taking into account the risk profile for the ThyssenKrupp group and with consideration of the benchmark analysis provided by ThyssenKrupp, we consider the staffing of the Compliance function with over 60 FTE (including assistants) to be appropriate and suitable, specifically with regard to the target strength.

ThyssenKrupp has a central compliance organization which is supported by the Compliance Managers employed by the respective group companies. Unlike the Compliance Officers, the Compliance Managers do not deal with the subject on a full-time basis, instead it is an addition to their core activities. Against the background of the diversified and multi-layered group organization, this basic organizational decision appears appropriate. However, there is a basic risk that compliance specifications are defined and exist in the individual group companies very differently and with varying quality. Therefore the central Compliance Organization should ensure that a consistent quality standard is maintained in spite of the decentralized implementation of the specifications, for example, through on-site training or regional meetings.

We also recommend increased monitoring of the Compliance Officers who are responsible for the local implementation of compliance, if applicable, through increased reporting obligations on compliance activities by the Compliance Manager.

As shown above, not all Compliance Officer positions in the individual regions are filled (see illustration 1). These should be filled as soon as possible to ensure that each region has a regional contact person who is responsible for compliance and who understands the local culture.

In addition, we recommend that the planned integration of the North America region (USA and Canada) in the Compliance Program valid across the ThyssenKrupp Group is implemented as soon as possible.

### **2.3.3. E-Learning**

#### **2.3.3.1. E-Learning Program**

##### **2.3.3.1.1. Actual situation at the time of audit**

At ThyssenKrupp there is a group-wide Compliance E-Learning Program that covers the areas of anti-corruption and anti-trust legislation and which is currently available in nine languages. To supplement the E-Learning, there is also on-site training for both areas. There is also an E-Learning offering with the title "Role and functions of Compliance Managers" which is targeted exclusively at the Compliance Managers for the group and which explains their tasks and responsibilities. See item 2.3.3.4 for details on this E-Learning offering.

Since October 1, 2013, the new area of Awareness & Prevention in CO/CPL (CO/CPL-AP) is responsible for the review and further development of E-Learning offerings in the areas of anti-corruption and anti-trust legislation. Since October 1, 2013, the monitoring of the E-Learning offerings (evaluation, organization etc.), is incumbent on the area Projects, Reporting & Processes in CO/CPL (CO/CPL-PRP).

Since 2006, two training rounds have been carried out (2006/2007 and 2007/2008). The current third round of training has been running since August 2012. In the years 2009 to 2011 there was no update to the training content, therefore there was no new round of training.

For each of the two E-Learning areas, the local Training Manager specified and commissioned by the Compliance Manager, who is usually employed at the same group company as the Compliance Manager, compiles a list of the employees who should participate in the respective E-Learning offering using the group-wide mandatory participant catalog (mandatory participants). The mandatory participants for both E-Learning offerings include, in particular, the Boards, CEOs, management employees as well as employees from Sales and Purchasing. The mandatory participant group for the E-Learning on anti-corruption also includes employees from the areas of Corporate Communication, Controlling, Accounting, Goods Received and Goods Control, as well as persons responsible in the areas of Security/Factory Security. The responsible Compliance Manager can register additional employees as participants in the E-Learning at their own discretion if they also come into contact with the content covered in the E-Learning offering.

The Training Managers enter the mandatory participants in an E-Learning Administration Tool (EAT) which transfers the registrations to the group-wide E-Learning Platform LiNet. Across the group, all mandatory participants are centrally informed about participation in the Compliance E-Learning offering via e-mail. The e-mail contains a message from the Board of ThyssenKrupp AG in German and English highlighting the importance of the training program and requesting that the employees attend the training.

The mandatory participants must only attend the planned training if there is an update to the training materials, not in a regular frequency. Employees who become mandatory participants during the current training round due to a new hire or change in function must be registered by the Compliance Manager. With regard to the number of registered mandatory participants, we were told that CO/CPL PRP carries out a plausibility test per group unit on the basis of the size of the society in question at least once a year. The training is based on products from the company Digital Spirit. The content has been modified to suit the requirements of ThyssenKrupp.

At the end of the E-Learning, the participants must pass a test as part of the repeatable participant controls. The system automatically documents whether E-Learnings are being offered and whether the participant controls have been passed. There is only a distinction between "passed" and "not participated", whereby the latter also includes employees who have taken the test but have not yet passed it. For reasons of co-determination, only the responsible Compliance Manager and the Training Manager are informed of the names on the non-participants. The Compliance Manager will encourage the non-participants to attend the training. The Compliance Officer at the Business Area and group levels monitor the completion of the E-Learnings by the mandatory participants using anonymous statistical data from the E-Learning System and, if applicable, will ask the responsible Compliance Managers to introduce measures to increase the completion rate. No cross-group standardized specifications for monitoring participation in training, corresponding follow-ups for non-participants, and, if applicable, escalations exist at the individual company level. We were told that, in this respect, the Compliance Managers work individually. However, within the scope of

direct contact by the Compliance Officer, the Compliance Managers are informed in particular about company-specific Key Performance Indicators (participation rates for E-Learning, information on courses that are not passed over a long period of time, and the number of registered employees for the E-Learning) and are also informed about their responsibilities in the regular Compliance newsletter.

We were told that there is not yet a numerical benchmark for the employees to be trained that is used by CO/CPL.

As of September 30, 2013, 77,832 of the registered 80,023 mandatory participants have taken part in the anti-corruption and anti-trust E-Learnings. This corresponds to an achievement level of 98.6% (including subsequent registrations) with consideration of a waiting period of eight weeks.

With regard to the employees, additional differentiated, target-group-specific training is held as a non-site training offering. For the financial year 2013/2014, approximately 5,300 employees are included in the training plan to attend on-site training in the areas of anti-corruption and anti-trust legislation. We were told that the participation and non-participation of employees invited to the on-site training will be statistically recorded and evaluated retroactively to October 1, 2013.

#### **2.3.3.1.2. Assessment and recommendation**

The Compliance E-Learning program represents a central prevention measure for ThyssenKrupp, in particular due to the high coverage and the IT-supported participation control. As no differentiated training is offered for different company areas as part of the Compliance E-Learning offering, this represents the basic provision of information relating to compliance and should also be supplemented by risk-specific on-site training which, for example, takes into account the individual risk situation of a Business Area, respective region, or the function and position of the employee in the company.

To make employees more aware of the subjects of corruption prevention and anti-trust legislation, we recommend that the participant catalog is regularly updated and that the relevant employee groups are included in the mandatory participant catalog.

The Code of Conduct initially came into effect in October 2013 and therefore is not taken into account in the third round of E-Learning. For the coming training round, we recommend that the content of the Code of Conduct is included in the E-Learning.

We were told that the expected number of participants at the start of the third training round from across the group is approximately 35,000. This figure was mentioned during a plausibility test. However, a detailed breakdown of the participants according to area of employment or similar has not yet taken place.

To ensure that all relevant employees are registered for the E-Learning, we recommend that an internal benchmark analysis is carried out so that a total plausibility test can be carried out as part of the Target-Actual Comparison.

The planned clear detailed statistical recording of participants in on-site training that we were told is planned for the FY 2014/15 should be carried out for improved follow-up of the training activities. In particular it should also be recorded which employees have been invited but who did not participate in the corresponding training.

### **2.3.3.2. Anti-corruption E-Learning**

#### **2.3.3.2.1. Actual situation at the time of audit**

The anti-corruption E-Learning introduces the importance of corruption prevention, the corresponding commitment of the Board, backgrounds and legal bases, the forms in which corruption appears, correct behavior and possible consequences of corruption for the employees in question and the company.

The participants in E-Learning are requested to confer with the Compliance Officers on the subject of corruption prevention in the case of questions or uncertainties. The contact data is given in the E-Learning. The E-Learning also includes references to the internal regulations and tools used at ThyssenKrupp (e.g. leaflets as a supplement to the corruption prevention guidelines) that can be accessed directly as part of the E-Learning.

A text-to-speech function, numerous case examples, and interactive elements support the exchange of the content. The E-Learning offers the chance to focus on individual areas through its direct links to supplementary information. The questions in the examples and the participant control are clear and promote awareness of the subject area. The system offers detailed feedback on each individual question in the participant control.

#### **2.3.3.2.2. Assessment and recommendation**

The anti-corruption E-Learning is targeted in its form and content and, due to the numerous case studies and control questions, it is particularly suitable for making the participants more aware of the subject and to provide decision aids for everyday company business.

### **2.3.3.3. Anti-trust E-Learning**

#### **2.3.3.3.1. Actual situation at the time of audit**

The anti-trust E-Learning supplements the guidelines "Einhaltung kartellrechtlicher Gesetze" (Compliance with Anti-Trust Legislation) and also the "Kartellrecht" (Anti-Trust Legislation) and "Verbandstätigkeit und Verhalten bei Zusammentreffen mit Wettbewerbern auf Verbandstreffen" (Association Activities and Behavior when Meeting Competitors at Association Meetings).

The E-Learning is split into eight chapters that deal with general issues in anti-trust legislation, with the legal bases of anti-trust legislation, as well as case groups in anti-trust legislation (agreements between competitors, agreements between suppliers and customers and the abuse of a market-dominant position), communication, and possible sanctions in the case of breaches of anti-trust legislation.

The E-Learning ends with two case studies and also a participant test with ten questions. The questions are randomly selected by the system from the question pool. Questions that must be answered as part of the participant control refer to sanctions in case of breach of anti-trust law and behavior in the case of critical information that is possibly relevant to anti-trust-legislation.

When taking the E-Learning, reference is made at various points to the guidelines on anti-trust legislation valid at ThyssenKrupp and the corresponding information leaflets. The participant is informed several times that if in doubt they should contact a Compliance Office or the legal department of ThyssenKrupp to prevent anti-trust risks for themselves or the company.

The E-Learning offering includes a text-to-speech function. The participants are made aware of anti-trust legislation through numerous case studies and interactive elements.

#### **2.3.3.3.2. Assessment and recommendation**

The E-Learning is organized in accordance with objectives and it supplements the guidelines and information leaflets on anti-trust legislation with relevant information that is explained using examples and supported via the obligation to actively participate.

The employees are made aware of anti-trust issues through the documents available at ThyssenKrupp on the subject of anti-trust legislation and the E-Learning on anti-trust legislation.

#### 2.3.3.4. E-Learning on Role and Function of Compliance Managers

##### 2.3.3.4.1. Actual situation at the time of audit

The E-Learning "Role and Function of Compliance Managers" was introduced in September 2013 and is targeted at the 320 Compliance Managers (as at September 30, 2013) in the ThyssenKrupp Group around the world. It is available in both German and English.

This E-Learning offering aims to give an overview of the ThyssenKrupp Compliance Program to the Compliance Managers and to explain their function and specific tasks relating to the implementation of the Compliance Program in their respective areas of responsibility. In contrast to the E-Learning offerings on anti-corruption and anti-trust legislation, there is no test at the end of the E-Learning.

The E-Learning contains essential information on the ThyssenKrupp Compliance Program, the culture of compliance, the integration of compliance in business processes, providing information and consulting, identification, reporting and handling, a summary, and contact data. The Corporate Compliance Office is responsible for both appointing the Compliance Managers as well as inviting the Compliance Managers to participate in the E-Learning "Role and Function of Compliance Managers". Participation in the E-Learning is mandatory for the Compliance Managers. As for the other E-Learning offerings, participants are invited to participate via an automatically generated e-mail (in German and English). An attachment to this e-mail contains two pdf documents (in German and English) with access and operating information for the E-Learning. The e-mail does not include a fixed date before which the E-Learning must be completed by the participant. However, the e-mail gives a time window of around one month during which participation in the E-Learning by the respective Compliance Manager is expected.

The organization and execution of the E-Learning is controlled centrally by CO/CPL. In addition to the invitation to participate in the E-Learning, CO/CPL is also required to evaluate the participation results. In contrast to the E-Learning offerings on anti-trust legislation and anti-corruption, CO/CPL can carry this out on a personal basis.

At the end of the E-Learning, the Compliance Manager must confirm that he or she is aware of the content of the E-Learning, including the information leaflet from July 20, 2012 "Anforderungen an die Funktion des Compliance Managers" (Requirements of the Function of the Compliance Manager), which explains how the Compliance Managers are integrated within the Compliance Organization and the requirements of the Compliance Managers. The information leaflet groups together the essential content of the E-Learning.

In the case of non-participation in the E-Learning, we were told that CO/CPL will contact the respective Compliance Manager and ask them to complete the E-Learning as soon as possible.

To ensure that all Compliance Managers are known to CO/CPL and that all staffing changes that have taken place for this position (for example, transfer within the company or leaving the company) in the individual group companies are reported to CO/CPL, we were told that the data is maintained as follows:

We were told that the data for the Compliance Managers is stored and maintained centrally by CO/CPL-PRP in the ThyssenKrupp investment database. This should ensure that a history is automatically created for each assignment for each group company and that it is stored retroactively for each point in time for the Compliance Manager of a group company - as for the company database.

It is modified via a manual adjustment, e.g. on the basis of proactive notifications from the group company or as a result of continual communication with the Compliance Managers, e.g. as part of the Compliance Newsletter and the execution of specific tasks. The Business Area Compliance Officers also report any changes to their area of responsibility. The master data is also updated through (semi) automatic processes (for example, via the deactivation of the e-mail address when a Compliance Manager leaves the ThyssenKrupp Group or via change notifications from the Executive Management area) (cf. the document "Arbeitsablauf Pflege Compliance Manager"; July 2011" (Workflow for Maintenance of Compliance Manager)).

The information leaflet for the description of the tasks of the Compliance Manager also contains a note that changes to personnel or responsibilities in relation of the function of the Compliance Manager must be agreed with the Compliance Executive and the responsible Compliance Officer.

#### **2.3.3.4.2. Assessment and recommendation**

The E-Learning offering for the Compliance Manager is structured and explains the essential information about the Compliance program to the Compliance Managers appointed by ThyssenKrupp. The E-Learning is supplemented by the information leaflet "Anforderungen an die Funktion des Compliance Managers" (Requirements of the Function of Compliance Manager).

As the function of the Compliance Manager is a task with which the employees in question are entrusted via CO/CPL, and which should also ensure a trusting cooperation between the Compliance Manager, the Regional Compliance Officers and the Compliance Officers, no test has been added to the end of the E-Learning. This is understandable, however, there should be regular scrutiny to ensure that the Compliance Managers are dealing intensively with the subject of Compliance and that implementation is of a high quality and that there is communication in the group company.

There should also be a guarantee that the Compliance Managers receive compliance information at regular intervals and that they actually take note of the information and thus that they meet their obligation to impart the compliance information within the group company. This can occur, for example, via regular reports by the Compliance Manager or the Regional Compliance Manager to CO/CPL about the compliance measures carried out in the group company.

We were told that, as the file update process with the current Compliance Managers takes place manually, there is a risk that Compliance Managers who are leaving the company or new Compliance Managers are not entered into the database. Therefore we recommend that as the role of Compliance Manager has a high status, there should be a requirement for regular reporting (e.g. every 6 months) by the Compliance Manager on the current status of their function.

### **2.3.4. Business Partner Checks**

#### **2.3.4.1. Actual situation at the time of audit**

The aim of the Business Screening at ThyssenKrupp is to prevent breaches of the corruption ban and the Compliance Program for fighting corruption in connection with consultants/intermediaries and/or to avoid a corresponding index effect and thus reduce as much as possible the risk of corruptive actions or other financial crimes against group companies and their employees.

We were told that Business Partner Screenings are carried at ThyssenKrupp if a consultant or intermediary is employed to provide sales support for the project or for day-to-day business or at the instigation of a company in the ThyssenKrupp Group. At ThyssenKrupp, the terms Consultant and Intermediary are used to refer to intermediaries, consultants, sales representatives, agents, sponsors and all other persons working for the company.

Rules for carrying out Business Partner Screenings that are valid across the group are included in the group guidelines for the involvement of intermediaries, consultants, and other persons commissioned for sales support as passed by the Board on October 26, 2009. The application of the guidelines is dependent on the actual function of the consultant/intermediary as required by the contracting parties, not on the designation of the commissioned person or the legal arrangement of the contractual relationship.

In accordance with the aforementioned group guidelines, it is essential that the sales area wanting to commission the consultant/intermediary conducts a review of all consultants/intermediaries before any possible business relationship. As part of this mandatory preliminary check, information must be obtained on the identity of the consultant/intermediary and research must be carried out to ensure that no agreements are made with "letter-box companies". The guidelines do not include any specifications of how the check should be carried out. The concrete implementation of the

specifications given in the guidelines lies instead at the discretion of the Area Board for the relevant Business Area. If the Compliance Officer is linked to a Business Partner in the check and must make a statement, there is an internal note from January 6, 2012 under the header "Gliederung und Prüfungspunkte einer Compliance Stellungnahme - Stand Januar 2012" (Structure and Checkpoints in a Compliance Statement - January 2012). This note gives specifications on the framework for reporting and points to be considered when making a statement.

According to the guidelines, the Chief Compliance Officer for ThyssenKrupp should only be contacted in this matter if a group company wants to engage politicians, members of the assembly, members of state governments, officials, office holders, or holders of other official functions as consultants/intermediaries. In addition, the Compliance Officer can also be included in the check via the respective Sales Unit wishing to cooperate with a consultant/intermediary.

Attachment II to the group guidelines includes concrete specifications on the form of agreements with consultants/intermediaries as well as contract clauses that must be included in the respective contracts. It states that:

- Agreements are only permitted in writing;
- Agreements must be detailed;
- Verbal agreements are not permitted;
- Services provided must be documented.

It also specifies that the agreements with consultants/intermediaries must include clauses prohibiting assignment and corruption. The agreements can optionally also include an audit clause and a tax clause.

The audit clause specifies that if business, transactions, or projects are the subject of an official investigation/a judicial inquiry, the consultant/intermediary will immediately provide all information relevant for the process or investigation if requested by ThyssenKrupp and must specifically give access to all documents and records that could be significant for ThyssenKrupp with regard to the inquiry or investigation.

The tax clause specifies that, in the case of official investigations or a judicial inquiry and if requested by ThyssenKrupp, the consultant/intermediary will immediately provide written confirmation to show whether, to what extent, when, to which tax authorities and with which reference number the consultant has declared as income the commission/remuneration payments received from the project/transaction/business.

As a result of the specification in the group guidelines that the implementation of the specifications given in the group guidelines is the task of the Area Board for the respective Business Area, the Area Boards for the five Business Areas have issued specific regulations for the respective Business Areas.

These area-specific regulations are given individually for the respective Business Areas in the "Zustimmungspflichtige Geschäftsvorfälle (ZGV)" (Business Transactions Subject to Approval) catalogs. They are regulated according to the order volume, commission value or the country in which the consultant/intermediary is to be engaged and/or in which the delivery is to take place, approval processes, release processes, information obligations.

We are told that the specifications defined via the Business Areas in the ZGVs are agreed with CO/CPL.

If CO/CPL, the Business Area Compliance Officer and/or a Regional Compliance Officer are asked by a company unit to provide support in the screening of a consultant/intermediary, the Compliance Officer and/or the Regional Compliance Officer act in an advisory capacity, they do not make the decision. They can only make recommendations on the basis of documents received and requested. The actual decision on whether to enter a business relationship is made by the person responsible for the business relationship - in accordance with the regulations in the group guidelines and the ZGVs.

In addition to the group guidelines, there is also a presentation entitled "Compliance Programm - Einschaltung von Vermittlern und Beratern" (Compliance Program - Intervention of Intermediaries and Consultants). We were told that this presentation is part of the on-site training program and is specifically used if training courses are held at company units that often work with consultants/intermediaries.

With regard to content, the presentation includes parts of the group guidelines and also covers the intervention of consultants, offshore companies as consultants, the closing of agent contracts, as well as business subject to approval.

ThyssenKrupp has started a project with the objective of implementing a web-based tool for the review and monitoring of Business Partners. A presentation entitled "Business Partner Compliance Tool" shows how the Business Partner Screen Tool to be implemented should be structured according to the current planning status.

The aim of the tool is to:

- Minimize risks in connection with the engagement of sales and marketing intermediaries;
- Document the checking and approval processes in an audit-proof manner;
- Standardize and harmonize processes for the engagement of sales and marketing intermediaries;
- Significantly increase transparency relating to the use of sales and marketing intermediaries.

According to the current planning status, the Business Partner Screenings should be carried out in two stages: In the first stage, approx. 10 to 15 predefined standard questions on the consultant/intermediary are answered by the company unit who wishes to enter into a business

relationship with the consultant/intermediary. Based on the results of these questions, a risk is calculated automatically and the potential consultant/intermediary is classified in a risk group (low, medium, high risk).

Depending on this risk classification, further research is carried out in the second stage and employees from different company areas/competences are involved in the decision on whether to cooperate with the consultation/intermediary.

While the local management can make the decision on cooperation with the consultant/intermediary if the risk identified in stage 1 is low, if a medium or high risk is identified, the Compliance Manager and the manager of a company unit and/or a Compliance Officer/Chief Compliance Officer and the management of a Business Area are included in the process and in making the decision.

We were told that the tender for the design and programming of the tool will take place this year so that, according to the current status, the tool can be implemented in the middle of 2014.

#### **2.3.4.2. Assessment and recommendation**

As a result of the current regulations at ThyssenKrupp relating to the screening of consultants and intermediaries, CO/CPL is only obliged to be involved in the check if the consultant/intermediary is either an official or if the regulations in the ZGVs apply. In all other cases, CO/CPL receives no information on the screenings carried out. As a result of the mainly decentralized implementation of the Business Partner Screenings, there is a lack of centralized transparency relating to the consultants/intermediaries employed at ThyssenKrupp. In particular, there is a risk that business partners to be screened are not actually screened.

We recommend that CO/CPL receives a report to show whether Business Partners subject to screening in accordance with internal regulations are actually screened. This report could be created, for example, when the responsible areas create a notification after a screening has been carried out.

A corresponding solution has been devised in connection with the implementation of the Business Partner Screening Tool. We recommend that the initiated process for implementation of a web-based Business Partner Screening Tool is continued and implemented as soon as possible.

Like the new Business Partner Screening Tool to be implemented, the Business Partner Screenings currently focus on consultants/intermediaries in accordance with the definition specified in the guidelines. Other business partners are currently not taken into account in a screening. Therefore, we recommend checking whether the Business Partner Screenings in the future should be enhanced to include further potential business partners.

## 2.3.5. Compliance-Relevant Guidelines

### 2.3.5.1. Cross-guideline observations

#### 2.3.5.1.1. Actual situation at the time of audit

Since October 1, 2013, CO/CPL-AP have been responsible for the creation and revision of the content of internal guidelines in the area of Compliance. Guidelines are passed by the Board and apply across the group. At ThyssenKrupp, additional rules and reference documents exist in addition to the guidelines, for example, information leaflets and Frequently Asked Questions (FAQs). These are subordinate to the guidelines and as a rule, are used for clarification purposes.

As a result of the compliance organization, it is the task of the 320 Compliance Managers (as at September 2013) to inform the employees in the respective group companies of the guidelines, information letters, and information leaflets. This applies, in particular, to new employees. Guidelines are made available in the ThyssenKrupp intranet and communicated to the Compliance Managers with the request to publicize them in the respective company unit/region. Due to the compliance organization at ThyssenKrupp, only a restricted review of the communication of the guidelines is possible. However, the on-site training and E-Learning offerings on anti-corruption and on anti-trust legislation include extensive information on the corresponding guidelines and information leaflets (on E-Learning, see also topic 1 under item 2.3.3.1).

There are not yet any basic group specifications for the creation of internal guidelines. We were told that a project group is currently working on devising standards for the creation of guidelines during the current year.

At ThyssenKrupp AG, the compliance-relevant guidelines for the areas of anti-corruption and anti-trust legislation are included as an attachment to the employment contract. By signing the employment contract, each new employee confirms receipt of the guidelines. There is no corresponding group-wide regulation. The respective Compliance Manager is currently responsible for forwarding information.

#### 2.3.5.1.2. Assessment and recommendation

The introduction of group-wide consistent standards for guidelines is already planned. We recommend that the following content is included in these standards:

- Definition of responsibilities for creation and revision of guidelines;
- Inclusion of findings from Compliance Audits, from breaches of rules that have occurred, from the consulting hotline, and from the results of compliance risk analyses;
- Definition of an update process, for example, with each significant change and at least once a year.

To guarantee that the names of all currently employed Compliance Managers that are reported to the Compliance Officer are up-to-date (and thus that compliance-relevant information is publicized to the employees), we recommend the definition of a process to ensure that the list of Compliance Managers is regularly updated (see also E-Learning "Role and Functions of Compliance Managers" item 2.3.3.4).

We recommend the definition of group-wide standards for the effective monitoring of the distribution of guidelines by the local Compliance Managers. As a check, a confirmation could be received from each Compliance Manager stating that the guidelines have been published in the local unit. To concentrate the information flow, corresponding notifications could be sent by the Compliance Manager to the Regional Compliance Officer or the Compliance Officer responsible for the Business Area and reported by them to the CO/CPL.

We also recommend that the Code of Conduct and the guidelines on corruption prevention and anti-trust legislation together with the accompanying documentation (information leaflets etc.) become a binding part of the employment contracts across the group, or that comparable measures are taken to ensure that new employees confirm that they have taken note of the information and that they also agree with the content.

## **2.3.5.2. Anti-Corruption Guidelines**

### **2.3.5.2.1. Actual situation at the time of audit**

On July 20, 2012 the current valid group guidelines on the prevention of corruption were passed by the Board of the ThyssenKrupp AG. These group guidelines are clarified and supplemented by the following accompanying rules:

- FAQ „Einladungen und Geschenke: Fragen und Antworten" (FAQ "Invitations and Gifts: Questions and Answers");
- Information leaflet "Zum Umgang mit Einladungen, Geschenken und Rabatten zur privaten Nutzung" (Handling of Invitations, Gifts and Discounts for Personal Use);
- Information leaflet "Korruptionsstrafrecht und steuerliche Behandlung von Zuwendungen an Dritte im geschäftlichen Verkehr" (Criminal Law on Corruption and Fiscal Handling of Contributions to Third Parties in Business Transactions);
- "Konzernrichtlinie über Gesellschaftliches Engagement, Mitgliedschaften und Ticketerwerb" (Group Guidelines on Social Engagement, Memberships and Purchase of Tickets) (since October 1, 2013 the responsibility of Corporate Function Communication and CO/CPL).

The guidelines formulate the basic requirements made of the employees in connection with the fight against corruption as follows:

"The ThyssenKrupp Group expects its employees at all levels of the company and irrespective of their hierarchical position to observe the valid anti-corruption legislation and this guideline on corruption prevention."

This means that the respective statutory standards apply in each country, irrespective of whether these are stricter or more permissive than in Germany. Secondly, the standard of the guideline itself is a minimum requirement.

Specific rules apply for donations to holders of offices, for facilitation payments as well as for invitations and gifts. The latter can be omitted if only the impression of extraneous considerations may arise, even if the donation would be permitted by law. Some Business Area guidelines include supplementary rules, for example, the guidelines for delegation trips which only applies to the Business Area Elevator.

The subjects of the purchase of tickets, hiring VIP lounges, business seats etc. are regulated in the "Konzernrichtlinie über Gesellschaftliches Engagement, Mitgliedschaften und Ticketerwerb" (Group Guidelines on Social Engagement, Memberships and Purchase of Tickets). There is a detailed supplementary German-language form available for the release and documentation when purchasing tickets for sport or cultural events. In addition, a group-wide standardized IT-supported process (Global Engagement Tool (GET)) for the internal approval and documentation of donations/sponsoring, memberships as well as the acceptance of tickets is planned for the financial year 2013/14.

The guidelines on corruption prevention require that the employees involve a Compliance Office if there is even the "slightest doubt" of the legitimacy of an operation. In specific cases, it is essential that approval is received from a superior and/or a consultation is held with the Compliance Officer before accepting or granting donations.

The content of the anti-corruption group guidelines is imparted in the E-Learning module on anti-corruption. The subject of anti-corruption is also covered in on-site compliance training.

#### 2.3.5.2.2. Assessment and recommendation

The selected benchmark (respective local legislation) is, in principle, appropriate as the guidelines ensure, via the worldwide minimum standard, that legislative weaknesses in individual countries cannot be exploited. Particular difficulties are faced by non-local /traveling employees who must become familiar with the local legislation if it is stricter than the guidelines. These uncertainties are, however, covered by the obligation to consult the Compliance Officer if there is any doubt.

With regard to the area of gifts and invitations, the "Merkblatt zum Umgang mit Einladungen, Geschenken und Rabatten zur privaten Nutzung" (Information Leaflet on the Handling of Invitations, Gifts and Discounts for Personal Use) includes criteria, checklists, and practical case studies covering correct behavior to reduce the risk of suspicious or corruptive donations. However, the attachment to this information leaflet specifies that invitations and gifts below specific guide values are always considered as permitted by ThyssenKrupp. Irrespective of the value of the specified guide value, we consider this statement in this general form to be unclear at the very least, when the attachment to the information leaflet itself states that if in doubt, a Compliance Officer should be involved and also that, if there is cause for the acceptance, that in specific countries or in dealings with office holders or customers, narrower threshold values are relevant. The statement that donations to office holders with a value of less than EUR 35 are always permitted should not be made so generally for Germany and other legal systems if a footnote in the information sheet itself states that specifications from authorities are often more stringent.

We recommend that the attachment is modified so that it is even clearer that donations below the value threshold must also be assessed according to the criteria in the information sheet. If applicable, the value thresholds can be used to decide whether special documentation, approval from a superior, and/or intervention of a Compliance Officer is required.

Each employee is obliged to contact the responsible Compliance Officer if there is any doubt. In certain cases, there is also an obligation to have the donations approved by the superior. Item 3.1 of the "Konzernrichtlinie über Gesellschaftliches Engagement, Mitgliedschaften und Ticketerwerb" (Group Guidelines on Social Engagement, Memberships and Purchase of Tickets) specifies that particular information on the purchase of tickets must be documented and a form is available for this purpose. However, no general documentation of donations is required.

Without documentation requirements, compliance with the guidelines cannot be fully monitored. Furthermore, a documentation requirement would improve transparency and awareness. Therefore, we recommend that, at least for donations above a specific value and for donations in critical circumstances, there is a general requirement for documentation of the process as well as regulations regarding the responsibility for, distribution and storage of the document. With regard to donations, sponsoring, memberships, and event tickets, the documentation should be carried out within the GET in the future.

We recommend that the basic principles of the "Konzernrichtlinie über Gesellschaftliches Engagement, Mitgliedschaften und Ticketerwerb" (Group Guidelines on Social Engagement, Memberships and Purchase of Tickets) are also included in the group guidelines on corruption prevention. This highlights the significance of the regulations and enables the employees to find all essential information for the area of corruption prevention in the guidelines of the same name.

With reference to the purchase of tickets (VIP boxes etc.), item 6 of the group guidelines covering the prevention of corruption refers to Part IV of the "Konzernrichtlinie über Gesellschaftliches Engagement, Mitgliedschaften und Ticketerwerb" (Group Guidelines on Social Engagement, Memberships and Purchase of Tickets). The primary aim of the regulations in part IV of these guidelines is the avoidance of a personal gain by the invited employees, however, in item 3.1 they are supplemented by more extensive compliance notes and also a reference to the anti-corruption guidelines as well as the above information leaflet.

### **2.3.5.3. Guidelines on Anti-Trust Legislation**

#### **2.3.5.3.1. Actual situation at the time of audit**

The current valid group guidelines on anti-trust legislation ("Compliance with Anti-trust Legislation") were passed by the Board of ThyssenKrupp AG on July 20, 2012. The guidelines are aimed at all employees with the request that they actively participate in the implementation of the Compliance Program in their area of responsibility.

The guidelines include an introduction stating that anti-trust breaches endanger the success of the company and that they are not a means for ThyssenKrupp to obtain orders.

It is explicitly stated that breaches of anti-trust legislation will not be tolerated and that, irrespective of the position of the employee in question, it could lead to personal sanctions (zero tolerance).

Therefore it is expected that all employees at all levels of the company and irrespective of their hierarchical position in the company comply with the valid legislation governing competition and anti-trust legislation. As a result of this demand, it follows that the respective statutory standards apply in each country, irrespective of whether these are more stringent or more lenient than in Germany in individual cases. It also follows that the guideline itself is a minimum standard.

With regard to content, the guideline "Einhaltung kartellrechtlicher Gesetze" (Compliance with Anti-Trust Legislation) covers possible risks and breaches that could occur when dealing with competitors and/or with association activities and association meetings.

The information included in the guidelines, which could be relevant for or prohibited in anti-trust legislation, is divided into seven sections, however, it does not go into detail. As an example, see item 6 of the guidelines which only includes an abstract note "Anschein kartellrechtswidrigen Verhaltens" (Appearance of Behavior in Breach of Anti-Trust Legislation) or item 7 which contains a reference to the information leaflet without any reference to the problems of association activities ("in the case of association activities the specifications and recommendations of the information sheet must be observed").

Sections eight and nine contain references to clarifying and supplementary information leaflets which supplement the guidelines and also to contact partners for possible follow-up queries in connection with anti-trust legislation.

The guidelines are clarified with the information sheet "Anti-Trust Legislation", which was passed by the Board of ThyssenKrupp AG on July 20, 2012. The information sheet should serve as a "red flag" and inform the employees of the ThyssenKrupp Group about the most important bases for anti-trust legislation based on the group guidelines for compliance with anti-trust legislation. In addition to the description of prohibited behavior, the information leaflet also explains the possible sanctions for the company (fines) and/or for the acting person (criminal, civil, and concerning industrial law) and the leniency rule.

An additional information leaflet explains the special subject of "Verbandstätigkeit und Verhalten bei Zusammentreffen mit Wettbewerbern auf Verbandstreffen" (Association Activities and Behavior when Meeting Competitors at Association Meetings), which was also passed by the Board on July 20, 2012. This leaflet describes information obligations, non-critical and critical association activities and information exchange and also includes guidelines for correct behavior in relation to association meetings.

Both the guidelines and the information leaflets are not considered to be a conclusive representation of all possible breaches of anti-trust legislation, instead they are intended as orientation aids for the behavior of the employees. The contact partners for questions relating to anti-trust legislation are CO/CPL and also the legal department of ThyssenKrupp AG.

The guidelines are supported by the E-Learning on anti-trust legislation (c.f. item 2.3.3.3). At ThyssenKrupp, the anti-trust guidelines are also referenced in the ThyssenKrupp Compliance Commitment from April 16, 2007.

### 2.3.5.3.2. Assessment and recommendation

The guidelines on anti-trust legislation and the information leaflets form an essential element for making the employees aware of risks related to anti-trust legislation.

We recommend that parts of the guidelines on anti-trust legislation are clarified and some information contained in the information leaflets on anti-trust legislation is integrated in the guidelines. The guidelines give an overview of anti-trust legislation. However, there is a risk that for employees who do not regularly come into contact with the area of anti-trust legislation, the guidelines may not be clear. As, we were told, the guidelines should be the central document for the determination of requirements, definitions, and the conduct of the employees, it should contain more extensive information.

In the guidelines and in the information leaflet "Kartellrecht" (Anti-Trust Legislation), the legal department are also named as contact partners, in addition to the Compliance Officer, for queries or in case of doubt. However, neither the guidelines nor the information leaflet included a contact address for the legal department. We consider it to be understandable that the area of Compliance is responsible for anti-trust queries in agreement with the area of Legal.

In contrast to the information leaflet on "Kartellrecht" (Anti-Trust Legislation), the information leaflet "Verbandstätigkeit und Verhalten bei Zusammentreffen mit Wettbewerbern auf Verbandstreffen" (Association Activities and Behavior when Meeting Competitors at Association Meetings) does not include any information on possible sanctions in case of breaches of the corresponding regulations. Therefore we recommend that relevant information is included in the information leaflet or that there is, at least, a reference to the information leaflet "Kartellrecht" (Anti-Trust Legislation).

### 2.3.5.4. Code of Conduct

#### 2.3.5.4.1. Actual situation at the time of audit

Following the decision of the Board of ThyssenKrupp AG from September 24, 2013, an official Code of Conduct has been effective at ThyssenKrupp since October 1, 2013.

The Code of Conduct, which includes a foreword by the Board, applies to all employees, managers, and board members at ThyssenKrupp. With regard to content, the Code of Conduct covers the areas of compliance with laws, corruption, anti-trust legislation, conflicts of interests, fairness in competition, prevention of money laundering, equal treatment, human rights, employee rights, employee representatives, occupational safety, health protection, environmental protection, donations, lobbying, corporate communication, reporting, confidentiality, data protection, and protection of property. The code also refers to possible sanctions for individual employees and for the company in the case of breaches of regulations, and it emphasizes the Zero Tolerance strategy of ThyssenKrupp in the areas of corruption prevention and anti-trust legislation.

The Code of Conduct is accessible to everyone from the intranet or Internet and is available in German, English and five other languages. As the Code of Conduct was only passed after the start of the 3rd round of training on the subject of compliance, it has not yet been explicitly mentioned in the current E-Learning offerings. However, the content is partly included in the existing E-Learning offerings (anti-corruption and anti-trust).

#### **2.3.5.4.2. Assessment and recommendation**

We recommend that the Code of Conduct is fundamentally embedded in the relationship between the company and its employees, that the Code of Conduct is distributed with the employment contract throughout the group in the future, and that it is a binding part of the contract. As the managers are intended as disseminators of the Code of Conduct in the company, they should be specifically informed and instructed on the significance and content of the Code of Conduct.

When the content of the training materials is next revised, the Code of Conduct should be included as a central component of the compliance training and E-Learning offerings. In the long term, the Code of Conduct should be available as a central compliance document in further selected languages to make it accessible to as many employees in the group as possible.

#### **2.3.5.5. Supplier Code of Conduct**

##### **2.3.5.5.1. Actual situation at the time of audit**

In May 2013, a code of conduct for suppliers was first published at ThyssenKrupp (Supplier Code of Conduct). The Corporate Function Procurement & Supply Management (CO/PSM) and Corporate Function Technology, Innovation & Sustainability (CO/PSM) are responsible for creating and updating the code.

The Supplier Code of Conduct and the corresponding declarations of agreement for the suppliers are available in the intranet and Internet in German, French, Spanish, Portuguese, Chinese and English. The Supplier Code of Conduct and its content has up until now been taught to approximately 3,000 participants as part of a specific E-Learning offering for employees working in Purchasing.

The content of the Supplier Code of Conduct covers the following areas: Dealings with employees, child labor, discrimination, forced labor, freedom of association, remuneration and working times, health protection, occupational safety, environmental protection, corruption, invitations and gifts, conflicts of interests, anti-trust legislation, and also money laundering. In addition, reference is made to Global Compact, the labor standards of the International Labor Organization (ILO) as well as the United Nations Convention and the Organization for Economic Cooperation and Development for fighting corruption.

The Supplier Code of Conduct applies to all ThyssenKrupp suppliers. We were told that in the first stage, based on their group-wide purchasing volume, 5000 suppliers were required to submit a written declaration that they had received and will comply with the Supplier Code of Conduct. We were told that a roll-out in two further stages is planned for the next two financial years. Like the Code itself, a printed form for the declaration can be accessed in the Internet and is available in the specified languages. If a supplier has already accepted a code of conduct or produces their own code whereby the content is the same as the Supplier Code of Conduct, the declaration is not necessary. We were told that the first codes from suppliers are already available for checking their equivalence. With regard to the compliance elements in the Supplier Code of Conduct, CO/PSM is supported in this matter by CO/CPL.

The following measures are planned, if required, for monitoring compliance with the Supplier Code of Conduct:

- Supplier Self Assessments in the form of a comprehensive questionnaire to be completed by the supplier, which is requested a maximum of once per year.
- Sustainability audit at supplier's premises carried out by a third party commissioned by ThyssenKrupp and paid for by the supplier.
- Contractual right of ThyssenKrupp to obtain information if there is a suspicion of non-compliance with the Supplier Code of Conduct.

ThyssenKrupp retains the right to terminate the supplier contract if there are breaches of the Supplier Code of Conduct. As the Supplier Code of Conduct was only issued in May 2013, there are not yet any verifiable results.

#### **2.3.5.5.2. Assessment and recommendation**

Until now, the Supplier Code of Conduct has not included any further notes on the range of information and communications available for suppliers at ThyssenKrupp. With regard to the areas of anti-corruption and anti-trust legislation, we would expand the notes to include the whistleblower system, expand the general Code of Conduct and specify a contact partner at ThyssenKrupp in case of queries.

A process should be defined to check that the name of the new supplier and the name of the person who has signed the Supplier Code of Conduct for the respective period are the same.

These topics appear to be covered sufficiently. However, some areas are only covered in a very general manner. In particular, regarding the areas of invitations and gifts as well as anti-trust legislation, the Supplier Code could contain more specific benchmarks or at least refer to the general Code of Conduct or the ThyssenKrupp website.

### **2.3.6. Compliance Consulting Hotline**

#### **2.3.6.1. Actual situation at the time of audit**

A compliance consulting hotline is available for employees of the ThyssenKrupp Group. Employees can use a group-wide telephone number or send an e-mail to submit compliance queries directly to the Compliance Officer. The Consulting Hotline is staffed by Compliance Officers. The Compliance Hotline and contact information are mentioned in the intranet, in training courses and E-Learnings, in internal advertising posters, as well as in each Compliance Newsletter (Compliance Update).

The Compliance Officers acting in an consulting capacity document each query as part of their general consulting report. This documentation can be used to establish which queries or subjects crop up frequently and the areas from which many or fewer queries originate. In addition, subjects with an increased information requirement can be identified and corresponding communication measures implemented as was the case, we were told, for the FAQ "Invitations and Gifts", for example. In addition, company areas can be identified from which few or no queries originate. The corresponding evaluations are carried out and communicated during the quarterly report to the Board.

#### **2.3.6.2. Assessment and recommendation**

There is not yet any standardized method or specification for this documentation (reporting template or similar) and storage of the individual queries via the activity report of the Compliance Officer. However, a standardized storage system would facilitate the subsequent clarification of a query, irrespective of the responsible Compliance Officer. This can be particularly relevant if an employee has a query and makes a decision based on information from the Compliance Officer which raises questions at a later point.

## 2.3.7. Compliance Case Management and Compliance Reporting, Whistleblower System

### 2.3.7.1. Creation of Audit Reports and Case Management

#### 2.3.7.1.1. Actual situation at the time of audit

##### *Creation of the audit report*

At ThyssenKrupp, Compliance Audits are carried out both with and without a specific cause.

The cause-independent Compliance Audits are agreed during the annual planning of the Department Investigations of the Corporate Function Compliance (CO/CPL-INV) together with the Corporate Function Internal Auditing (CO/AUD). The Business Areas can present suggestions for this. The final decision on the cause-independent audits to be carried out lies with COP/CPL-INV.

Cause-independent Compliance Audits are carried out in the following process steps:

- Preparation of audit;
- Execution of forensic audit;
- Create report on the reports on the forensic audit;
- Evaluation of results of the forensic audit;
- Legal check and evaluation of results from the forensic audit;
- Determination of measures to be implemented by the audited area.

The audit preparation is carried out by both CO/CPL-INV and CO/AUD together. With the anti-corruption audits, the forensic part of the audit is subsequently carried out by CO/AUD. However, this does not represent a legal evaluation. Based on the report from CO/AUD, CO/CPL-INV makes an initial assessment whether and/or which findings of the audit should be investigated. It is also decided whether the legal evaluation of the findings should be carried out externally or internally. The results of the audit are subject to a legal evaluation after this evaluation. The coordination of the external lawyers or consultants is also the responsibility of the area CO/CPL-INV. The audit process in the area of anti-trust legislations differs because no forensic audit is carried out by CO/AUD. In reality, the facts are clarified directly by CO/CPL-INV, if applicable, in cooperation with an external law practice specializing in anti-trust legislation.

The determination of measures to be implemented by the audited group unit as a consequence of the results of the audit and the tracking of these measures is carried out by the area CO/CPL-INV.

The creation of the audit report was implemented in the 2nd quarter of 2012/2013. The aim of this implementation is to guarantee efficient report creation as part of the audit process as well the clear and condensed representation of the audit results. The audit results and the legal audit of these results are also categorized and recorded statistically.

The *cause-related* Compliance Audits are generally based on information received by ThyssenKrupp, for example, via the BKMS® system and/or the Ombudsman. Due to the internal organization, all information received by ThyssenKrupp from the Ombudsman or via BKMS® system is directed automatically to the manager of the area CO/CPL-INV and from there it is assigned for further processing.

According to the documents provided to us, the cause-dependent Compliance Audit is carried out in the following process steps:

- Check of information;
- If applicable, forensic data analysis;
- Comments on the forensic analysis;
- Evaluation of forensic analysis;
- Legal audit and evaluation of the results of the forensic analysis;
- Determination of measures to be implemented by the audited area.

The audit of the information and, if necessary, a possible data analysis are carried out in consultation with CO/CPL-INV and CO/AUD. The evaluation of the forensic investigation is the responsibility of the area CO/CPL-INV. We were told that a legal assessment of the evaluated information is carried out by external law practices, however, sometimes also by internal employees. The internal responsibility for cooperation with the external representatives lies with the area CO/CPL-INV. The determination of measures to be implemented by the audited group unit as a consequence of the results of the audit and the tracking of these measures is carried out by the area CO/CPL-INV.

A Competence, Responsibility and Reporting matrix (RACI) was also created for the reports following cause-related Compliance Audits. This gives information on the author, the recipient and the company areas to be informed in the case of corruption audits and whistleblowing cases.

In each Board meeting (usually every fourteen days), there is a written report on the compliance activities at ThyssenKrupp.

Every quarter, a compliance report is created for the Board and the Audit Committee and it gives information on the status of the Compliance Audit. When the individual audits are represented, there is a distinction between corruption and anti-trust audits and also between on-going, started, and completed audits. We were told that the basic audit results are formulated for the Board, while the remaining results are included and presented in a statistical evaluation.

We were told that there is no group-wide valid emergency plan for breaches of corruption and anti-trust legislation at ThyssenKrupp.

#### *Follow-up measures*

The implementation of the measures prescribed by CO/CPL-INV is a task of the group company in question. CO/CPL-INV is responsible for monitoring the implementation of the measures.

The follow-up process is as follows:

After a completed Compliance Audit, CO/CPL-INV presents to the respective group unit the basic results of the audit as well as the required measures. These are included in the "Catalog of Measures" (Excel table). The catalog of measures is used for documenting the implementation of individual measures. In addition to a description of the required measures and those to be implemented, the Catalog of Measures also includes the person with overall responsibility for implementation of the measures (usually the CEO of the respective group unit) as well as the deadline for implementation of the measure.

The implementation status of the measures is queried each quarter by CO/CPL. The measure tracking is controlled by CO/CPL. The respective investigator is responsible for the content-based control of the implementation.

The evidence provided by the respective group units relating to the implementation of the prescribed measures is checked by CO/CPL and the implementation of the measure is confirmed. The audit for the respective company unit is only formally completed when all measures have been implemented.

#### **2.3.7.1.2. Assessment and recommendation**

On the whole, the process of carrying out cause-independent and cause-related Compliance Audits is structured in a systematic and appropriate way.

Information on the status of the measure implementation is currently documented in an Excel sheet. However, employees responsible for the implementation of the measures in the respective group companies cannot edit some fields in the Excel table which is why it should not be possible to make any manipulative changes to the measures, deadlines, or other specifications.

Nevertheless we recommend that in the medium term a web-based, system-controlled solution is implemented for the follow-up measures to exclude the risk of the Excel table being changed or lost.

We also recommend the implementation of a group-wide valid emergency plan for breaches of corruption and anti-trust legislation, which should be made available to all group companies. An emergency plan is intended to be an instruction to the decision makers from the respective group companies to follow in case of emergencies and it takes the form of a checklist. We also recommend the implementation of a group-wide valid emergency plan for breaches of corruption and anti-trust legislation, which should be made available to all group companies. An emergency plan is intended to be an instruction to the decision makers from the respective group companies for situations in which, due to the urgency and unpredictability of a situation, rapid decisions must be made in order to prevent greater damage.

The emergency plan should be created in the form of a checklist and the essential and/or necessary measures should be quickly communicated to the decision makers on site.

We know from experience that, in unpredictable situations that may be relevant from both legal and image points of view, essential and necessary measures are often not carried out, therefore the emergency plan should take into account essential measures in the affected group company in addition to the regulations in the press guidelines (e.g. inclusion of company credit card, blocking of access authorizations etc.).

To avoid the group companies wanting to clarify a breach of corruption or anti-trust legislation with consideration of the emergency plan but without the participation of CO/CLP, we recommend that a consultation requirement is specified in the emergency plan. In addition, the emergency plan should only be available to the Compliance Manager and a limited number of other persons responsible at the group company.

### **2.3.7.2. Whistleblower system**

#### **2.3.7.2.1. Actual situation at the time of audit**

ThyssenKrupp has implemented a whistleblower system which enables information gathering in the case of compliance breaches. The notification of possible breaches to legislation or guidelines can take place via one of the four channels:

- Personal points of contact at the company, e.g. superiors, Compliance Manager, or the Compliance or Legal Department;
- Internet-based system (BKMS® system): Available worldwide in 34 languages;

- Telephone hotline (toll-free numbers in 60 countries, available in 34 languages);
- External Ombudsman.

Irrespective of the option to provide information via official channels at ThyssenKrupp, the employees are primarily encouraged to turn to the personal points of contact at the respective company unit if possible, specifically to their own superior and the on-site Compliance Manager responsible.

For the implementation of the Internet and hotline-based whistleblower channels, ThyssenKrupp uses the web portal software Business Keeper Monitoring System (BKMS®) from the company Business Keeper. The whistleblower can enter information themselves via BKMS® using an input template. He or she can also communicate the information by telephone using the automated hotline system. In this case, the message is recorded, then transferred to text by external persons and is only then made available to the responsible office at ThyssenKrupp. The BKMS® uses technical measures to ensure that the whistleblower can also give information anonymously. In this case, the whistleblower can set up a protected mailbox which enables direct communication between the Compliance Officer and the whistleblower in spite of anonymity.

Whistleblowers also have the opportunity to contact the Ombudsman. We were told that there is explicit authorization to keep the identity of whistleblowers secret.

The area of Investigations (CO/CPL-INV) is informed automatically about information received via BKMS®. It is then assigned to the investigator responsible for the Business Area for determination of the facts. Information submitted from other sources (e.g. via the Ombudsman) is, we were told, subsequently maintained in the BKMS® by the Compliance Officer responsible for clarification of the facts. The BKMS® is also used for the subsequent tracking of the information. The decision on deleting information or marking a process as completed can only be made using the Double-Verification Principle and this is inherent in the system.

Employees are made aware of and informed of the whistleblower system using the intranet, the ThyssenKrupp website and in Compliance Update no. 13, incl. an attachment from August 6, 2013. ThyssenKrupp explicitly ensures the whistleblowers that their information will be handled in confidence and that no penalties can result from providing information. External persons can get information on using the whistleblower system from the website for ThyssenKrupp and use this for submitting the information.

#### **2.3.7.2.2. Assessment and recommendation**

The group-wide organization of the whistleblower system with the option to submit confidential and/or anonymous information on breaches of regulations increases the communication of compliance-relevant facts and thus the effectiveness of the CMS.

As the whistleblower system is also aimed at external persons, it should also be mentioned in the Supplier Code of Conduct.

## **II. Further development of Compliance Management System (Audit subject 2)**

### **1. Audit assignment**

An audit of the Compliance Management System (CMS) to prevent breaches of anti-trust and corruption legislation as per IDW PS 980 took place on September 30, 2011. As a result, the investigation relating to audit subject 2 should exclusively refer to the extent to which the recommendations made in the audit report relating to the CMS audit from September 30, 2011 have already been implemented.

### **2. Execution of audit**

Starting from the audit of the CMS description by KPMG in 2011 (see under Actual situation at time of audit), the implementation of the recommendations and observations made by KPMG as the result of their audit in the period from July 31, 2013 to October 18, 2013 was investigated. In this regard, the Chief Compliance Officer first reported on the implementation status of the individual recommendations and observations and we were provided with numerous and extensive documents (mainly PowerPoint presentations on the measures taken as well as internal guidelines) in a data room. Building on this, the Corporate Function Compliance (CO/CPL) was sent a questionnaire on August 30, 2013 and asked to provide additional information on the individual measures taken and/or an explanation. The questions were answered in writing on October 1, 2013 (part 1) and on October 14, 2013 (part 2); in the meantime, personal meetings were held with employees of CO/CPL. The documents provided were explained by employees of CO/CPL at our request. There was also an overview of the E-Learning offerings in the area of anti-trust and anti-corruption legislation.

### **3. Actual situation at the time of audit**

KPMG audited the CMS description created on November 14, 2011 during the period from April 1, 2011 to September 30, 2011 (the CMS description is enclosed with the KPMG audit report as attachment 1). The CMS description has not been changed since then; changes and enhancements to the Compliance Program were made and documented in separate documents (usually PowerPoint presentations). It is planned to merge them into one document. The existing, publicly accessible KPMG short report and also the long version, which is not publicly accessible but which was made available to us, are split into six areas in accordance with IDW PS 980:

- Compliance culture and compliance objectives (separate areas in IDW PS 980, therefore seven areas there)
- Compliance risks
- Compliance program
- Compliance organization
- Compliance communication
- Compliance monitoring and improvement

The KPMG reports contain recommendations as well as two observations, arranged according to areas. In this regard, and with regard to content, the short and long version are the same. In the reports, the points highlighted as observations are (1) the potential for improvement when guaranteeing prompt registration for the corresponding E-Learning Compliance training for new employees or employees who have transferred from other positions in the ThyssenKrupp Group and who deal with compliance-relevant tasks and (2) the required modification of sales agent contracts to meet the current compliance requirements and the associated communication of the compliance requirements to the group company.

ThyssenKrupp has implemented a number of measures with regard to the KPMG observations and for implementation of the KPMG recommendations, whereby the respective implementation status is shown briefly below. Some measures have already been completed. With regard to the measures that have not yet been implemented, it must be considered that, in the past, some changes were made at the Board-level regarding the assignment of responsibility for compliance.

With regard to the two observations by KPMG, the following can be recorded:

- ThyssenKrupp has undertaken an intensive review of the E-Learning and assessment for anti-trust legislation and anti-corruption. Different measures have been taken to ensure the prompt registration in the E-Learning Compliance trainings of new employees or employees who have transferred from other positions in the ThyssenKrupp Group and who deal with compliance-relevant tasks. This includes central coordination whereby the Compliance Manager data is maintained centrally by CO/CPL. It is modified via a manual adjustment, e.g. on the basis of proactive notifications from the group company or as a result of continual communication with the Compliance Managers, (e.g. as part of the Compliance Newsletter and the execution of specific tasks). The Compliance Managers of the group companies are also contacted directly via e-mail and informed about essential indicators (e.g. fulfillment rates in the Compliance Manager's area of responsibility or the number of courses that have not been completed for a long time). In addition, the Business Area Compliance Officers report any changes to

their area of responsibility. This is enhanced by (semi-) automated processes which update the master data (for example, via the deactivation of the e-mail address when a Compliance Manager leaves the ThyssenKrupp Group or via a change notification from the area Executive Management).

- ThyssenKrupp has implemented measures to make the group companies aware of the modification of existing legacy contracts to the current compliance standards within consulting and training. Starting with a risk assessment and based on the specifications of the group guidelines for the intervention of intermediaries, consultants and other persons commissioned to provide sales support, the complete process for the inclusion of intermediaries is presented and discussed in on-site training - if relevant for the target group. The subject is also taken into account in the E-Learning offering for anti-corruption. In addition, following the audit by KPMG, letters were sent to numerous group companies who were, if applicable, informed about the need for modification of the sales agent contracts. In addition, with the cooperation of KPMG, meetings were held with the Compliance Executives of the Business Area, in which the results of the audit by KPMG were discussed and specific improvement requirements - e.g. relating to sales agent contracts - were discussed. The results of the KPMG audit were presented to the Compliance Managers in a Compliance Update. The improvement recommendation relating to dealing with legacy contracts was also explicitly presented. The subject of the modification of sales agent contracts to meet the current compliance specifications is also taken into account by CO/CPL as part of compliance consulting. It has not yet been possible to carry out a full survey of all contracts affected, however, the modification of all affected contracts above a materiality threshold is planned. In this context, the comprehensive recording of sales agent contracts will be carried out during the introduction of the Business Partner Compliance Tool.

The following points can be made with regard to the recommendations of KPMG:

- Areas of "Compliance Culture" and "Compliance Objectives"
  - The compliance and integrity aspects were included in the group mission statement. This is accessible from the ThyssenKrupp website.
  - A Code of Conduct was developed and is accessible from the ThyssenKrupp website.

- Compliance risks
  - The revision of the process for surveying compliance risks has begun.  
In accordance with the KPMG recommendation, a bottom-up risk survey is now also planned as per the documents provided to us.
- Compliance program
  - The E-Learning for Compliance has been revised and there is now a third version available.  
There is also a course for anti-trust legislation and anti-corruption (cf. the remarks to audit subject 1).
  - The recommendation to define and communicate cross-group and binding requirements to guarantee the most wide-ranging compliance conformity of suppliers was met via the roll-out of the Supplier Code of Conduct in May 2013. The Supplier Code of Conduct is available on the website in six languages. The audit of the effectiveness of the compliance conformity of suppliers has begun and the first "Sustainability Audits" should be carried out before the end of 2013.
  - An E-Learning offering for purchasers and purchasing project managers has been developed for the Supplier Code of Conduct and excerpts shown to us.
  - A Business Partner Compliance Tool should be introduced in the financial year 2013/14; We were informed about the concept and current planning status.
  - The planning letters sent to the Business Areas now clarify that compliance requirements must be included in the planning process.
  - With regard to the integrity checks in the staffing process, we were provided with a protocol from the Human Resources Compliance working group. According to this, the inclusion of a structured integrity check within the staffing processes is planned. We were told that the criterion of integrity is already embedded in Personal Development (PerspActive). The group-wide inclusion of the Compliance Guidelines as an attachment to the employment contract is planned.
- Compliance organization
  - There is stronger central coordination of administrative activities, and the essential compliance-related processes in risk-oriented process descriptions are currently documented and a compliance functional guideline produced. In this context, the review of the roles and responsibilities of persons dealing with compliance-related tasks has been completed and documented in a PowerPoint presentation.

- Compliance communication
  - A stronger network of Compliance Managers is encouraged, and communication through compliance updates in the form of newsletters is supported. A Compliance Community and Regional Compliance Communities should be set up as well as meetings arranged on a regional, global or Business Area level. Furthermore, regional training measures and the use of online tools are already implemented to encourage interaction between CO/CPL and the Compliance Managers in the group units.
- Compliance monitoring and improvement
  - The increase in staffing has begun. On October 1, 2013, for example, the names of the persons responsible for the new departments Awareness & Prevention (CO/CPL-AP), Projects, Reporting & Processes (CO/CPL-PRP) and Investigations (CO/CPL-INV) and "Regions" will be announced. The still vacant positions in the new organizational structure are currently being filled; until then, substitution rules apply. If required, external support is used, in particular with regard to questions on anti-trust legislation.
  - For implementation of the measures suggested in the Compliance Audit, the respective CEO of the unit in question has overall responsibility and will report on and provide evidence of the implementation status on a quarterly basis. CO/CPL-PRP checks the evidence provided in close cooperation with CO/CPL-INV and confirms the implementation of the measures, which are recorded in a catalog of measures, also for the purpose of statistical surveys.
  - An employee survey relating to the perception of the compliance culture is planned as part of a survey on the group mission statement.

#### 4. Assessment and recommendation

The recommendations that could be rapidly implemented have been implemented since the conclusion of the KPMG audit as per IDW PS 980 o November 14, 2011. ThyssenKrupp has started to implement the more in-depth recommendations; at the time of our audit, these measures had not yet been conclusively implemented. Some of the implemented measures that are still to be completed are already in the roll-out phase, in any case, detailed designs are available. CO/CPL detailed these measures individually and implementation within the individual time plans (mainly in the financial year 2013/2014) seems realistic to us. The actions already implemented and those that have begun appear to be suitable for meeting the recommendations of KPMG and to be a suitable reaction to the two observations made by KPMG.

The changes in the area of compliance are regarded as a dynamic process and are also influenced by changes in the organizational structure. Thus the organizational and personnel assignment of the (Board) responsibility for Compliance has been subject to change since 2010. This may be the reason why several started measures could not yet be fully completed. Coordination with the group units in question is also time-intensive in a group with the size and organization of ThyssenKrupp.

The current dynamics in the area of compliance become clear, for example, via the change in the structure and process organization made within the ACT group program, via the transfer of compliance consulting to the Business Areas, in the further development of the reporting system, the introduction of an E-Learning offering for Compliance Managers, the execution of webinars on the subject of corporate responsibility for compliance, and via the introduction of a Supplier Code of Conduct.

In the sense of a recommendation that goes beyond that in the original audit subject 2, it should be noted that there are a variety of compliance guidelines, information brochures, and information leaflets. The reason for this is the understanding of the compliance organization that some guidelines and information leaflets are reserved for specific addressee groups, for example, on the subjects of association work and press trips. However, we consider it feasible that such a variety of documents could give the impression of a more reactive compliance culture. It could give the impression that measures to prevent compliance breaches in the past were too meticulous and thus that there is no capacity for proactive measures (example, group guidelines on press trips, pass by the Board of ThyssenKrupp AG on February 5, 2013). However, overall the current measures taken are suitable, also in the context of creating the sense of a proactive compliance culture.

We suggest that the existing compliance documentation is reviewed once more to check whether there are overlaps in the information and whether it may make sense to aggregate the information. We were informed that such an aggregation has already been considered and that the structure of the guidelines has been discussed across the group - not just in the area of compliance. This should be viewed as a positive step and should be implemented.

In the sense of a recommendation that goes beyond that in the original audit subject 2, it should also be noted that the restriction of CO/CPL to the prevention of anti-trust and corruption breaches may cause delimitation and assignment queries and/or risks as the distinction from other compliance questions must not always be explicit. For example, new developments in legislation may primarily relate to other compliance questions, but there may also be a certain relevance for questions relating to anti-trust and corruption breaches (like, for example, the new *Außenwirtschaftsgesetz* (German Foreign Trade and Payments Act) or the *Ordnungswidrigkeitengesetz* (Administrative Offenses Act)). In response to queries, we were told that the responsibility for the new German Foreign Trade and Payments Act lies in the area of responsibility of the Corporate Function (Taxes & Customs).

Internal charts should only use the traffic-light colors green, amber, and red if they are used in the context of a warning function or provide information on an implementation status. This can increase the employees' awareness of risks. They are currently still used inconsistently.

An employee survey relating to the perception of the compliance culture should not be carried out as part of a survey on the group mission statement, specifically not against the background of the significance of anti-trust and corruption breaches for ThyssenKrupp. Regular surveys on the perception of the compliance culture must be carried out so that target/actual comparisons can be carried out. A detailed survey in the sense of the promotion of risk awareness is also necessary and should be separate from a more general survey of the mission statement. In addition to information gathering, the survey should also serve to further raise awareness of all compliance risks and compliance breaches.

As compliance in the sense of the prevention of anti-trust and corruption breaches has played a major role for the group in the past, and as compliance will also be significant in the future, it may be appropriate to introduce rules on reporting to a committee of the Supervisory Board, e.g. to the Audit Committee, via a feasible rendering of the German Corporate Governance Code (DCGK) subitem 5.3.2, and formally document them, for example, in the agenda of the Audit Committee, if applicable, based on the measures relating to the Internal Audit suggested under audit subject 3 below.

### **III. Investment controlling as part of future large investment projects (Audit subject 3)**

#### **1. Audit assignment**

Audit object 3 is the process of investment controlling of large investment projects in accordance with the current Investment Guidelines as well as the process-independent auditing activity carried out by the Internal Auditing department in projects of this type.

#### **2. Execution of audit**

The audit was carried out from August 29, 2013 to October 18, 2013, whereby some preliminary provisions were made earlier on July 31, 2013. The changes to the investment guidelines for ThyssenKrupp AG (current version from February 1, 2013), including the responsibilities and investment approval processes, were first explained to us using numerous documents (e.g. presentations) and also in several meetings with the managers of the Corporate Functions responsible and other employees of ThyssenKrupp. The same applies for the changes made within the group organization during the period of the voluntary special audit. The Corporate Function Controlling, Accounting & Risk (CO/CAR) and the Corporate Function Internal Auditing (CO/AUD) were provided with questionnaires on September 2, 2013, which were to be completed in writing (by CO/AUD on September 11, 2013 and by CO/CAR on September 12, 2013) and the answers given with additional evidence. Furthermore, random tests were carried out to check compliance with the investment approval process; we were provided with a list of all current investment projects with an application volume in excess of EUR 25 million and also given an overview of the databases and project documentation (investment applications and decisions). With regard to Internal Auditing, their audit planning and audit activities in particular were explained to us along with their reporting and the group guidelines on Internal Auditing, presentation documents, and the results of previous assessments of the activity and staffing of Internal Auditing by a third party were made available. We were also informed about the activity by Internal Auditing in a random sample carried out by us using the list of current investment projects with an application volume in excess of EUR 25 million. With regard to reporting by Internal Auditing to the Board and the Supervisory Board, additional random samples were also provided to us for inspection.

### 3. Actual situation at the time of audit

#### 3.1. Investment Guidelines

There are Investment Guidelines dated February 1, 2013. They contain gradings into four investment levels based on the application volume. Investment level IV contains investments with an application volume in excess of EUR 25 million. There is no further differentiation above this investment threshold which is why all investment projects with an application volume of more than EUR 25 million are viewed as large investment projects in the context of the audit assignment. The decision committee for large investment projects of this type is the full Board of ThyssenKrupp AG. The investment guidelines do not define any further levels that necessitate the involvement of other committees. However, in accordance with the articles of association for ThyssenKrupp, the approval of the Supervisory Board is required if the measure serves to open up a new field of business and is of particular importance to the group (business transaction subject to approval).

The investment guidelines also contain rules that should ensure that the rules in the investment guidelines cannot be evaded and, for example, investment applications are not attributed to a lower investment level. The following cases are also regulated "no settlement between investment and disinvestment", "no reclassification of special permits for a particular purpose", "involvement of CC CT in the case of business being moved between two Business Areas", "dealings when acquiring and disposing of companies", and "ban on division into several applications in the case of investments that belong together", furthermore the particular risks of additional investment payouts that have already been included in the application volumes must be taken into account.

#### 3.2. Target Investment Value

A target investment amount and/or planned total investment volume is defined each year at the group level for the coming year (budget year) which is subject to the approval of the Board. The target investment value is distributed over the Business Areas so that each Business Area has their own total investment volume ("target investment value").

#### 3.3. Investment Process

In accordance with the Investment Guidelines, investment applications for investments with an application volume in excess of EUR 25 million are presented to the Corporate Center Controlling & Risk (CC CT) by the Business Area making the application. [Note: According to the guidelines, the

individual approval obligation, i.e. presentation to CC CT, starts from just level II, i.e. from EUR 5 million. The EUR 25 million specified here, and also the following processes, exclusively describe investments in level IV, i.e. from EUR 25 million] Investment applications must include an assessment of sensitivity and scenarios. In CC CT, the investment application is checked from the perspective of the group with regard to the financial and strategic attractiveness, a statement is made and the application presented to the full Board of ThyssenKrupp AG for a decision. Questions on the technical assessment in the investment application basically remain the responsibility of the Business Area as the specialist knowledge is also available here. However, CC CT also involves further Corporate Centers and group functions to deal with non-business-related questions, e.g. ThyssenKrupp real Estate for real-estate-specific aspects or the Corporate Center Technology & Innovation for research-specific questions.

### 3.4. Investment Controlling of On-Going Projects

Investment projects are entered in an investment database (InCo) and are basically listed individually. The completeness of the investment database is ensured with control measures (e.g. comparison with the values entered in the consolidation software HFM).

Operational investment controlling, i.e. the control of the actual realization of the investment is basically carried out at the Business Area level. This also applies to the associated accounting questions. The review of the intrinsic value of the activated acquisition and production costs for ongoing large investment projects is carried out by the operating companies as part of the rule process for quarterly and standard financial statements in cooperation with the auditor. In accordance with the investment guidelines, each Business Area is basically obliged to comply with the (total) target values and planning premises defined by the parent company so that corresponding countermeasures are usually already available at the Business Area level to counteract target value deviations. However, overruns of both the application volumes for investment projects as well as, in particular, the (total) investment target value must still be reported to CC CT by Business Area. Overruns of individual investment projects are also recorded in the investment database and taken into account in Cash Management.

If overruns are reported by individual investment projects, CC CT decides whether these overruns need to be communicated to individual members of the Board or to the full Board. This decision criteria in this respect are, for example, the amount of the overrun, the reasons for the overrun, as well as the possibility for investment budget reductions to compensate for the overrun. In addition, the threat to the investment target value of the Business Area is also relevant. In cases in which there is a suspicion that the overrun is the result of a violation of regulations (e.g. intentionally incorrectly completed economic feasibility studies at the time of application), this is reported to Corporate Center Internal Auditing (CC IA).

The Supervisory Board at ThyssenKrupp AG is informed about any budget overruns if overruns of the investment budget for individual projects either individually or together would lead to an overrun of the investment target values for the Business Area in question as approved by the Supervisory Board for the respective financial year.

Recalculations are carried out for individual completed or ongoing investment projects. This is used, for example, to subject the original planning premises and their compliance by the Business Areas to a critical review and to also use the results found for the assessment of future investment projects (lessons learned). The results of the recalculations are presented to the Board of ThyssenKrupp AG.

The group risks calculated on the basis of group-wide consistent threshold values that have not yet been taken into account in the projection or planning are dealt with in the Risk Committee, which meets four times each year, and are then reported to the Board of ThyssenKrupp AG, who then reports in turn to the Audit Committee. If significant, the target/actual deviations also belong to the risks listed for large ongoing investment projects. Changes to the risks in the respective quarter are an essential element of the risk reporting and are transparent. For example, the risk report starts with an overview of the basic changes.

### **3.5. Activity of Internal Auditing**

The activity of Internal Auditing is differentiated into auditing activities according to time, i.e. during and after completion of an investment project. CC IA is informed by CC CT about investments with an application volume in excess of EUR 25 million and decides whether a process-related audit takes place. Irrespective of this, a retroactive audit of the investment can be carried out at any time. This process should ensure that there can always be a second audit and validation instance in addition to the standard process of investment application and approval. With regard to ongoing investment projects, CC IA is informed by CC CT about deviations from the planning premises such as, for example, budget overruns.

The audit planning of the Internal Audit is carried out according to risk. The audit planning approach, including the risk evaluation, and the audit plan for the next year are presented to the Audit Committee on an annual basis. Internal Auditing informs the Board of the results of their audits and the implementation of measures on a monthly basis. The Audit Committee is usually informed once a year; in addition, Internal Auditing reports on special topics if required, e.g. in the case of audit applications by the Audit Committee to Internal Auditing.

#### 4. Assessment and recommendation

The application and release process for large investment projects is essentially suitable. The Investment Guidelines apply a relatively low value threshold for (large) investment projects after which approval of the investment by the full Board is required. During our audit, there were no circumstances found that indicated non-compliance with the Investment Guidelines.

Sensitivity and scenario analyses are obligatory in the investment application, and an ex post audit of planning assumptions by means of an investment recalculation is also carried out if applicable. This is to be considered positive. During the execution of the investment, the regular revision of the effects of changes to the planning assumptions (e.g. market environment, market prices) on the efficiency of the investment project for the Business Area as a whole; any possible depreciation requirement should also be identified.

Regardless of the adequacy of the controlling processes, it may be appropriate to implement ongoing monitoring as a precautionary measure for large investments with an application volume of EUR 150 million - with the inclusion of technical questions - under the responsibility of CO/CAR (i.e. at the group level) as well as regular reporting in this regard to the Board and Supervisory Board, and to include this in the Investment Guidelines (cf. also the recommendation on audit subject 4). In this respect, a further investment level should be introduced in the Investment Guidelines. From this investment level, in individual cases, external assessments of the technical feasibility or other specific aspects should be included and, if required, updated in specific time intervals. We were informed that the existing investment guidelines were currently being expanded to include a separate regulation for large investment projects in which the above-mentioned recommendations were being included.

With regard to the auditing activity of Internal Auditing, which is on the whole correctly organized, it must first be noted that their communication with other group functions could be more comprehensively regulated in the group guidelines for Internal Auditing and/or in some points of the guidelines for the other group functions. Thus it has not yet been formally defined that budget overruns are reported to Internal Auditing, also that Internal Auditing has no direct access to the investment database. Direct access could be enabled so that, in the context of Continuous Auditing, regular investment projects could be observed with regard to an enhanced monitoring requirement. However, this assumes that - as was explained to us - such communication takes place at that time via the "direct line" to the required extent, however the formal inclusion of a corresponding authority for Internal Auditing - even given the general group-wide trend towards formulated guidelines - seems to be appropriate. As guidelines for Internal Auditing already exist together with investment guidelines, questions relating to the communication with investment controlling could

also be regulated in more detail in the guidelines. In this context, it can be generally noted that the guidelines that exist at the group level are currently authored in very different formats: The investment guidelines are very detailed and the guidelines for Internal Auditing are also very structured. The guidelines for Risk Management consist of a detailed PowerPoint presentation. In this context, the rules for the Risk Committee could also be regulated in the Rules of Procedure.

With regard to the communication of Internal Auditing with the Audit Committee, the guidelines for Internal Auditing could also provide direct communication also outside of specific exceptional cases. At the same time, the wording could also be modified to suit the practical issues of direct reporting by Internal Auditing to the Auditing Committee - currently at least once a year. The guidelines currently still include indirect reporting via the Chair of the Board.

In addition to this, it would be worth recommending additional steps which could promote the status of Internal Auditing within the framework of company-internal monitoring. Thus, a quarterly report by Internal Auditing to the Audit Committee should be checked. The regulation provided from January 1, 2014 with the change to § 25c par. 4a no. 3g and/or par. 4b no. 3g KWG as a result of the legislation for protecting from risks and for planning the reorganization and handling of credit institutes and financial groups could be used as a guide in this matter. In addition, there should be checks to ensure that the Audit Committee is more involved in the audit planning for Internal Auditing. Furthermore, further clarification of the cooperation between the Audit Committee and Internal Auditing should be checked.

In this context, the staffing levels of Internal Auditing should be looked at, which was already raised as an issue during an external assessment of Internal Auditing. The benchmarking analyses carried out in 2010 found the staffing levels were comparatively low. Since then the staffing levels have improved slightly, however, with regard to the current benchmarking analyses, it is recommended that the Board and Supervisory Board of ThyssenKrupp AG look again at the budget allocated to Internal Auditing. Currently there are only plans to increase human resources in the area of Compliance (i.e. for the prevention of breaches of anti-trust legislation and corruption); there, at least, the benchmark analyses provided to us gave positive results.

Between the group function Internal Auditing and Compliance, there is cooperation to the extent that Compliance - like other group functions - can make suggestions to Internal Auditing during audit planning. For the specific Compliance Audits, there is joint planning between CO/AUD and CO/CPL, whereby the final decision lies with CO/CPL. Furthermore, in the case of corruption, CO/CPL carries out a legal assessment based on the reports from Internal Auditing. According to information from the Director of CO/AUD, there is no cooperation that endangers the (process) autonomy of Internal Auditing. Thus, the activity of Compliance is basically also the subject of the audit carried out by Internal Auditing. When revising the group guidelines for Internal Auditing as recommended, a clearer distinction should be made between the areas of responsibility for the group functions Internal Auditing and Compliance (with consideration of the "3 Lines of Defense model") to clarify this matter.

## **IV. Follow-up reporting by the Board to the Supervisory Board (Audit subject 4)**

### **1. Audit assignment**

Audit object 4 refers to the provisions of the current rules of information for follow-up reporting by the Board to the Supervisory Board in accordance with section 90 (1) of the German Stock Corporation Act (AktG) with the aim of checking whether it can be guaranteed that the Supervisory Board will receive timely knowledge of budget overruns or other significant misdevelopments in future large investment projects.

### **2. Execution of audit**

We reviewed the publicly available documents (e.g. statutes, rules of procedure), starting with the voluntary special audit. We then were given an overview of several expert reports that deal with the monitoring obligations of the Supervisory Board and how they are carried out by its employees, and also investigated the implementation and/or implementation status of some recommendations included in the expert reports. The findings from the meetings held on audit subject 3 and also from the responses received to the questionnaire sent to Corporate Function Controlling, Auditing & Risk (CO/CAP) and Corporate Function Internal Auditing (CO/AUD) were used. Further meetings were held with employees from ThyssenKrupp and supplementary documents and statements were provided and clarified (e.g. excerpts from Supervisory Board minutes). In the "Monthly Executive Report (MER)" - a 110-page report with the essential indicators at the group and Business Area level, including planning figures, deviation analyses, and comments - was provided for the month of August as an overview.

### **3. Actual situation at the time of audit**

The provision of information by the Supervisory Board is covered in several regulations in the Articles of Association and in the Rules of Procedure for the Board as well as the Rules of Procedure for the Supervisory Board and the Audit Committee. For example, section 5 of the Rules of Procedure for the Board with regard to information provided to the Supervisory Board by the Board as well as section 4 of the Rules of Procedure for the Audit Committee with regard to the Audit Committee's right to information.

The "Monthly Executive Report (MER)" created for the Board was completely restructured in April 2012 and is provided to the members of the Supervisory Board each month. Delivery to the Chair of the Supervisory Board usually takes place on the 15th working day for the month under review via the Corporate Office. The MER contains essential indicators (particularly relating to finance) for the whole group and the Business Areas, including comparative figures for previous periods and forecasts as well as comments on the corresponding deviation, which is highlighted with a traffic light, so that a suitable Target/Actual analysis can be carried out on the basis of this information.

The Supervisory Board is included in the investment planning via the approval requirement for annual investment planning by the group as per the Articles of Association and the financing thereof, whereby the Supervisory Board makes the decisions relating to the approval of the total investment volume and/or the (group) target investment value and its allocation to the Business Areas, and whereby the Strategy, Finance and Investment Committee of the Supervisory Board first deal with planning, including scenario/sensitivity analyses. In addition, in accordance with section 7 of the Articles of the Association, there is an approval requirement if the measure serves to open up a new area of business and is of major significance to the group. The investment guidelines themselves do not provide for any integration of the Supervisory Board in the decision on individual measures and also do not define any size classes that are of major significance to the group.

The Supervisory Board is informed about any budget overruns if overruns of the investment budget for individual projects either individually or together would lead to an overrun of the investment target values for the Business Area in question as approved by the Supervisory Board for the respective financial year.

In the past, the practical - both active as well as passive - side to the provision of information for the Supervisory Board was clarified in the expert reports provided to us - in particular with regard to large investment projects - both with regard to their timeliness and the scope and quality of information. In the context of further increasing monitoring efficiency, the expert reports provided to us also suggested that the Supervisory Board should deal with scenario analyses for investment projects above a certain size and also analyze the basic planning premises so that the resilience of the forecasts can be better discussed. Further suggestions include the possibility for the Supervisory Board, in important cases, to allocate audit assignments directly to internal or external experts who are not linked to the Board (including the presentation of audit results by the person commissioned, not by the Board), the possibility for the Supervisory Board to occasionally meet without the attendance of the Board Members, as well as more technical questions, such as the possible waiver of the circulation procedure and the timely provision of meeting documents, whereby the problems were highlighted in PowerPoint presentations.

According to excerpts from minutes provided to us, the implementation of the above recommendations from the expert reports have been discussed by the Supervisory Board. So, in the context of the implementation of these recommendations, the scenario/sensitivity analyses, amongst other things, will be increasingly carried out (or have already been carried out as per the minutes of minutes for the Supervisory Board), the existing, but not yet common, possibility of commissioning external experts who are independent of the Board was emphasized, specifically however, the responsibility of the individual members of the Supervisory Board was also highlighted.

With regard to the recommended meetings of the Supervisory Board, sometimes without the attendance of the Board members, Art. 4, par. 7 of the Rules of Procedure for the Supervisory Board at ThyssenKrupp AG should be changed as they currently still require the attendance of a Board member as a rule. In addition, the Supervisory Board has also clarified the tasks and the distinction between the Audit Committee and the Strategy, Finance and Investment Committee. Other changes to the Rules of Procedure are also planned, however they have been deferred to take into account the findings of the voluntary special audit, if applicable.

As part of a self-evaluation via a "Questionnaire on the Efficiency of the Supervisory Board at ThyssenKrupp AG", the Supervisory Boards are given the chance to give feedback on the preparation of the meetings, the meetings themselves and follow-up to them, and to make further appraisals and suggestions.

There is cooperation between the Supervisory Board, or rather Audit Committee, and Internal Auditing to the extent that the Corporate Center Internal Auditing creates an audit plan each year which is submitted to the Board for approval and which is given to the Supervisory Board (Audit Committee) for their information. Each year, Internal Auditing summarizes the results of their activities in a report for the Board and the Audit Committee. Internal Auditing basically reports to the Supervisory Board (Audit Committee) via the Chair of the Board. The Board and Supervisory Board require that direct reporting to the Supervisory Board (Audit Committee) is carried out in exceptional cases.

The Supervisory Board has also dealt with the report on the external audit of Internal Auditing in a meeting.

#### **4. Assessment and recommendation**

The sense and purpose of the inclusion of a follow-up report in the context of a target/actual comparison in the Stock Corporation Act section 90 (1) ("whereby deviations of the actual development from objectives reported earlier have to be explained and the reasons specified") by means of the Transparency and Disclosure Act (TransPuG) are to place the Supervisory Board in the position of being able to assess the forecast quality of the Board. The legislator had already

introduced the Early Risk Management System with the Law on Control and Transparency in the Corporate Sector (KonTraG) 1998 in section 91 (2) of the Stock Corporation Act. The sense and purpose of the Early Risk Management System is to receive information early enough for the Board to be able to successfully take countermeasures in good time. In this context, the Board has an obligation to provide information and the Supervisory Board has an obligation to gather information. Cf. BT-Drs. 13/9712, page 15 (explanatory memorandum to KonTraG), BT-Drs. 14/8769, page 13-14 (explanatory memorandum to TransPuG) as well as the details in DCGK subitem 3.4 and subitem 4.1.4 and subitem 5.1.1. The "template" for the "Monthly Executive Report (MER) and a review of the MER for August 2013 clarify that the Supervisory Board can use this information to carry out an appropriate Target/Actual analysis which is suitable for identifying significant misdevelopments at the group level or at the Business Area level and/or give the Chair of the Supervisory Board cause to investigate the developments and request additional information.

The MER, which has previously only been distributed to the Chair of the Supervisory Board, could also be provided to the Chair of the Audit Committee on a monthly basis. For example, from the MER, conclusions can be made on the necessity of impairment tests. Furthermore in this context, it is also very important for the Chair of the Audit Committee to be able to assess the forecast quality of the Board. However, up until now, the Chair of the Audit Committee has received the quarterly figures for the purposes of public reporting and also to make a forecast.

Until now, the Supervisory Board has basically been included in investment planning via the approval requirement for the annual investment planning for the group and the financing thereof as specified in the Articles of Association whereby the Supervisory Board decides on the approval of the total investment volume and/or the (group) investment target value and is informed about the allocation to the Business Areas and receives detailed information in the meetings. In addition, the Strategy, Finance and Investment Committee deals with investment planning at the group level and in the Business Areas.

In accordance with the recommendation on audit subject 3, it may be appropriate to include an additional investment level in the Investment Guidelines for large investments with an investment volume in excess of EUR 150 million. For investments in this level, - in addition to the measures discussed within the recommendations to audit subject 3 - there should also be regular reporting to the Supervisory Board, in particular in the case of budget overruns and other misdevelopments (e.g. technical problems). This can take place via information to the relevant committees (e.g. Strategy, Finance, and Investment Committee and the Audit Committee). The results of the investment recalculations for large projects of this type should be provided to the Supervisory Board as conclusions can be made on the forecast quality of the Management. We were informed that the existing investment guidelines were currently being expanded to include a separate rule for large investment projects.

Based on the follow-up report as per section 90 (1) of the Stock Corporation Act (AktG), the Supervisory Board could consider electing the Chair of the Audit Committee to the Strategy, Finance and Investment Committee so that risks relating to accounting can be identified early. It could also be worth considering also providing the Chair of the Audit Committee with the MER on a monthly basis. As a member of DAX, ThyssenKrupp is obliged to provide quarterly reports and the Supervisory Board and/or Audit Committee commissions the annual auditors to carry out a critical review of the quarterly reports. For example, concluded contracts and/or binding offers can necessitate contingency reserves. In the case of large projects, the intrinsic value of purchasing and production costs needs to be reviewed.

In addition to members of the Board, members of the Risk Committee, for example, should also be regularly invited to the meetings of the Supervisory Committees, specifically those of the Audit Committee and the Strategy, Finance and Investment Committee and report back from the different departments to give committee members the chance to identify who does the groundwork for the Board. Conclusions can also be made on the reliability of the internal processes.

## D. CLOSING REMARKS

---

The voluntary special audit at ThyssenKrupp gave rise to the aforementioned observations.

We have created this report to the best of our knowledge based on the investigations carried out by us, the documents provided, and the information imparted to us.

Hamburg/Frankfurt a. M., November 12, 2013

Markus Brinkmann  
Partner

ppa. Christoph Wunsch  
Senior Manager

Prof. Dr. Hans-Joachim Böcking  
Professor for Business  
Administration

BDO AG  
Wirtschaftsprüfungsgesellschaft  
(auditing company)

BDO AG  
Wirtschaftsprüfungsgesellschaft  
(auditing company)

Auditing  
Corporate Governance

ThyssenKrupp AG, Essen, Germany

---

*Attachment 1*

*General Engagement Terms for German Public Auditors and  
and Public Audit Firms as well as Special Conditions (as of January 1, 2002)*

# General Engagement Terms

## for

### Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften

#### [German Public Auditors and Public Audit Firms]

#### as of January 1, 2002

This is an English translation of the German text, which is the sole authoritative version

#### 1. Scope

(1) These engagement terms are applicable to contracts between *Wirtschaftsprüfer* [German Public Auditors] or *Wirtschaftsprüfungsgesellschaften* [German Public Audit Firms] (hereinafter collectively referred to as the *Wirtschaftsprüfer*) and their clients for audits, consulting and other engagements to the extent that something else has not been expressly agreed to in writing or is not compulsory due to legal requirements.

(2) If in an individual case, as an exception, contractual relations have also been established between the *Wirtschaftsprüfer* and persons other than the client, the provisions of No. 9 below also apply to such third parties.

#### 2. Scope and performance of the engagement

(1) Subject of the *Wirtschaftsprüfer's* engagement is the performance of agreed services – not a particular economic result. The engagement is performed in accordance with the *Grundsätze ordnungsmäßiger Berufsausübung* [Standards of Proper Professional Conduct]. The *Wirtschaftsprüfer* is entitled to use qualified persons to conduct the engagement.

(2) The application of foreign law requires – except for financial attestation engagements – an express written agreement.

(3) The engagement does not extend – to the extent it is not directed thereto – to an examination of the issue of whether the requirements of tax law or special regulations, such as, for example, laws on price controls, laws limiting competition and *Bewirtschaftungsrecht* [laws controlling certain aspects of specific business operations] have been observed; the same applies to the determination as to whether subsidies, allowances or other benefits may be claimed. The performance of an engagement encompasses auditing procedures aimed at the detection of the defalcation of books and records and other irregularities only if during the conduct of audits grounds therefor arise or if this has been expressly agreed to in writing.

(4) If the legal position changes subsequent to the issuance of the final professional statement, the *Wirtschaftsprüfer* is not obliged to inform the client of changes or any consequences resulting therefrom.

#### 3. The client's duty to inform

(1) The client must ensure that the *Wirtschaftsprüfer* – even without his specific request – is provided, on a timely basis, with all supporting documents and records required for and is informed of all events and circumstances which may be significant to the performance of the engagement. This also applies to those supporting documents and records, events and circumstances which first become known during the *Wirtschaftsprüfer's* work.

(2) Upon the *Wirtschaftsprüfer's* request, the client must confirm in a written statement drafted by the *Wirtschaftsprüfer* that the supporting documents and records and the information and explanations provided are complete.

#### 4. Ensuring independence

The client guarantees to refrain from everything which may endanger the independence of the *Wirtschaftsprüfer's* state. This particularly applies to offers of employment and offers to undertake engagements on one's own account.

#### 5. Reporting and verbal information

If the *Wirtschaftsprüfer* is required to present the results of his work in writing, only that written presentation is authoritative. For audit engagements the long form report should be submitted in writing to the extent that nothing else has been agreed to. Verbal statements information provided by the *Wirtschaftsprüfer's* staff beyond the engagement agreed to are never binding.

#### 6. Protection of the *Wirtschaftsprüfer's* intellectual property

The client guarantees that expert opinions, organizational charts, drafts, sketches, schedules and calculations – especially quantity and cost computations – prepared by the *Wirtschaftsprüfer* within the scope of the engagement will be used only for his own purposes.

#### 7. Transmission of the *Wirtschaftsprüfer's* professional Statement

(1) The transmission of a *Wirtschaftsprüfer's* professional statements (long form reports, expert opinions and the like) to a third party requires the *Wirtschaftsprüfer's* written consent to the extent that the permission to transmit to a certain third party does not result from the engagement terms.

The *Wirtschaftsprüfer* is liable (within the limits of No. 9) towards third parties only if the prerequisites of the first sentence are given.

(2) The use of the *Wirtschaftsprüfer's* professional statements for promotional purposes is not permitted, an infringement entitles the *Wirtschaftsprüfer* to immediately cancel all engagements not yet conducted for the client.

#### 8. Correction of deficiencies

(1) Where there are deficiencies, the client is entitled to subsequent fulfilment [of the contract]. The client may demand a reduction in fees or the cancellation of the contract only for the failure to subsequently fulfil [the contract]; if the engagement was awarded by a person carrying on a commercial business as part of that commercial business, a government-owned legal person under public law or a special government-owned fund under public law the client may demand the cancellation of the contract only if the services rendered are of no interest to him due to the failure to subsequently fulfil [the contract]. No. 9 applies to the extent that claims for damages exist beyond this.

(2) The client must assert his claim for the correction of deficiencies in writing without delay. Claims pursuant to the first paragraph not arising from an intentional tort cease to be enforceable one year after the commencement of the statutory time limit for enforcement.

(3) Obvious deficiencies, such as typing and arithmetical errors and *formelle Mängel* [deficiencies associated with technicalities] contained in a *Wirtschaftsprüfer's* professional Statements (long-form reports, expert opinions and the like) may be corrected - and also be applicable versus third parties - by the *Wirtschaftsprüfer* at any time. Errors which may call into question the conclusions contained in the *Wirtschaftsprüfer's* professional statements entitle the *Wirtschaftsprüfer* to withdraw – also versus third parties - such statements. In the cases noted the *Wirtschaftsprüfer* should first hear the client, if possible.

#### 9. Liability

(1) The liability limitation of § [ "Article" ] 323 (2) [ "paragraph 2" ] HGB [ "Handelsgesetzbuch": German Commercial Code ] applies to statutory audits required by law.

(2) Liability for negligence; an individual case of damages

If neither No. 1 is applicable nor a regulation exists in an individual case, pursuant to § 54a (1) no. 2 WPO [ "Wirtschaftsprüferordnung": Law regulating the Profession of *Wirtschaftsprüfer* ] the liability of the *Wirtschaftsprüfer* for claims of compensatory damages of any kind – except for damages resulting from injury to life, body or health - for an individual case of damages resulting from negligence is limited to €4 million; this also applies if liability to a person other than the client should be established. An individual case of damages also exists in relation to a uniform damage arising from a number of breaches of duty. The individual case of damages encompasses all consequences from a breach of duty without taking into account whether the damages occurred in one year or in a number of successive years. In this case multiple acts or omissions of acts based on a similar source of error or on a source of error of an equivalent nature are deemed to be a uniform breach of duty if the matters in question are legally or economically connected to one another. In this event the claim against the *Wirtschaftsprüfer* is limited to €5 million. The limitation to the fivefold of the minimum amount insured does not apply to compulsory audits required by law.

(3) Preclusive deadlines

A compensatory damages claim may only be lodged within a preclusive deadline of one year of the rightful claimant having become aware of the damage and of the event giving rise to the claim – at the very latest, however, within 5 years subsequent to the event giving rise to the claim. The claim expires if legal action is not taken within a six-month deadline subsequent to the written refusal of acceptance of the indemnity and the client was informed of this consequence. The right to assert the bar of the preclusive deadline remains unaffected. Sentences 1 to 3 also apply to legally required audits within statutory liability limits.

## 10. Supplementary provisions for audit engagements

(1) A subsequent amendment or abridgement of the financial statements or management report audited by a *Wirtschaftsprüfer* and accompanied by an auditor's report requires the written consent of the *Wirtschaftsprüfer* even if these documents are not published. If the *Wirtschaftsprüfer* has not issued an auditor's report, a reference to the audit conducted by the *Wirtschaftsprüfer* in the management report or elsewhere specified for the general public is permitted only with the *Wirtschaftsprüfer's* written consent and using the wording authorized by him.

(2) If the *Wirtschaftsprüfer* revokes the auditor's report, it may no longer be used. If the client has already made use of the auditor's report, he must announce its revocation upon the *Wirtschaftsprüfer's* request.

(3) The client has a right to 5 copies of the long-form report. Additional copies will be charged for separately.

## 11. Supplementary provisions for assistance with tax matters

(1) When advising on an individual tax issue as well as when furnishing continuous tax advice, the *Wirtschaftsprüfer* is entitled to assume that the facts provided by the client – especially numerical disclosures – are correct and complete; this also applies to bookkeeping engagements. Nevertheless, he is obliged to inform the client of any errors he has discovered.

(2) The tax consulting engagement does not encompass procedures required to meet deadlines unless the *Wirtschaftsprüfer* has explicitly accepted the engagement for this. In this event the client must provide the *Wirtschaftsprüfer*, on a timely basis, with all supporting documents and records – especially tax assessments – material to meeting the deadlines, so that the *Wirtschaftsprüfer* has an appropriate time period available to work therewith.

(3) In the absence of other written agreements, continuous tax advice encompasses the following work during the contract period:

- a) preparation of annual tax returns for income tax, corporation tax and business tax, as well as net worth tax returns on the basis of the annual financial statements and other schedules and evidence required for tax purposes to be submitted by the client
- b) examination of tax assessments in relation to the taxes mentioned in (a)
- c) negotiations with tax authorities in connection with the returns and assessments mentioned in (a) and (b)
- d) participation in tax audits and evaluation of the results of tax audits with respect to the taxes mentioned in (a)
- e) participation in *Einspruchs- und Beschwerdeverfahren* [appeals and complaint procedures] with respect to the taxes mentioned in (a).

In the aforementioned work the *Wirtschaftsprüfer* takes material published legal decisions and administrative interpretations into account

(4) If the *Wirtschaftsprüfer* receives a fixed fee for continuous tax advice, in the absence of other written agreements the work mentioned under paragraph 3 (d) and (e) will be charged for separately.

(5) Services with respect to special individual issues for income tax, corporate tax, business tax, valuation procedures for property and net worth taxation and net worth tax as well as all issues in relation to sales tax, wages tax, other taxes and duties require a special engagement. This also applies to:

- a) the treatment of nonrecurring tax matters, e. g. in the field of estate tax, capital transactions tax, real estate acquisition tax
- b) participation and representation in proceedings before tax and administrative courts and in criminal proceedings with respect to taxes, and
- c) the granting of advice and work with respect to expert opinions in connection with conversions of legal form, mergers, capital increases and reductions, financial reorganizations, admission and retirement of partners or shareholders, sale of a business, liquidations and the like.

(6) To the extent that the annual sales tax return is accepted as additional work, this does not include the review of any special accounting prerequisites nor of the issue as to whether all potential legal sales tax reductions have been claimed. No guarantee is assumed for the completeness of the supporting documents and records to validate the deduction of the input tax credit.

## 12. Confidentiality towards third parties and data security

(1) Pursuant to the law the *Wirtschaftsprüfer* is obliged to treat all facts that he comes to know in connection with his work as confidential, irrespective of whether these concern the client himself or his business associations, unless the client releases him from this obligation.

(2) The *Wirtschaftsprüfer* may only release long-form reports, expert opinions and other written statements and the results of his work to third parties with the consent of his client.

(3) The *Wirtschaftsprüfer* is entitled – within the purposes stipulated by the client – to process personal data entrusted to him or allow them to be processed by third parties.

## 13. Default of acceptance and lack of cooperation on the part of the client

If the client defaults in accepting the services offered by the *Wirtschaftsprüfer* or if the client does not provide the assistance incumbent on him pursuant to No. 3 or otherwise, the *Wirtschaftsprüfer* is entitled to cancel the contract immediately. The *Wirtschaftsprüfer's* right to compensation for additional expenses as well as for damages caused by the default or the lack of assistance is not affected, even if the *Wirtschaftsprüfer* does not exercise his right to cancel.

## 14. Remuneration

(1) In addition to his claims for fees or remuneration the *Wirtschaftsprüfer* is entitled to reimbursement of his outlays: sales tax will be billed separately. He may claim appropriate advances for remuneration and reimbursement of outlays and make the rendering of his services dependent upon the complete satisfaction of his claims. Multiple clients awarding engagements are jointly and severally liable.

(2) Any set-off against the *Wirtschaftsprüfer's* claims for remuneration and reimbursement of outlays is permitted only for undisputed claims or claims determined to be legally valid.

## 15. Retention and return of supporting documentation and records

(1) The *Wirtschaftsprüfer* retains, for seven years, the supporting documents and records in connection with the completion of the engagement – that had been provided to him and that he has prepared himself – as well as the correspondence with respect to the engagement.

(2) After the settlement of his claims arising from the engagement, the *Wirtschaftsprüfer*, upon the request of the client, must return all supporting documents and records obtained from him or for him by reason of his work in the engagement. This does not, however, apply to correspondence exchanged between the *Wirtschaftsprüfer* and his client and to any documents of which the client already has the original or a copy. The *Wirtschaftsprüfer* may prepare and retain copies or photocopies of supporting documents and records which he returns to the client

## 16. Applicable law

Only German law applies to the engagement, the conducting thereof and any claims arising therefrom.

## **SPECIAL CONDITIONS FOR THE INCREASE OF THE LIABILITY UNDER THE GENERAL ENGAGEMENT TERMS AS OF JANUARY 1, 2002**

The amounts of EUR 4 million and EUR 5 million respectively as provided for in No.9 part 2 of the attached General Engagement Terms are uniformly substituted by the amount of EUR 5 million.

If, in the client's opinion, the foreseeable contractual risk will be considerably higher than EUR 5 million, BDO AG Wirtschaftsprüfungsgesellschaft will agree, at the client's request, to offer to the client an increased liability limit if and to the extent the liability insurance for the increased amount can be obtained from a German professional liability insurer; the premium expense arising out of an increased liability will be subject to a separate agreement.

The above mentioned provisions are not applicable when a greater or lesser liability limit has been provided by law for the respective professional service, particularly in connection with a statutory audit. In such a case the statutory liability regulations continue to be applicable.

If various causes of damage occur, BDO AG Wirtschaftsprüfungsgesellschaft is liable within the scope of the increased liability limit only to the extent that causation can be attributed to BDO AG Wirtschaftsprüfungsgesellschaft or its employees in relation to other causes relevant to the damage. This applies in particular in the case of a joint assignment with other auditors. If, as agreed by the client, a third party is engaged for the execution of an assignment BDO AG Wirtschaftsprüfungsgesellschaft will only be liable for negligence in connection with the selection of that third party.

BDOAG  
Wirtschaftsprüfungsgesellschaft