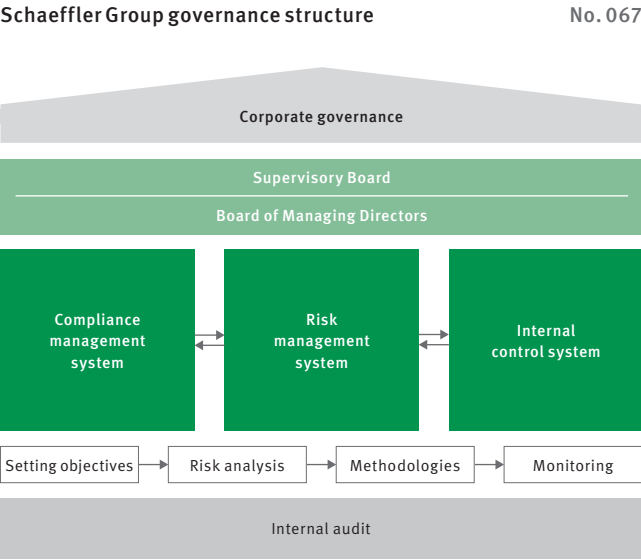


3. Governance structure

The Schaeffler Group considers maintaining the corporate culture of a global family business essential and intends to play a leading role as a listed family business. Its focus is on customer relationships and acting with integrity. Its corporate values drive the nature of its transactions. Transactions and business relationships inconsistent with the group’s corporate values are rejected.



The governance structure promotes transparency and supports the values of a global family business (sustainable, innovative, excellent, and passionate). The components of the governance structure support our business units in effectively identifying and managing risk.

The Schaeffler Group has continued to improve the processes within its governance structure with a view to meeting the needs of its customers while at the same time protecting the company. The governance structure is aimed at promoting the coordinated operation of the subsystems and, hence, the early identification of risks to the continued existence and development of the Schaeffler Group. Clearly assigned responsibilities and a robust internal control system are in place to manage significant risks. The Group Compliance and Risk Committee (GCRC) represents a key governance component in this regard, increasing transparency in internal structures, the organization, and in responsibilities. The GCRC is chaired by the Schaeffler Group’s Chief Compliance Officer. It consists of the heads of the subsystems and the heads of other risk and corporate functions. The GCRC is responsible for assisting the Board of Managing Directors with its organizational responsibilities with respect to compliance and risk management. Among the key objectives of the GCRC are defining and delineating responsibilities and interfaces and preventing redundancies in the process. In addition, it is expected to create a consistent and complete view of the risk situation in the divisions, functions, and regions based on a uniform measurement and prioritization methodology. A further objective is developing and monitoring risk mitigation activities. The Compliance & Risk Working Group consisting of staff representatives from the functions represented on the GCRC provides operational support to the GCRC.

The activities of the subsystems within the governance structure are coordinated based on the internationally recognized three lines of defense model. It assigns clear responsibility for dealing with risks to the company’s continued existence and development and is based on the principle that primary responsibility for a risk lies with its originator.

Three lines of defense model

No. 068

Lines of defense	Responsible unit or function	Area of responsibility
First line of defense	Operating business units	At the first tier, operating business units are responsible for performing controls within all business processes to prevent risk. If prevention is not feasible, risks have to be identified and reduced to an appropriate level.
Second line of defense	Risk functions (e. g. controlling, risk management, compliance, and legal)	The second tier defines global standards and controls, regularly monitors compliance with them, and reports on their effectiveness. It is also responsible for regular and independent risk assessment.
Third line of defense	Internal Audit	The third tier is the audit by Internal Audit. Independent and objective audits are designed to ensure process efficiency in risk management, internal controls, and corporate governance.

The business units bear primary responsibility for the risks inherent in their business. Hence, the Schaeffler Group's employees represent the first line of defense against potential risks. The Schaeffler Code of Conduct encourages them to turn to their supervisor or the corresponding control function with any questions or concerns they might have regarding dealing with risks and inappropriate business practices. An anonymous whistleblowing system is available for this purpose where necessary.

With its corporate governance structure and its three lines of defense model, the Schaeffler Group fulfils its obligation to manage the company responsibly and to maintain effective controls.

Proper Performance of Reasonable Assurance Engagements Relating to Compliance Management Systems IDW PS 980 by an independent audit firm, the next step planned is a review of the implementation of the CMS by an independent audit firm.

The CMS comprises, in particular, managing and monitoring the activities necessary to prevent, or detect early on, violations of law in the area of corruption, money-laundering, competition and antitrust law, and economic criminal activity. It also serves to actively manage risk and protect the company and its employees. The CMS consists of seven core components: Compliance culture, compliance objectives, vulnerability analysis, compliance program, compliance organization, communication, and monitoring and improvement.

3.1 Compliance management system

Integrity is one of the mainstays of the Schaeffler Group's manner of conducting business. Under the Schaeffler Code of Conduct, the Board of Managing Directors and all employees are required to comply with all applicable local, national, and international laws and regulations, wherever the Schaeffler Group does business. A compliance organization covering the entire Schaeffler Group provides them with support in doing so.

The Schaeffler Group's Board of Managing Directors emphatically supports the underlying compliance management system (CMS) and the necessity of consistently complying with legal requirements and internal regulations.

The CMS is based on the three pillars of prevention, detection, and reaction and is part of the second line of defense within the Schaeffler Group's governance structure. The CMS in its current state is the result of a comprehensive revision initiated by the Board of Managing Directors as part of the "Compliance Fit & Proper" program, a component of the "ONE Schaeffler" program. Following the successful completion of a review of the underlying conceptual design in accordance with the Principles for the

The compliance organization derives its arrangements for preventing violations of antitrust and competition legislation, corruption, economic crime, and money-laundering from a regular groupwide risk analysis using a risk based approach. The risk analysis provides information on the current situation with respect to risks arising from operations and on the effectiveness of the preventive arrangements in place. The analysis is primarily based on interviews with management and employees of all divisions and regions with the objective of obtaining estimates of the probability of occurrence and the size of the potential loss of pertinent risk scenarios from the interviewee that are as close to the business processes as possible. These estimates are supplemented with sector and expert knowledge, experience with actual compliance violations, results of controls and audits, as well as by using operations-, market-, and country-specific risk criteria ranging from publicly available risk indicators, such as the Corruption Perception Index compiled by Transparency International, to issues regarding the location-specific design of Sales and Distribution.

The Schaeffler Group's Group Chief Compliance Officer heads up the compliance organization and reports directly to the Chief Executive Officer. The Group Chief Compliance Officer also has a

reporting line to the Chairman of the Supervisory Board and reports to the chairman of the audit committee on a regular basis. The compliance department provides the Group Chief Compliance Officer with the support of a network of experienced compliance specialists spanning all of the Schaeffler Group's Europe, Americas, Greater China, and Asia/Pacific regions. He also utilizes a centralized team of experts located at the corporate head office in Herzogenaurach which was expanded in 2016 and consists of the "Advisory", "Risk Analysis & Solutions", and "Forensics & Investigations" departments. The responsibilities of this team of experts include defining and monitoring appropriate groupwide compliance standards and activities, consulting on compliance, and improving processes and controls. The team is also responsible for independently investigating alleged violations and following up on the necessary consequences. It analyzes the causes of misconduct, derives suggestions for remedial measures, and follows up on their implementation. Violations of laws and regulations or of internal rules on compliance with these are not tolerated and result in disciplinary action.


Measures designed to prevent compliance violations include the Schaeffler Group's Code of Conduct, guidelines on behavior in compliance with antitrust and competition legislation, fighting corruption, and protecting confidential information, web-based and classroom training sessions, and a compliance helpdesk available for consultation on specific compliance issues. Training sessions are continually refined and updated and adapted to the employees' areas of responsibility. For instance, case studies in the Risk Awareness training session are customized to the relevant business units in order to make the presentation of potential risks as specific and clear as possible. In addition, the company has also put in place arrangements for detecting possible compliance violations; these arrangements include audits and controls as well as a whistleblowing system which can be used to report violations on an anonymous basis. All such reports received are reviewed independently. Reprisals against employees reporting concerns about misconduct within the company in good faith are prohibited.

The Schaeffler Group has further expanded its arrangements and measures for complying with legal requirements and internal rules in 2016. A new code of conduct applicable to all employees worldwide was introduced. In addition to requirements relating to general conduct, the principles and practices described also cover conduct vis-à-vis business partners and third parties, dealing with sensitive information, employees and co-workers, and requirements regarding the environment, health, and safety. In accordance with the corporate values, bribery or any form of corruption are not tolerated. All Schaeffler Group employees are expressly prohibited from engaging in bribery or corruption in any way. The same applies to conduct violating competition or anti-trust laws. The Schaeffler Group stays away from any

transactions that cannot be effected or continued without unacceptable conduct.


The company continued the implementation of a register of contacts with competitors as well as a groupwide business partner due diligence process. This underlines the standard the Schaeffler Group expects of its business partners with respect to acting with integrity and abiding by rules. In 2016, the compliance training program included training on risk awareness, the Schaeffler Code of Conduct, and security of information including classification of information. New training measures were introduced to protect against cybercrime and CEO fraud.

The company maintains a groupwide insider list in order to comply with capital markets regulations. The members of the Board of Managing Directors and the Supervisory Board as well as employees were informed of their obligations under capital markets laws and the consequences of the listing. In addition, there is an insider committee whose activities include maintaining the insider list, deciding on how to deal with potential insider information, and ensuring compliance with the requirements of capital markets laws.

 For further detail on significant compliance-related risks see "Report on opportunities and risks".

3.2 Risk management system


Like the compliance management system, the risk management system is part of the second line of defense in the Schaeffler Group's governance structure. It comprises all activities and arrangements made to identify, assess, manage, and monitor risk. A risk is defined as the danger that events or actions will prevent a company from achieving its plan or successfully implementing its strategies. For all identified risks, the probability of occurrence and possible impact on achieving objectives are continually identified, assessed, appropriate action initiated and followed-up on.

 For further detail on the risk management system see "Report on opportunities and risks".

3.3 Internal control system

The second line of defense also comprises the Schaeffler Group's internal control system. The internal control system consists of technological and organizational arrangements and controls that have been systematically designed to ensure compliance with guidelines and to prevent loss or damage that may be caused by the company's employees or by third parties. Controls can be

performed both process-dependent or independently of the process. The Schaeffler Group's internal control system is based on the COSO model and consists of the following components: Control environment, risk assessment, control activities, information and communication, and monitoring. It is focused on financial reporting and represents the arrangements and controls ensuring that the consolidated financial statements are prepared in accordance with financial reporting standards and ensuring accurate external financial reporting.

 For further detail on the internal control system see "Report on opportunities and risks".

3.4 Internal Audit

Internal Audit represents the third line of defense of the Schaeffler Group's governance structure. Internal Audit provides independent and objective audit and consulting services focused on adding value and improving business processes. The internal audit function contributes to meeting the corporate objectives the Schaeffler Group has communicated by assessing and helping to improve the effectiveness of the compliance management system, risk management, controls, and management and supervisory processes using a systematic and goal-oriented approach. Responsibility for establishing the internal audit function and for its effectiveness rests with the Board of Managing Directors and cannot be delegated. Hence, Internal Audit reports to the entire Board of Managing Directors. Organizationally, Internal Audit is assigned to the Chief Executive Officer of Schaeffler AG.

The Schaeffler Group has made the following arrangements to ensure the independence and objectivity of Internal Audit:

- direct organizational link to the Chief Executive Officer to ensure there are no gaps in audit coverage;
- neither the head of Internal Audit nor audit staff have any operational responsibilities;
- reports annually on potential impairment of independence to the CEO/Board of Managing Directors/audit committee;
- audit planning and significant changes therein have to be approved by the Board of Managing Directors and documented appropriately.

Internal Audit consists of the functions "Methods, Reporting and Quality Assurance", "Corporate Audits" and "IT and Special Audits". It also has locations in each of the four regions.

The responsibilities of Internal Audit specifically include, but are not limited to, the following activities:

- audit and assessment of the appropriateness, efficiency, and effectiveness of the internal control system;
- audit and assessment of the appropriateness, efficiency, and effectiveness of the management and supervisory processes;
- audit and assessment of the finance and accounting systems, the information system, and the reporting system;
- audit and assessment of the effectiveness of risk and compliance management;
- audit and assessment of the effectiveness of arrangements for preventing and detecting fraud;
- audit of arrangements for safeguarding assets;
- audit and assessment of the implementation of and compliance with legal requirements and the company's internal rules ("orderliness");
- performance of special investigations with respect to fraud, conflicts of interest and other irregularities.

Internal Audit performs systems and effectiveness audits. Systems audits involve auditing selected areas (e.g. Procurement) and documenting and analyzing the actual processes in place. Any findings documented during such systems audits are assigned to one of three assessment areas ("orderliness", "internal monitoring system", "business processes"). Effectiveness audits involve testing the effectiveness of the risk management system or the internal control system within the Schaeffler Group. Compliance risks are covered in the "orderliness" assessment area.

In a risk analysis done in preparation for audit assignments, Internal Audit exchanges information with other departments (e.g. Compliance and Corporate Security, Controlling, Legal, Quality, Risk Management).

In order to obtain sufficient reliable, relevant, and constructive information to achieve its audit objectives, Internal Audit regularly performs its audit assignments on location.

In its audit reports, Internal Audit communicates its findings, its recommendations for mitigating risk, and the persons responsible for implementation, with whom they agree binding implementation dates. In a monitoring and follow-up process, Internal Audit monitors implementation of its recommendations for remediating identified deficiencies.

In accordance with the International Standards for the Professional Practice of Internal Auditing 2016 of the Institute of Internal Auditors (IIA), the head of Internal Audit has established a quality assurance and improvement program covering all of Internal Audit's responsibilities.