Rules of Procedure of the Audit and Cybersecurity Committee of GEA Group Aktiengesellschaft

Section 1
Basic principles

(1) The Audit and Cybersecurity Committee of the Supervisory Board of GEA Group Aktiengesellschaft is set up on the basis of the Rules of Procedure of the Supervisory Board of GEA Group Aktiengesellschaft. Unless stated otherwise in the Rules of Procedure of the Audit and Cybersecurity Committee, the provisions set forth in the Rules of Procedures of the Supervisory Board of GEA Group Aktiengesellschaft will apply mutatis mutandis. In particular, this holds true for the provisions governing the calling of meetings, resolutions, the minutes, reports to the Supervisory Board as well as confidentiality obligations.

(2) Pursuant to section 107 (3) sentence 4 AktG (Aktiengesetz – German Stock Corporation Act), the Rules of Procedure of the Audit and Cybersecurity Committee lay down the responsibilities delegated to the Audit and Cybersecurity Committee for final deliberation and/or the extent to which the Audit and Cybersecurity Committee shall merely prepare the matters referred to it for the Supervisory Board.

(3) For the purpose of performing the tasks assigned to it, the Audit and Cybersecurity Committee will be entitled to request all necessary information from the auditor and the Executive Board, and to inspect all business documents of the company and the group or to require that the Executive Board submit such documents.

(4) The Audit and Cybersecurity Committee will meet at least four times a year. Additional meetings may be held, if necessary.

(5) Audit and Cybersecurity Committee meetings will be called by the Chair of the Audit and Cybersecurity Committee by giving one week's notice of such a meeting. Additions to the agenda must be communicated no later than 4 days prior to the meeting unless an urgent case justifies later notification.

Section 2
Composition

(1) The Audit and Cybersecurity Committee is made up of four Supervisory Board members, two shareholder and two employee representatives, respectively.

(2) The Supervisory Board ensures that the Audit and Cybersecurity Committee members have the necessary specialized knowledge and abilities as well as the adequate sector experience to properly perform the committee's duties.

(3) The Audit and Cybersecurity Committee will be headed by its Chair, who is elected from

amongst the shareholder representatives by the Supervisory Board.

(4) The Audit and Cybersecurity Committee Chair shall be independent and shall have expertise in the areas of accounting and auditing (which in each case also includes sustainability reporting and the respective audit), in particular knowledge and experience in the application of accounting principles and internal control systems. He/she must neither be the Chair of the Supervisory Board nor a former member of the company's Executive Board whose term expired less than two years ago. The Committee Chair shall be a financial expert as defined in section 100 (5) AktG.

Section 3
Basic responsibilities and powers of the Audit and Cybersecurity Committee

(1) In particular, the Audit and Cybersecurity Committee will be responsible for monitoring the accounting process, the efficiency of the internal control system, the risk management system, the internal audit system, the audit of the annual financial statements (in particular the selection and the independence of the auditor, the quality of the audit as well as the additional services provided by the auditor, the engagement of the auditor, the definition of audit focus areas and the agreement on an audit fee), information- and cybersecurity, sustainability reporting and the respective audit, as well as compliance.

(2) The Audit and Cybersecurity Committee will assist the Executive Board in an advisory capacity in the relevant subject-areas. As one of two financial experts of the Supervisory Board, the Audit and Cybersecurity Committee Chair will maintain regular contact with the company's Chief Financial Officer between the scheduled meetings.

(3) The Chair of the Supervisory Board and the Audit and Cybersecurity Committee Chair as well as any other member of the Audit and Cybersecurity Committee - via the Audit and Cybersecurity Committee Chair - may obtain information directly from the heads of those corporate functions of the company which - at corporate or group level - are responsible for the tasks relating to the Audit and Cybersecurity Committee in accordance with paragraph (1) above. If the Chair of the Supervisory Board or the Audit and Cybersecurity Committee Chair obtain such information, they will communicate this information to the (other) members of the Audit and Cybersecurity Committee and notify the Executive Board and/or the Executive Board member responsible for the corporate function in question accordingly without undue delay.

Section 4
Accounting and non-financial reporting

(1) The Audit and Cybersecurity Committee will discuss matters relating to accounting, in particular those arising in connection with fundamental issues, such as the application of new or amendments to accounting standards hitherto applied as well as accounting options exercised by the company.

(2) The Audit and Cybersecurity Committee will prepare the proceedings and resolutions of the Supervisory Board in connection with the adoption of the annual financial statements, the approval of the consolidated financial statements as well as the group management report combined with the management report of GEA Group Aktiengesellschaft, including the non-financial group declaration and, if prepared, the separate non-financial group report, as well as on the appropriation of net earnings. The Audit and Cybersecurity Committee will submit proposals for resolution to the Supervisory Board. For this purpose, the Audit and Cybersecurity Committee will conduct a preliminary review of the annual and consolidated financial statements, the combined management report including the non-financial group declaration, the proposal for the appropriation of net earnings and, if applicable, the non-financial group report. The Audit and Cybersecurity Committee is responsible for commissioning any external audit or audit reviews of the content of non-financial reporting respectively.

(3) The Audit and Cybersecurity Committee will discuss with the Executive Board the quarterly statements and the half-yearly financial report, and – where relevant – the auditor's report on the audit review of the half-yearly reports.

On a case-by-case basis, the Audit and Cybersecurity Committee will discuss with the Executive Board specific accounting and valuation matters of group-wide importance that arise in connection with the separate and consolidated financial statements.

Section 5
Audit of the annual financial statements

(1) The Audit and Cybersecurity Committee will discuss the documents relating to the annual financial statements with the Executive Board and the auditor. It will discuss the assessment of the audit risk, the audit strategy and audit planning, including the audit methods, the audit process and the audit focus areas, as well as the audit results with the auditor. The Audit and Cybersecurity Committee will receive the auditor's reports on the results of the audit, also with regard to the internal control and risk management system where the accounting process is concerned.

(2) The Audit and Cybersecurity Committee will prepare the proceedings and resolutions of the Supervisory Board in connection with the proposal for the appointment of an auditor to be submitted to the Annual General Meeting and also submit a corresponding proposal to the Supervisory Board. For drawing up its proposal, the committee must verify the quality of the audits performed by the auditor. It will obtain a statement from the designated auditor in which the latter sets out whether and – if applicable – which business, financial, personal or other relationships that could cast doubt on its independence do exist between the auditor, its governing bodies and head auditors, on the one hand, and the company and its board members, on the other hand. This statement must include all members of the auditor's network. Moreover, this statement is also to embrace the extent to which other services were provided to the company in the previous fiscal year, in particular in terms of consulting fees, and/or to the extent to which such services have been contractually agreed for the following year.

(3) Implementing the resolution passed by the Annual General Meeting relative to the appointment of the auditor, the Audit and Cybersecurity Committee will prepare the audit engagement for the annual and consolidated financial statements including the combined management report and will resolve on its key terms and conditions. The audit engagement will specify the audit scope, audit planning and methods, the audit focus areas determined by the Audit and Cybersecurity Committee, the agreed audit fee as well as the auditor's duty to inform. Within the framework of the audit engagement, the Audit and Cybersecurity Committee and the auditor agree that the Audit and Cybersecurity Committee Chair shall be promptly notified of any potential grounds for exclusion or partiality that arise in the course of the audit, unless such reasons are immediately eliminated.

(4) The Audit and Cybersecurity Committee Chair and the Chair of the Supervisory Board will sign the letter of engagement.

(5) Assignments to the auditor or companies to which the auditor is related in legal, economic or personal terms may only be given if the services involved do not constitute prohibited non-audit services. Such permitted non-audit services require the prior approval of the Audit and Cybersecurity Committee that shall give proper consideration to threats to auditor independence and the safeguards put in place. The Audit and Cybersecurity Committee will regulate the specifics of the procedure to be followed in a separate guideline.

(6) The Audit and Cybersecurity Committee will prepare the tender of audit engagement mandates on behalf of the Supervisory Board and handle the entire tendering process with complete autonomy and with the support of the company up to the point where a recommendation is submitted to the Supervisory Board. In this context, it will observe the applicable legal provisions, in particular the guidelines on statutory audits set forth in EU Regulation No. 537/2014.

(7) If the Executive Board intends to hire staff of the auditor as employees holding senior management functions within the company or at one of its subsidiaries while reporting directly to the Executive Board, the latter shall confer with the Audit and Cybersecurity Committee on such matter. In this context, the rules and regulations stipulated in the Wirtschaftsprüferordnung (WPO - German Public Accountants Act), in particular section 43 (3) WPO, must be observed.

Section 6
Cooperation with the auditor

(1) It is agreed with the auditor that the latter will provide information on the following topics – amongst other things and not limited to such topics - during the committee meetings:

1. all findings and incidences of significance for the tasks of the Supervisory Board that come to the auditor's attention in the course of the audit. Moreover, the Audit and Cybersecurity Committee Chair shall be notified thereof without undue delay;

2. any facts ascertained in the course of the audit that are inconsistent with the declaration on the German Corporate Governance Code issued by the Executive Board and the Supervisory Board;

3. all critical accounting matters as well as alternatives to the accounting treatment of transactions discussed with the Executive Board, as well as any essential writ- ten communication between the auditor and the Executive Board;

4. any controversial issues that have arisen between the auditor and the Executive Board in the course of the audit and the audit review;

5. any essential shortcomings of the internal control and risk management system, in particular with regard to the accounting process;

6. any other circumstances that must be disclosed or reported to the Audit Commit- tee under the law, in particular as set out in EU Regulation No. 537/2014 on statutory audits.

(2) Between meetings, the Audit and Cybersecurity Committee Chair will regularly consult with the auditors on current issues relating to the audit of the financial statements, in particular their progress, whereupon he/she will provide a corresponding report to the Audit and Cybersecurity Committee.

Section 7
ICS, risk management, internal audit, information- and cybersecurity and compliance

(1) The Audit and Cybersecurity Committee will deal with fundamental issues relating to the internal control system that is to be set up by the Executive Board, in particular its appropriateness and efficiency; in this respect, the Audit and Cybersecurity Committee will also make sure that sustainability aspects and targets important for the company are adequately considered, including processes and systems for registration and processing of data related to sustainability. These topics will be discussed with the Executive Board, specifically with regard to the accounting process.

(2) The Audit and Cybersecurity Committee will discuss with the Executive Board the basic principles of risk identification and the risk management system that is to be set up by the Executive Board; moreover, it will deal with the company's risk monitoring system, in particular its appropriateness and efficiency; in this respect, the Audit and Cybersecurity Committee will also make sure that sustainability aspects and targets important for the company are adequately considered, including processes and systems for registration and processing of data related to sustainability. As part of the Executive Board's regular reporting on risks and opportunities, the Audit and Cybersecurity Committee will receive information on any changes that might have occurred. This will include legal disputes and risks to the group resulting therefrom.

(3) Based on the audit results for the current fiscal year prepared by Internal Audit and discussed by the Audit and Cybersecurity Committee on a quarterly basis, as well as further intelligence, the Audit and Cybersecurity Committee will discuss and deliberate the preliminary audit plan for the next fiscal year with the Executive Board member responsible for Internal Audit as well as the Head of Internal Audit. Proposals on audits and audit focus areas submitted by the

Audit and Cybersecurity Committee shall be incorporated into the audit plan, which must be approved by the Executive Board prior to the start of the new fiscal year. Subsequently, the audit plan will be presented to the Audit and Cybersecurity Committee for its implied consent. Moreover, the Audit and Cybersecurity Committee will also discuss and deliberate the fundamental issues regarding the organizational set-up, resources and the personnel allocated to Internal Audit with the Executive Board member responsible for Internal Audit as well as the Head of Internal Audit. During the meetings of the Audit and Cybersecurity Committee, the Head of Corporate Internal Audit will regularly report on the main findings ascertained in the course of the internal audits conducted. The Audit and Cybersecurity Committee will discuss the performance and the efficiency of the corporate internal audit department with the Executive Board.

(4) Apart from the potential requests for information addressed to the Head of Internal Audit by the Chair of the Supervisory Board and the Audit and Cybersecurity Committee Chair in accordance with section 3 (3) of these Rules of Procedure, the Head of Internal Audit may in turn also get directly in touch with the Committee Chair or the Chair of the Supervisory Board in special exceptional circumstances. For instance, such exceptional circumstance would occur if the Executive Board restricted the functionality of Internal Audit to such an extent that the proper execution of the independent oversight function on the part of Internal Audit would no longer be guaranteed. In such cases, the Executive Board member responsible for Internal Audit must also be notified without undue delay.

(5) During its meetings, the Audit and Cybersecurity Committee will receive regular reports by the Chief Information Security Officer related to information- and cybersecurity topics. Apart from the Chair of the Supervisory Board, the Audit and Cybersecurity Committee Chair and/or the members of the Audit and Cybersecurity Committee will be entitled to obtain information directly from the Chief Information Security Officer outside of meetings. Section 3 (3) of these Rules of Procedure will also apply in such cases.

(6) During its meetings, the Audit and Cybersecurity Committee will receive regular reports on compliance issues. Apart from the Chair of the Supervisory Board, the Audit and Cybersecurity Committee Chair and/or the members of the Audit and Cybersecurity Committee will be entitled to obtain information directly from the Chief Compliance Officer outside of meetings. Section 3 (3) of these Rules of Procedure will also apply in such cases. The Audit and Cybersecurity Committee must be notified of any changes to the compliance budget.

(7) Furthermore, as early as possible, the Audit and Cybersecurity Committee will receive reports from the Executive Board on the following items during its meetings, with the Audit and Cybersecurity Committee Chair receiving such reports between meetings:

1. any and all substantial shortcomings and essential weaknesses in the organization and implementation of the accounting process, the internal control system, risk management as well as the internal audit,
2. new significant incidents related to information- and cybersecurity and
3. new significant compliance violations.

(8) The Audit and Cybersecurity Committee will monitor the efficiency of the EMIR system that ensures compliance with the provisions of Regulation (EU) No. 648/2012 as well as the relevant laws passed in connection therewith. The Audit and Cybersecurity Committee will receive the audit certificate in accordance with section 20 (3) WpHG (Wertpapierhandelsgesetz – German Securities Trading Act).

Section 8
Reports and complaints

On a regular basis, the Audit and Cybersecurity Committee will be advised by the Executive Board and/or the Chief Compliance Officer of the receipt and handling of information or complaints from individuals employed with the company, the group or third parties in relation to accounting, internal controls, the audit of the annual financial statements and other matters.

Section 9
Internal governance

(1) The meetings of the Audit and Cybersecurity Committee will be attended by the Chairman of the Executive Board, the Chief Financial Officer as well as the auditor, unless otherwise determined by the Audit and Cybersecurity Committee Chair on a case-by-case basis.

If the auditor is expressly called in as an expert or respondent by the Audit and Cybersecurity Committee Chair in addition to his/her regular participation pursuant to subparagraph (1) above, the Chairman of the Executive Board and the Chief Financial Officer shall not attend the relevant meeting unless the Supervisory Board or the Audit and Cybersecurity Committee deem their participation necessary.

(2) The Audit and Cybersecurity Committee Chair may permit further persons to attend the meetings of the Audit and Cybersecurity Committee.

(3) As necessary, the Audit and Cybersecurity Committee will meet without the Executive Board and also consult with the auditor on a regular basis without the Executive Board.

(4) The Audit and Cybersecurity Committee Chair will be entitled to inspect any and all business documents, books, business information saved on data carriers, as well as assets and liabilities of the company. Following a decision of the Audit and Cybersecurity Committee, this right may also be extended to the committee members.

(5) For performing its duties, the Audit and Cybersecurity Committee may use the services of auditors, legal advisors as well as other external consultants on a case-by-case basis. The Audit and Cybersecurity Committee Chair may permit such individuals and other respondents to attend committee meetings. The Audit and Cybersecurity Committee Chair will be entitled to obtain reasonable external advice after informing the Chair of the Supervisory Board accordingly. The expenses will be borne by the company.

Section 10
Reports and statements

(1) The Audit and Cybersecurity Committee Chair will deliver a report on the Audit and Cybersecurity Committee's work no later than at the next Supervisory Board meeting following the respective committee meeting.

(2) Insofar as statements for implementing resolutions passed by the Audit and Cybersecurity Committee have to be issued or accepted, the Chair, or in his/her absence the Supervisory Board Chair, will act on behalf of the Audit and Cybersecurity Committee