Format of Meetings in Fiscal 2022

		Committees						
	Plenary	Personnel and Governance	Audit and Compliance	Technology and Strategy	Nomination	People and Culture	Finance and Investment	Go-To-Market and Operations
Total number of meetings	7	4	11	6	4	5	11	4
Thereof physical meeting	0	0	2[1]	1[1]	0	0	0	0
Thereof hybrid session	4	3	9[2]	5[3]	2	0	10[2,3]	4
Thereof telephone/video conference	3	1	0	0	2	5	1	0

[1] Thereof one joint meeting between the Technology and Strategy Committee and the Audit and Compliance Committee
[2] Thereof two joint meetings between the Finance and Investment Committee and the Audit and Compliance Committee
[3] Thereof one joint meeting between the Finance and Investment Committee and the Technology and Strategy Committee

The Work of the Supervisory Board Committees

The committees made a key contribution to the work of the Supervisory Board in 2022, notably by preparing relevant agenda items and resolutions for Supervisory Board meetings and by regularly reporting on their deliberations in general and on their decisions taken. The following committees were in place in the year under review:

– **Personnel and Governance Committee**, **Audit and Compliance Committee**, **Finance and Investment Committee**, **Technology and Strategy Committee**, **People and Culture Committee**, **Nomination Committee, Go-To-Market and Operations Committee**

Each of the aforementioned committees was active in 2022. For more information about the Supervisory Board committees, particularly their respective composition, tasks, and responsibilities, see the *Corporate Governance Statement* and the *Corporate Governance section of SAP's Web site*.

Besides the matters described above, the committees focused primarily on the following topics in 2022:

– The *Personnel and Governance Committee* held four regular meetings in the reporting year. In particular, the Committee, in fulfillment of the tasks assigned to it, extensively prepared and discussed in advance the deliberations of the Supervisory Board and its resolutions on the new Executive Board compensation system. It also approved two loans for officers of SAP who hold procura powers. At its meeting in February, it did preparatory work on the Supervisory Board's proposal to the 2022 Annual General Meeting of Shareholders with respect to the adjustment of Supervisory Board compensation. It also deliberated on the draft Supervisory Board report for the financial year 2021, SAP's competitive position, and the Executive Board's customer relationship management (CRM) strategy. When the Committee met in April 2022, it reviewed the composition of the Supervisory Board committees that was envisaged after the Annual General Meeting of Shareholders on May 18, 2022. On July 27, 2022, the Committee conducted its regular review of pension payments made to former Executive Board members and deliberated on the creation of a formalized process for the feedback of the Supervisory Board vis-à-vis Executive Board members. In addition, it updated the target number of women on the Executive Board and the diversity concept. It was resolved that SAP should voluntarily keep to its target of having two women on the Executive Board. The Committee additionally dealt, at both its April and July meetings, with the search for a successor to SAP's CFO Luka Mucic, who would be leaving the Company in March 2023. Even between meetings, the Committee members were in continual contact with the personnel consulting firm that had been enlisted for this purpose, and conducted interviews of potential candidates. The Committee chairperson reported on the status of the candidate search in the meetings of the full Supervisory Board. Finally, in August, the Committee initiated the proposed resolution by the full Supervisory Board on the appointment of the new CFO. The focus of the October 2022 meeting was once again the aforementioned feedback process and its implementation. In addition, the Committee deliberated on the process for cultivating and shortlisting internal talents who were considered potential successors to Executive Board positions.

– The *Audit and Compliance Committee* held 11 regular meetings in 2022 – two of which jointly with the Finance and Investment Committee and one jointly with the Technology and Strategy Committee. Said schedule included one short telephone conference per quarter to vote on the quarterly reporting, and one session per quarter to address regular and topical agenda items. In its meetings, the Committee also had the opportunity to engage with the auditor without the Executive Board present, which was an integral part of the meeting agenda. The Committee comprehensively prepared the resolutions of the Supervisory Board for all topics assigned to it, as described above. Regular agenda items included the course of business in the respective quarter, the accounting processes, the preparation of end-of-quarter closings, and the quarterly reports due for publication. In addition, the (new) Committee chairperson was in regular contact with the auditor. Other recurring meeting topics included the monitoring of SAP's risk management system, internal control system, and compliance system (including specific compliance issues, the status of corresponding SAP-internal investigations, and case-related collaboration with authorities), and cybersecurity. In its February 2022 meeting, the Committee prepared the Supervisory Board's resolutions on the financial statements of SAP SE and the Group for 2021 in the run-up to the Annual General Meeting of Shareholders, which were adopted at the audit meeting. Other material topics dealt with by the Committee beyond the regular meeting topics in its ordinary meetings and those described in the "Sustainability" section of this report included quarter-specific matters and the compensation system for SAP's Sales organization. Further, the Committee monitored the progress of selected lawsuits involving SAP. The Audit and Compliance Committee also received regular updates on activities relating to the change in auditor for SAP's financial statements and consolidated financial statements, particularly progress reports on the onboarding of the new auditor. In addition, the Committee continually monitored the quality of the current and future auditor and the management report. To this end – in addition to evaluating satisfaction surveys for the previous year's audit by the current auditor – the Committee obtained and referred to regular reports from the auditor on its internal quality assurance standards and to any material findings from internal quality audits, external quality controls, and peer reviews, and from any investigations conducted by the government or regulators into the auditor's audits. The Committee discussed the audit focus for 2022 with the auditor at its meeting in July. As reported in more detail below, the Committee also held two joint meetings with the Finance and Investment Committee in February and December 2022 to discuss the Group annual plan for 2022 and the preliminary Group annual plan for 2023. The joint meeting with the Technology and Strategy Committee in July focused on the results of the assessment by NIST (National Institute of Standards and Technology, a department of the U.S. Department of Commerce) and the progress of certain internal audits. The auditor attended all Audit and Compliance Committee meetings except for the joint meetings with the Finance and Investment Committee and the Technology and Strategy Committee, and reported in depth on its audit work and on its quarterly reviews of selected software and cloud agreements.

– The *Finance and Investment Committee* held six regular meetings and five extraordinary meetings in 2022, and outside these meetings it passed two resolutions by correspondence. It held a joint meeting with the Audit and Compliance Committee in February and again in December 2022, and a joint meeting with the Technology and Strategy Committee in December 2022 as described in more detail below. In an extraordinary meeting in January 2022, the Committee approved the acquisition of a minority interest in Icertis, a contract lifecycle management specialist based in the United States. It also discussed the planned acquisition of Taulia, an American working capital management firm, at length and ultimately resolved to recommend the acquisition to the Supervisory Board. In the joint meeting with the Audit and Compliance Committee in

February 2022, the members of both Committees discussed the annual budget for 2022 and voted in favor of recommending its approval to the Supervisory Board. At the Finance and Investment Committee meeting on the same day, the new head of the Investor Relations team introduced himself, provided an overview of the core topics in his remit, and presented his strategic concept. When it met in April, the Committee and the Executive Board discussed selected investor relations and capital market topics, strategic business plans for various product areas, plans for future collaboration with SAP partners, and potential divestments. The Executive Board also reported on the major investments planned and on its analysis of employee efficiency. During the Committee's first meeting in July, it deliberated on the sale of the Litmos business as described above. At its second meeting in July, the Committee dealt with Investor Relations matters and engaged in a detailed discussion about the efficiency of SAP's development organization. The Executive Board also presented its new strategy for investing in the venture capital sector in collaboration with the Sapphire Ventures team. After extensive consultation, the Committee resolved to recommend that the Supervisory Board approve the set-up of a new fund for direct investments totaling US$1.25 billion and a further venture capital fund for fund-of-funds investments totaling US$100 million. The Committee also resolved, by way of correspondence, to recommend the Supervisory Board's consent to a share buy-back program worth €500 million and approved the extension of existing bilateral bank loans. In the October meeting, the Executive Board updated the Committee on investor relations and treasury topics, explained its plans to streamline the portfolio, and presented its regular report on the success of the Company's recent acquisitions. Beyond this, the Committee and the Executive Board discussed management efficiency and competency, and examined process optimizations in the cloud. In addition, the Committee reviewed its own activities and the format of its meetings, with a view to good corporate governance. At its two extraordinary meetings held on December 12 and 13, 2022, the Committee was apprised of planned improvements to selected business areas and drafted a resolution to recommit funds previously dedicated in July 2022 for Sapphire Ventures fund-of funds activities. In December 2022, the Committee held a second joint meeting with the Audit and Compliance Committee, at which the Executive Board presented the preliminary Group annual plan for 2023. This meeting was held in preparation for the Supervisory Board meeting in February 2023, at which the full Supervisory Board resolved to approve the Group annual plan for 2023.

- The *Technology and Strategy Committee* held six meetings in 2022, which included one joint meeting with the Audit and Compliance Committee and one joint meeting with the Finance and Investment Committee. The Committee discussed the outlook for key technology trends in the software industry in the years to come and SAP's corporate and product strategies. The Executive Board explained SAP's midmarket and customer experience strategies to the Committee members at its February meeting, where the two bodies also discussed the specific requirements resulting from the rapid growth and expansion of medium-sized customers. In April, the Committee turned its attention to artificial intelligence and "data to value" – the act of deriving business value from data – placing particular focus on the integration of data sources in compliance with legal and regulatory requirements. In July 2022, the Executive Board updated the Committee on the strategic plans for process intelligence and automation and explained how SAP Signavio solutions would be used to expand SAP's opportunities in the business process optimization space. At the joint meeting with the Audit and Compliance Committee, also in July, the Committee was updated on progress in the areas of enterprise vulnerability management and asset management. When it met in October 2022, the Committee examined SAP's innovation strategy as regards business transformation, business network, and sustainability. At their joint meeting in December, the Technology and Strategy Committee and the Finance and Investment Committee deliberated on the efficiency of SAP's development organization and were given an overview of SAP's current development processes and tools by the Executive Board.
- The *People and Culture Committee* met five times in the reporting year. The focus of its February meeting was on strategic personnel planning as relate to the "the future of work" concept and the evolution of skills. The Committee was presented in this regard with a detailed overview of the past and expected demographic development of the SAP SE workforce, and discussed the skills and

expertise the Company would require of employees in the future. In addition, the global head of Diversity and Inclusion introduced herself to the Committee, following which the Committee looked at the career development of employees in expert functions and discussed the refining of SAP's leadership culture introduced the year before. Performance management was a key topic of the July meeting, where an initiative to promote appreciation and respect at the Company was presented. The Committee then reviewed the progress made in this initiative and the feedback received from employees in this connection at its October meeting, where it also looked at investments in headcount and the compensation budgets for 2023. The Committee held an extraordinary meeting in November where it and the Executive Board looked in-depth at the talent development process the Company was pursuing in the SAP S/4HANA area. The two bodies addressed three specific aspects in this regard: improving the quality of the recruitment process, training and upskilling staff, and promoting the performance culture at SAP.

– The *Nomination Committee* met four times in 2022. In February 2022, it deliberated on proposed successors for the departing Supervisory Board member Bernard Liautaud. Following corresponding interviews and careful evaluation of the competencies of all persons under consideration, it resolved the nomination of Jennifer Li as further candidate for election to the Supervisory Board by the Annual General Meeting on May 18, 2022. The Committee came to the conclusion that Jennifer Li had the best qualifications to succeed Bernard Liautaud and that her other mandates outside SAP would not prevent her from performing her duties as a member of the Supervisory Board and making valuable contributions to the work of the SAP Supervisory Board. The Committee also met on July 27, 2022, where it discussed succession planning on the Supervisory Board, particularly for the position of chairperson, and agreed that the search for suitable candidates should continue to be conducted both within SAP and outside the Company. As in the past, the Committee enlisted the help of a renowned personnel consulting firm for this purpose. In its meeting on October 27, 2022, the Committee members discussed the status of the candidate search and the initial results submitted to it by the consulting firm. At the Committee's meeting in December, the personnel consultant presented a short list of candidates, which the Committee discussed in depth before deliberating on the next steps in the search.

– The *Go-To-Market and Operations Committee* likewise met four times in the reporting year. At the February meeting, the Committee was informed of the cloud revenues generated in 2022 versus the year before, apprised of the current cloud backlog growth, and presented with the Executive Board's current strategy to accelerate growth in the cloud. In April, the Executive Board presented a new strategy for technology and sales that addressed how SAP would position its technologies in the market going forward and the role SAP Business Technology Platform would play in this. In July, the Committee was updated on SAP's competitive situation and, based on this information, discussed with the Executive Board what strategic decisions would result from this. The two bodies then deliberated on how SAP cloud solutions could be run more efficiently in key strategic business areas. The October meeting focused on the transformation of the Cloud Success Services (CSS) area, which had been triggered at the beginning of 2021. The core of this transformation was the merger of various user departments into one CSS unit that supported SAP's cloud portfolio. The Executive Board first explained how this measure was intended to ensure end-to-end customer relationships that focused on customer success and customer lifetime value. It then presented the Committee with the CSS targets and the Company's plans for expanding the organization further. The Committee also examined how SAP's partner ecosystem evolved with the shift to the cloud. The business update included a discussion about how SAP would react in the event of interruptions to its energy supply. The Executive Board explained to the Committee how SAP was currently protecting its data centers and for which scenarios the Company was preparing itself, including in the case of hyperscalers and their server systems, which would likewise be affected by energy bottlenecks.

The work of the committees and their regular reports to the full Supervisory Board ensured that we were kept fully informed of all matters covered by the committees and were able to discuss them thoroughly.

Conflicts of Interest

Members of the Supervisory Board and of the Executive Board had no conflicts of interest that recommendations E.1 and E.2 of the GCGC require to be disclosed to the Supervisory Board. Insofar as Supervisory Board members hold executive positions in companies or have material equity in companies that currently have business dealings with SAP, we do not see any impairment of their independence. The scope of these transactions is relatively small and, moreover, takes place at arm's length.

Training and Professional Development

The members of the Supervisory Board were once again offered various training and professional development opportunities throughout the year, with appropriate support from the Company. On-boarding sessions and leaflets are available for new Supervisory Board members to familiarize themselves with their tasks and responsibilities when they assume office. Where it made sense, presentations and training offerings were recorded and placed on a specially configured training platform to enable the remaining Supervisory Board members to take part in them as well. The members of the Audit and Compliance Committee were invited to short seminars in April 2022 on "New EU reporting requirements for sustainability" (Corporate Sustainability Reporting Directive), and on the "OECD/G20 New World Tax Order for Digital Business" (a basic approach adopted by OECD/G20 to reform international business taxation). An external expert attending the Supervisory Board's meeting in October provided a general overview of the importance of sustainability for companies and the expectation of investors where this was concerned. In December 2022, external experts held an information session for members of the Supervisory Board on the future legal framework in the area of ESG and its relevance for the work of the Supervisory Board.

SAP SE and Consolidated Financial Reports for 2022

KPMG AG Wirtschaftsprüfungsgesellschaft, Berlin (KPMG) audited the SAP SE and consolidated financial reports for 2022. The Annual General Meeting of Shareholders elected KPMG as the SAP SE and SAP Group auditor on May 18, 2022. The Supervisory Board proposed the appointment of KPMG on the recommendation of the Audit and Compliance Committee. Prior to the proposed resolution being put to the Annual General Meeting of Shareholders, KPMG had confirmed to the chairperson of the Supervisory Board and the Audit and Compliance Committee that circumstances did not exist that might prejudice or raise any doubt concerning its independence as the Company's auditor. In that connection, KPMG informed us of the volume of the services that were not part of the audit which it had either provided to the Group in the past year or was engaged to provide in the year to come. The Supervisory Board has agreed with KPMG that the auditor should report to the Supervisory Board and record in the auditor's report any fact found during the audit that is inconsistent with the declaration given by the Executive Board and the Supervisory Board concerning implementation of the German Corporate Governance Code. KPMG examined the SAP SE financial statements prepared in accordance with the German Commercial Code, the consolidated financial statements prepared in accordance with International Financial Reporting Standards (IFRSs) as required by the German Commercial Code, section 315e, and the combined SAP Group and SAP SE management report prepared in accordance with the German Commercial Code, and certified them without qualification. The auditor thus confirmed that, in its opinion and based on its audit in accordance with the applicable accounting principles, the SAP SE and consolidated financial statements give a true and fair view of the net assets, financial position, and results of operations of SAP SE and the SAP Group. The auditor also confirmed that the combined SAP SE and SAP Group management report is consistent with the corresponding financial statements and as a whole gives a suitable view of the position of SAP SE and the SAP Group and of foreseeable opportunities and risks. In accordance with section 317 (3a) of the German Commercial Code, the auditor also examined and confirmed that the renderings of the financial statements, the management report, the consolidated financial statements, and the combined management report contained in the files submitted on an electronic data carrier, which can be accessed by the issuer on the secure client portal, and prepared for the purposes of disclosure comply in all material respects with the requirements of section 328 (1) of the German Commercial Code regarding the electronic reporting format ("ESEF format"). KPMG had completed its audit of SAP's internal control over financial reporting and certified without qualification that it complies with the applicable U.S. standards. The auditor stated in its opinion that it considers SAP's internal controls with respect to the consolidated financial statements to be effective in all material respects. Additionally, it provided assurance on the non-financial declaration and the disclosures contained therein on the topics identified as material – namely, the environment, employees, human rights, corruption and bribery, customer loyalty, and data privacy and data security – in the combined management report, and on the separate review of the compensation report and selected qualitative and quantitative sustainability disclosures outside of the financial statements and management report. All Audit and Compliance Committee members and Supervisory Board members received – initially in the form of drafts that were identical to the final documents – the documents concerning the financial statements mentioned above, the audit reports prepared by KPMG, and the Executive Board's proposal concerning the appropriation of retained earnings in good time. On February 22, 2023, the Executive Board prepared the financial accounts of SAP SE and the Group for 2022, comprising the SAP SE financial statements, the consolidated financial statements, and the combined management report, and submitted them without delay to the Supervisory Board.

The Executive Board explained the financial statements of SAP SE and the SAP Group and its proposal concerning the appropriation of retained earnings at the meeting of the Audit and Compliance Committee on February 22, 2023 (based on the drafts identical to the final documents) and at the meeting of the Supervisory Board on February 22, 2023. Members of the Executive Board answered questions from the Committee and the Supervisory Board. At the Audit and Compliance Committee meeting, they also explained the compensation report and the Annual Report on Form 20-F prepared in accordance with the applicable U.S. standards.

After the Executive Board had explained them, the Audit and Compliance Committee and the Supervisory Board reviewed the financial statement documents (based on drafts identical to the final documents), taking KPMG's audit reports (or the drafts identical to the final documents) into account. The Audit and Compliance Committee then passed the compensation report on to the Supervisory Board for release. The representative of the auditor who attended presented full reports on the audit and the results of the audit to the Audit and Compliance Committee and Supervisory Board meetings and explained its audit reports (or final drafts thereof). The auditor also reported that it had not identified any material weaknesses in SAP's internal control and risk-management systems for financial reporting. Both the Audit and Compliance Committee and the Supervisory Board asked detailed questions about the form, scope, and results of the audit. The Audit and Compliance Committee reported to the Supervisory Board on its own review of the financial statements of SAP SE and the SAP Group, its discussions with the Executive Board and with the auditor, and its supervision of the financial reporting process. It confirmed that, as part of its supervisory work, it had addressed the SAP Group's internal control, risk management, and internal auditing systems, and found the systems to be effective.

The Committee also reported that KPMG had told it that no circumstances had arisen that might give cause for concern about KPMG's impartiality, and informed us about the services KPMG had provided that were not part of the audit. The Committee reported that it had examined the auditor's independence, taking the non-audit services it had rendered into consideration, and stated that, in the Committee's opinion, the auditor possessed the required degree of independence and professional qualification.

The Audit and Compliance Committee and the Supervisory Board satisfied themselves that KPMG had conducted the audit properly. In particular, they concluded that both the audit reports and the audit itself fulfilled the legal requirements. On the basis of the report and the Audit and Compliance Committee's recommendation, the Supervisory Board approved the results of the audit and, since there were no findings from our own examination, we gave our consent to the SAP SE financial statements, the consolidated financial statements, the combined Group management report, and adopted the compensation report pursuant to the German Stock Corporation Act, section 162. The financial statements and combined management report were thus formally adopted upon approval by the Supervisory Board. The Supervisory Board's opinion of the Company and the Group coincided with that of the Executive Board as set out in the combined management report. The Supervisory Board considered the proposal presented by the Executive Board concerning the appropriation of retained earnings. We had regard to the requirements of dividends policy, the effects on the liquidity of SAP SE and the SAP Group, and the interests of the shareholders. We also discussed these matters with the auditor. We then endorsed the Executive Board's proposal concerning the appropriation of retained earnings, in accordance with the Audit and Compliance Committee's recommendation. The corporate governance statement pursuant to the German Commercial Code, sections 315d and 289f was approved for publication by the Supervisory Board by way of correspondence vote prior to the meeting to discuss the financial statements. Finally, we adopted this present Report.

Changes on the Executive Board and Supervisory Board in 2022

There were no changes on our Executive Board in 2022. The appointment of the new CFO as described above will only come into effect in 2023.

The Supervisory Board bade farewell in 2022 to Bernard Liautaud who, after 14 years as a member, resigned from his position with effect from the closing of the Annual General Meeting of Shareholders on May 18, 2022. The Supervisory Board thanks Bernard Liautaud for his commitment to SAP. On May 18, 2022, the Annual General Meeting of Shareholders elected Jennifer Li to the Supervisory Board as his successor.

In addition to the ongoing COVID-19 pandemic, we now face major challenges from the war in Ukraine and its humanitarian, geopolitical, and economic implications. The Supervisory Board thanks the members of the Executive Board and all SAP employees for their tireless commitment to SAP under these extraordinary circumstances.

For the Supervisory Board

Professor Hasso Plattner

(Chairperson)

Independent Assurance Practitioner's Report

To the Supervisory Board of SAP SE, Walldorf

We have performed a limited assurance engagement on the non-financial statement of SAP SE (further "Company" or "SAP") and on the non-financial statement of the parent company that is combined with it, which are published in the Management Report, (further "combined non-financial statement") for the period from January 1 to December 31, 2022.

Responsibilities of Management

Management of the company is responsible for the preparation of the combined non-financial statement in accordance with Sections 315c in conjunction with 289c to 289e HGB ["Handelsgesetzbuch": German Commercial Code] and Article 8 of REGULATION (EU) 2020/852 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of June 18, 2020 on establishing a framework to facilitate sustainable investment and amending Regulation (EU) 2019/2088 (hereinafter the "EU Taxonomy Regulation") and the Delegated Acts adopted thereunder, as well as for making their own interpretation of the wording and terms contained in the EU Taxonomy Regulation and the delegated acts adopted thereunder as set out in section "Sustainable Finance: EU Taxonomy Disclosures" of the combined non-financial statement.

This responsibility includes the selection and application of appropriate non-financial reporting methods and making assumptions and estimates about individual non-financial disclosures of the group that are reasonable in the circumstances. Furthermore, management is responsible for such internal control as they consider necessary to enable the preparation of a combined non-financial statement that is free from material misstatement, whether due to fraud or error.

The EU Taxonomy Regulation and the Delegated Acts issued thereunder contain wording and terms that are still subject to considerable interpretation uncertainties and for which clarifications have not yet been published in every case. Therefore, management has disclosed their interpretation of the EU Taxonomy Regulation and the Delegated Acts adopted thereunder in section "Sustainable Finance: EU Taxonomy Disclosures" of the combined non-financial statement. They are responsible for the defensibility of this interpretation. Due to the immanent risk that indeterminate legal terms may be interpreted differently, the legal conformity of the interpretation is subject to uncertainties.

Independence and Quality Assurance of the Assurance Practitioner's firm

We have complied with the independence and quality assurance requirements set out in the national legal provisions and professional pronouncements, in particular the Professional Code for German Public Auditors and Chartered Accountants (in Germany) and the quality assurance standard of the German Institute of Public Auditors (Institut der Wirtschaftsprüfer, IDW) regarding quality assurance requirements in audit practice (IDW QS 1).

Responsibility of the Assurance Practitioner

Our responsibility is to express a conclusion with limited assurance on the combined non-financial statement based on our assurance engagement.

We conducted our assurance engagement in accordance with International Standard on Assurance Engagements (ISAE) 3000 (Revised): "Assurance Engagements other than Audits or Reviews of

Historical Financial Information" issued by the IAASB. This standard requires that we plan and perform the assurance engagement to obtain limited assurance about whether any matters have come to our attention that cause us to believe that the company's non-financial statement, is not prepared, in all material respects, in accordance with Sections 315c in conjunction with 289c to 289e HGB and the EU Taxonomy Regulation and the Delegated Acts issued thereunder as well as the interpretation by management disclosed in section "Sustainable Finance: EU Taxonomy Disclosures" of the combined non-financial statement. We do not, however, issue a separate conclusion for each disclosure.

In a limited assurance engagement, the procedures performed are less extensive than in a reasonable assurance engagement, and accordingly, a substantially lower level of assurance is obtained. The selection of the assurance procedures is subject to the professional judgment of the assurance practitioner.

In the course of our assurance engagement we have, among other things, performed the following assurance procedures and other activities:

- Interviewing employees responsible for the materiality analysis at group level in order to obtain an understanding on the approach for identifying key issues and related reporting limits of SAP,
- Carrying out a risk assessment, inclusive of media analysis, on relevant information on sustainability performance of SAP in the reporting period,
- Assessing the design and implementation of systems and processes for identifying, handling, and monitoring information on environmental, employee and social matters, human rights and combating corruption and bribery, including the consolidation of data,
- Interviewing staff on group level, who are responsible for the disclosures on concepts, due diligence processes, results and risks, the performance of internal control activities and the consolidation of the disclosures,
- Inspecting selected internal and external documents,
- Analytically assessing the data and trends of the quantitative information, which is reported on group level of all locations,
- Evaluating the local data collection, validation, and reporting processes as well as the reliability of the reported data by means of a sampling survey at two locations,
- Interviewing of responsible staff on group level to obtain an understanding of the approach to identify relevant economic activities in accordance with the EU taxonomy,
- Evaluating the design and implementation of systems and procedures for identifying, processing, and monitoring information on turnover, capital expenditures and operating expenditures for the taxonomy-relevant economic activities for the first two environmental objectives climate change mitigation and climate change adaptation,
- Evaluating the data collection, validation, and reporting processes, as well as the reliability of the reported data for the taxonomy-aligned economic activities in conjunction with the assessment of the technical evaluation criteria for the substantial contribution, the fulfilment of the DNSH-criteria and the documentation of the minimum safeguard,
- Assessment of the overall presentation of the disclosures.

In determining the disclosures in accordance with Article 8 of the EU Taxonomy Regulation, management is required to interpret undefined legal terms. Due to the immanent risk that undefined legal terms may be interpreted differently, the legal conformity of their interpretation and, accordingly, our assurance engagement thereon are subject to uncertainties.

Assurance Opinion

Based on the assurance procedures performed and the evidence obtained, nothing has come to our attention that causes us to believe that the combined non-financial statement of SAP SE, Walldorf for the period from January 1 to December 31, 2022 has not been prepared, in all material respects, in accordance with Sections 315c in conjunction with 289c to 289e HGB and the EU Taxonomy Regulation and the Delegated Acts issued thereunder as well as the interpretation by management as disclosed in section “Sustainable Finance: EU Taxonomy Disclosures” of the combined non-financial statement.

Restriction of Use

This assurance report is solely addressed to SAP SE, Walldorf.

Our assignment for SAP SE, Walldorf and professional liability is governed by the General Engagement Terms for Wirtschaftsprüfer (German Public Auditors) and Wirtschaftsprüfungs-gesellschaften (German Public Audit Firms) (Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften) in the version dated January 1, 2017 (*https://www.kpmg.de/bescheinigungen/lib/aab_english.pdf*). By reading and using the information contained in this assurance report, each recipient confirms having taken note of provisions of the General Engagement Terms (including the limitation of our liability for negligence to EUR 4 million as stipulated in No. 9) and accepts the validity of the attached General Engagement Terms with respect to us.

Mannheim, den 22. Februar 2023

KPMG AG
Wirtschaftsprüfungsgesellschaft

Beyer
Wirtschaftsprüfer
[German Public Auditor]

Wiegand
Wirtschaftsprüfer
[German Public Auditor]

Non-Financial Statement Including Information on Sustainable Activities

With this section and the information referenced to in this section, SAP SE fulfills its duty to produce a non-financial statement (NFS) for the holding company, pursuant to section 289b–e of the German Commercial Code (HGB), and a non-financial group statement, pursuant to section 315b–c in conjunction with section 289c–e of the German Commercial Code (HGB), in the form of a combined non-financial statement. The relevant non-financial matters are referenced in the table below and can be found in the relevant sections of our combined management report.

Additionally, following Article 8 of Regulation 2020/852 of the European Parliament and of the Council of the European Union (EU Taxonomy), we have included information on how and to what extent SAP's activities are associated with economic activities that qualify as environmentally sustainable under this regulation.

For more information, see the *EU Taxonomy Disclosures* subsection.

Reporting Framework

The social and environmental data and information included in the SAP Integrated Report have been prepared in accordance with the Global Reporting Initiative (GRI) Standards.

Business Model

SAP's business model is described in the *Strategy and Business Model* section of the combined management report. Good governance is a prerequisite for continued success and is described throughout the combined management report. Therefore, we did not include governance as an individual material topic in our materiality assessment and our non-financial statement.

Non-Financial Disclosures in SAP's Combined Management Report

SAP determines which non-financial information has to be disclosed based on a materiality analysis we perform using internal and external input. For more information, see *Materiality* in the *Further Information about Economic, Environmental, and Social Performance* section in our SAP Integrated Report.

The individual non-financial aspects to be covered by the non-financial statement are addressed in the following sections of our combined management report if material. No material risks according to section 289c (3) sentence numbers 3 and 4 HGB have been identified.

	Due Diligence; Policies and Guidelines (Concepts)	Measures and Results, Including KPIs Relevant for Steering and Compensation	References to Financial Statements and Notes
Environmental Matters	*Energy and Emissions: Vision and Strategy; Due Diligence*	**KPI: Net carbon emissions** *Energy and Emissions: How We Measure and Manage Our Performance* *Performance Management System* *Strategy and Business Model: Measuring Our Success* *Expected Developments and Opportunities*	
Employee Matters	*Employees: Vision and Strategy; Due Diligence* *Expected Developments and Opportunities: Opportunities from Our Employees*	**KPI: Employee Engagement Index** *Employees: How We Measure and Manage Our Performance* *Performance Management System* *Strategy and Business Model: Measuring Our Success* *Financial Performance: Review and Analysis* *Expected Developments and Opportunities*	*Notes to the Consolidated Financial Statements, Section B – Employees*
Human Rights	*Human Rights: Vision and Strategy; Due Diligence*	*Human Rights: How We Measure and Manage Our Performance*	
Anti-Corruption and Bribery Matters	*Business Conduct: Vision and Strategy; Due Diligence*	*Business Conduct: How We Measure and Manage Our Performance*	*Notes to the Consolidated Financial Statements, Note (G.3)*
Customer Matters	*Customers: Vision and Strategy; Due Diligence*	**KPI: Customer Net Promoter Score, Revenues** *Customers: How We Measure and Manage Our Performance* *Performance Management System* *Strategy and Business Model: Measuring Our Success* *Financial Performance: Review and Analysis* *Expected Developments and Opportunities*	*Notes to the Consolidated Financial Statements, Section A – Customers* *Consolidated Income Statements – Revenue*
Security, Data Protection, and Privacy	*Security, Data Protection, and Privacy: Vision and Strategy; Due Diligence for Security Topics; Due Diligence for Data Protection Topics*	*Security, Data Protection, and Privacy: How We Measure and Manage Our Performance*	

Sustainable Finance: EU Taxonomy Disclosures

Assessment of Eligibility and Alignment

In 2022, as in 2021, we identified the activity “8.1 Data processing, hosting, and related activities” as turnover-relevant Taxonomy-eligible economic activity contributing to climate change mitigation.

The criteria for Taxonomy-alignment of activity 8.1 were not met in fiscal year 2022. We expect that the transition from Taxonomy-eligible to Taxonomy-aligned will progress over the next few years corresponding to the fulfillment of the technical screening criteria. For instance, according to the EU Taxonomy regulation, refrigerants used in data centers need to conform with a certain level of global warming potential. The refrigerants employed by SAP do not meet this threshold yet. An immediate exchange would lead to additional toxic waste and costs. Therefore, SAP intends to replace the refrigerants according to our regular maintenance schedule over the course of the next few years. Also, SAP’s data center co-locations and hyperscalers are not yet in full alignment with the criteria set out in the Taxonomy regulation. Together with our providers, we are evaluating options to reach Taxonomy alignment over the next few years.

Furthermore, SAP assessed whether any capital and operational expenditures had been incurred related to the purchase of output from Taxonomy-eligible or Taxonomy-aligned economic activities. In 2022, SAP capitalized an amount of €151 million relating to the purchase of vehicles. While a portion of these expenses, specifically relating to the purchase of electric vehicles, may be Taxonomy-aligned, we could not obtain the necessary verification from our suppliers. Therefore, SAP classified the full amount as Taxonomy-eligible (purchases of output of the activity “3.3 Manufacture of low carbon technologies for transport" contributing to climate change mitigation) but not as Taxonomy-aligned.

In single locations, SAP operates combined heat/cool and power generation facilities using fossil gaseous fuels. However, the associated potential Taxonomy-eligible and aligned revenues, capital expenditures, and operational expenditures are negligible. No further activities for nuclear or gas are applicable.

SAP also evaluated whether activity “7.2 Renovation of existing buildings” is relevant for SAP. While SAP regularly conducts renovation measures, for 2022 renovation expenses were considered immaterial compared to SAP’s total investments and were not clearly distinguishable from other related but non-eligible costs. We therefore concluded that activity 7.2 is not relevant for 2022.

Business Conduct

Vision and Strategy

In an increasingly complex business environment, making the right decisions and abiding by ethical choices has never been more important. As a company operating in numerous countries across the globe, SAP is required to adhere to strict international legislation that defines acceptable business conduct and practices.

At SAP, we also expect our business practices to not only meet international rules and legal requirements, but to adhere to our internal high standards of ethics and integrity. We understand that our customers expect this as well. SAP's reputation for doing business the right way is one of our most important assets. By striving to make ethical choices and acting with integrity, we aim to continue to grow SAP in a way that meets both our own and our customers' high ethical expectations.

Due Diligence

Governance

The **Office of Ethics and Compliance** (OEC) contributes to SAP's success by providing trusted advice to SAP managers, leaders, and employees across the entire business. The OEC strives to advance SAP's business goals by promoting a strong culture of integrity and helping SAP to "Win the Right Way."

In 2022, our aim to maintain a robust compliance program, based on our corporate values and voluntary commitments, as well as international standards, continued. The OEC team grew for the fifth consecutive year, from 142 employees in 2021 to 154 employees in 2022. The group chief compliance officer (GCCO) continues to report directly to the group CEO.

At SAP, ethical behavior is an integral part of our cultural values that can influence our daily decision-making at every level of the business and in every market. To help nurture this environment, the OEC's various teams continually address compliance challenges and improve policies, guidelines, systems, and measures related to their implementation.

The OEC has field compliance officers across the globe, in both high- and low-risk jurisdictions. Field compliance officers are often the first point of contact for the business when compliance matters arise. In those high-risk countries in which the OEC is not physically represented and where there might be local language needs, the OEC operates a network of compliance stewards drawn largely from either our legal, finance, or human resources (HR) departments. Compliance stewards support the OEC's field compliance officers by offering advice on specific and straightforward compliance questions; they work alongside our global network of compliance ambassadors (drawn from all areas of the Company) to amplify compliance messages and provide a further link for local employees to the relevant field compliance officer.

Compliance matters are regularly discussed with Executive and Supervisory Board members at quarterly Audit and Compliance Committee meetings as well as during regular touchpoints with Executive Board and Supervisory Board members. Compliance matters are also discussed by the GCCO in quarterly Global Compliance Governance Committee meetings. Participants at these meetings include members of Global Finance, Customer Success, Global Communications, Global Security, and Global Risks & Assurance Services (GR&AS).

Where appropriate, and in response to identified compliance concerns, the OEC engages external counsel and forensic consulting resources to perform corruption risk assessments of high-risk market units or other related supporting tasks. This may include, for example, device collections or comprehensive root cause analyses for identified risks.

Outside SAP, the OEC regularly exchanges ideas and best practices for compliance processes with relevant peers in the software industry and beyond. In Germany, the OEC participates in the annual DAX Chief Compliance Officer Round Table. SAP is also a Corporate Member of the Association of Certified Fraud Examiners (ACFE), and the GCCO is also a member of the European Chief Compliance Officers Forum (ECCIOF) and the UN Global Compact's Think Lab focused on transformational governance.

Guidelines and Policies

In 2022, a revised and updated version of the *Code of Ethics and Business Conduct (CoEBC)*[55] was rolled out throughout the Company and made available outside of SAP. It replaced multiple existing local Codes of Business Conduct and provides, in a single document, the primary ethical and legal framework within which SAP conducts business and remains on course for success. The revised CoEBC is available in 22 languages.

SAP also expects all partners and suppliers to commit to meeting our high standards of integrity and sustainability. For this reason, we have the SAP Partner Code of Conduct and the SAP Supplier Code of Conduct in place so that partners and suppliers understand what is expected of them.

How We Measure and Manage Our Performance

Enforcing Policies and Guidelines

All employees are bound by the CoEBC; they are required to acknowledge its contents and confirm their commitment to it on an annual basis. In 2022, we continued to monitor employee certification of the CoEBC for employees worldwide, recording a 99.9% certification rate for permanent SAP employees (excluding those from acquired companies).

Communication

The OEC's dedicated communications team consistently distributes integrity-related communications, at all levels of the Company – including to senior leaders, managers, and employees, as well as topic-related content for SAP partners. Executive Board members and senior leaders regularly host all-hands meetings as well as leadership team meetings and smaller gatherings, which include integrity-focused topics, demonstrating their dedication to ethical business.

Quarterly OEC newsletters provide all SAP employees with information on a range of compliance-related topics. Additionally, a quarterly newsletter with a focus on leadership and management topics is sent specifically to executive and senior management.

Employees can use the SAP One employee portal at any time to access all global policies, guidelines, and additional information. The SAP Compliance mobile app[56] also provides convenient, ongoing access to compliance-related information. Externally, our Web site sap.com features information and guidance for our external stakeholders.

All Board areas have re-committed their support for OEC's Compliance Ambassador Program and have nominated employees to participate in it. In 2022, a fifth cohort was introduced, bringing the number of participants from over 500 in 2021 to over 1,100 in 2022. The program is designed to give employees a further point of contact in the business when compliance matters arise. Ambassadors participate in an extensive curriculum of monthly on-boarding sessions over an 18-month period. They are expected to cascade and transfer information on the importance of compliance and ethics throughout their teams and lines of business.

[55] Link leads to information that was neither part of the statutory audit nor the independent limited assurance engagement performed by our external auditor.

[56] The SAP Compliance Mobile App is only available on Company-issued Apple devices; Apple devices represent 90% of devices issued.

Training Offerings

Our training programs cover topics such as anticorruption and antibribery, conflicts of interest, governance for customer commitments, working with public sector customers, and compliant partner engagement.

In addition to four mandatory online training courses for all SAP employees,[57] a further two mandatory online training courses were launched in 2022 for all employees in the Customer Success Board area. The completion rate for these exceeded 99.9%. A new Ethical Leadership workshop was also delivered live to all People Managers across the Company. The global completion rate for this workshop was 99%.

Despite continuing restrictions caused as a result of the COVID-19 pandemic, field compliance officers continued to hold training sessions – largely virtually – for employees across the organization, from customer-facing staff to individuals in supporting roles, such as corporate affairs and marketing.

Compliance Processes

The OEC also evaluates SAP's third-party service providers to assess whether SAP's compliance standards are met. New suppliers and third parties seeking a partnership with SAP are scrutinized according to a risk-based compliance due diligence process, which is repeated every two to five years thereafter. Supplier and partner relationships are formally defined in contracts that outline their obligation to abide by SAP's compliance requirements. In almost all cases, these include a "right to audit" clause. The OEC also has a team dedicated to conducting compliance audits of partners and suppliers to assess adherence to SAP's requirements and to identify and address compliance risks.

The OEC's Compliance Monitoring & Analysis (CMA) team monitors the effectiveness of SAP's compliance processes and controls through regular testing of high-risk transactions, identified using a data analytics tool developed with PricewaterhouseCoopers GmbH (PwC) and through manual sampling. The CMA team also analyzes findings from investigations and partner audit reports to identify potential enterprise-wide process deficiencies and patterns of misconduct that indicate a compliance risk. The team then conducts root cause analyses on the highest-risk topics and recommends remediation actions to mitigate the risks.

Speak Out at SAP

Speak Out at SAP is SAP's independently managed whistleblower reporting tool, through which any matters or concerns can be reported easily, and, if desired, anonymously. The tool is available 24 hours a day, seven days a week, both internally to SAP employees and externally to concerned parties, including customers, suppliers, and partners.

Reports may be submitted either directly by the reporter through the Internet-based portal, or by phone, with local language support across the globe in order to maximize accessibility for reporters. In all cases, SAP continues to maintain a strict non-retaliation policy.

Compared with the previous whistleblower reporting tool, we observed a substantial increase in the number of concerns reported through Speak Out at SAP since the tool's launch in 2021. Within this increase, a number of the concerns raised came from external parties, such as partners, customers, and suppliers.

Beyond Speak Out at SAP, we provide further reporting channels, including an internal ticketing system, a postal address for written submissions, as well as local contact persons worldwide.

Investigating Misconduct

The OEC's investigations team is comprised of dedicated investigators who probe allegations of misconduct within the OEC's area of responsibility. Where appropriate, the OEC engages the assistance of an external law firm when examining conduct that may violate SAP's policies and

[57] Excludes employees on parental leave, long-term sick leave, sabbaticals, and on early retirement. Training last assigned in 2021 with biennial frequency.

procedures or applicable laws. When misconduct is substantiated, SAP takes proportionate disciplinary action.

For more information about the material allegations currently being investigated by the OEC, see the Notes to the Consolidated Financial Statements, *Note (G.3).*

Related Risks for SAP

The actions and processes to address risks in business conduct are described above. No material risks were identified regarding the non-financial risk assessment. For financial risks, see also *Ethical Behavior* in the *Risk Management and Risks* section.

Audit Scope

The content of the *Business Conduct* section was not subject to the statutory audit of the combined group management report. However, our external auditor performed an independent limited assurance engagement for the content of this section.

Risk Management and Risks

Our Risk Management

Internal Control and Risk Management Systems

As a global company, SAP is exposed to a broad range of risks across our business operations. Consequently, our Executive Board has established comprehensive internal control and risk management structures that enable us to identify and analyze risks early and take appropriate action. Our internal control and risk management systems are designed to identify potential events that could negatively impact the Company and to provide reasonable assurance regarding the operating effectiveness of our internal controls over our financial reporting.

These systems comprise numerous control mechanisms and are an essential element of our corporate decision-making process; they are therefore implemented across the entire Group as an integral part of SAP's business processes. We have adopted an integrated internal control and risk management approach to help maintain appropriate and effective global risk management while also enabling us to aggregate risks and report on them transparently.

Appropriateness and Effectiveness of SAP's Entire Internal Control and Risk Management System[62]

We have a governance model in place across the internal control and risk management systems, as well as a central software solution to store, maintain, and report all risk-relevant information. In the *Business Conduct* section of our combined management report, we describe in more detail the governance structure as well as the measures and guidelines SAP has implemented to ensure compliance not only with international rules and legal requirements but also with our internal standards of ethics and integrity. Furthermore, SAP monitors risks relating to material sustainability matters. Material non-financial topics are listed in the section *Non-Financial Statement Including Information on Sustainable Activities.* The governance model, policies, and guidelines as well as the control measures we have implemented relative to these topics are described in the respective chapters in this combined management report. SAP constantly reviews and adjusts its entire internal control and risk management system as well as the policies and guidelines we have implemented regarding the material sustainability topics. We considered the results from external audits, such as the audit of our internal control system for financial reporting and early risk detection system conducted by our auditor KPMG, as well as internal sources, such as audit reports from our Global Risk & Assurance Services (GR&AS) team, to evaluate the effectiveness of our internal control and risk management systems. If issues are identified, SAP takes remedial action. While the non-financial internal control system has not yet reached the same maturity level as the financial internal control system, no material indication has come to our attention that SAP's entire internal control and risk management system is not appropriate or effective.

Legal and Regulatory Requirements

Due to our public listings in both Germany and the United States, we are subject to both German and U.S. regulatory requirements that relate to internal controls and risk management over financial reporting, such as provisions in the German Stock Corporation Act, section 91 (2), the U.S. Sarbanes-Oxley Act (SOX) of 2002, specifically sections 302 and 404, and the German Corporate Governance Code. Hence, our Executive Board has established an early warning system (risk management system) to enable compliance with applicable regulations.

---

[62] The appropriateness and effectiveness of SAP's entire internal control and risk management system, except for the internal control system for financial reporting and early risk detection system, was neither part of the statutory audit nor the independent limited assurance engagement performed by our external auditor.

Risk Management Policy and Framework

The risk management policy issued by our Executive Board governs how we manage risk in line with the Company's risk appetite and defines a methodology that is applied uniformly across all parts of the Group.

Risk Management Pillars

Our risk management system is based on the framework published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) entitled "Enterprise Risk Management – Integrating with Strategy and Performance." Updated in 2017, this framework is built on four pillars, namely: a global risk management governance framework, a dedicated risk management policy, a global risk management organization, and a standardized risk management methodology.

In accordance with the COSO framework, SAP's enterprise risk management covers risks in the areas of strategy, operations, finance, and compliance (the latter also covering ethical behavior, corporate governance, and sustainability).

Our Global Risk Management Governance Framework

The risk management governance framework at SAP represents a comprehensive system of approaches and processes to ensure control through a clearly structured risk management system and a supporting risk culture. The risk culture is considered the basis of SAP's risk management system. Risk culture at SAP comprises a system of values, beliefs, knowledge, attitudes, and understanding concerning risks and risk management as part of our corporate culture. To support and continuously foster SAP's risk culture, we conduct risk activities for the entire SAP organization such as mandatory training in ethical behavior, code of conduct, and risk management.

Our Executive Board is responsible for ensuring the effectiveness of the internal control system and our risk management system. The effectiveness of both systems and their implementation in the different Board areas is monitored by each Executive Board member. The Audit and Compliance Committee of the Supervisory Board regularly monitors the effectiveness of SAP's internal control and risk management systems. Our GR&AS organization regularly provides a status update on the internal control and the risk management systems to the Audit and Compliance Committee of the Supervisory Board. Every year, SAP's external auditors assess whether the SAP Group early-warning system for risk detection is adequate to identify risks that might endanger our ability to continue as a going concern. Additional assurance is obtained through the external audit of the effectiveness of our system of internal controls over financial reporting.

Our Global Risk Management Policy

The risk management policy is reviewed annually and stipulates responsibilities for conducting risk management activities and defines reporting and monitoring structures. Our global SAP risk management policy clearly states that each employee is responsible for active engagement in the risk management process as well as for the continuous identification of risks, based upon clear rules of engagement in adherence to the policy. The risk management system primarily analyzes risks. Opportunities are assessed or analyzed where it is deemed appropriate.

Our Global Risk Management Organization

Our global risk management organization is responsible for the implementation of a Group-wide effective risk management system. Furthermore, GR&AS is responsible for the regular maintenance and implementation of our risk management policy, as well as the standardized internal and external risk reporting.

All GR&AS risk managers, working with assigned risk contacts in the relevant business units, identify and assess risks associated with material business operations and monitor the implementation and effectiveness of the measures chosen to mitigate risks.

Further financial risk management activities are performed for example by our Global Treasury and Global Tax departments. General legal risks are managed by the Global Legal department. Sanction and embargo-related risks are managed by the Export Control department, harassment and other HR-related issues by our Global Labor & Employee Relations Office, security-related risks by our SAP Global Security Office, and IP risks by our Global IP Office. Non-financial risks are reported jointly by GR&AS and SAP's Sustainability organization. All risks are tracked, maintained, and reported within SAP's risk management system.

During the merger and acquisition and post-merger integration phase, newly acquired companies are subject to risk management performed by our Corporate Development Mergers and Acquisitions (M&A) function. Furthermore, for as long as the newly acquired companies are not integrated, existing risk management structures are maintained or enhanced within the acquired companies for the purposes of compliance with legal requirements.

SAP reviews the exposure of its business units to potential compliance risks on a regular basis. Quantitative and qualitative internal data as well as external information, such as Transparency International's Corruption Perceptions Index, are considered in our wider compliance risk analysis. Based on this information, we perform a detailed assessment for all SAP-relevant high-risk countries and derive local and global mitigations.

The GR&AS unit, led by the Chief Risk Officer (who also acts as Chief Audit Executive), combines internal audit, SOX, internal controls, and global governance, risk, and compliance activities. The Chief Risk Officer reports to our Group CFO and is responsible for SAP's internal control and risk management programs. Additionally, the Office of Ethics & Compliance (OEC) continually addresses compliance challenges and improves policies, guidelines, systems, and measures related to their implementation. For more information about SAP's governance structure in the area of compliance, see section *Business Conduct*.

Internal Control and Risk Management System for Financial Reporting

The purpose of our system of internal control over financial reporting is to provide reasonable assurance that our financial reporting is reliable and compliant with generally accepted accounting principles. Because of the inherent limitations of internal controls over financial reporting, this system might not prevent or bring to light all potential misstatements in our financial statements.

Our internal control system consists of the internal control and risk management system for financial reporting (ICRMSFR), which also covers the broader business environment and is part of the overall risk management system of SAP. Using the current COSO Internal Control – Integrated Framework of 2013, we have defined and implemented internal controls along the value chain on a process and subprocess level to ensure that sound business objectives are set in line with the organization's strategic, operational, financial, and compliance goals.

SAP's ICRMSFR is based on our Group-wide risk management methodology. It includes organizational, control, and monitoring structures designed to ensure that data and information concerning our business is collected, compiled, and analyzed in accordance with applicable laws and properly reflected in our IFRS Consolidated Financial Statements.

Our ICRMSFR also includes policies, procedures, and measures designed to ensure compliance of SAP's financial reports with applicable laws and standards. We analyze new statutes, standards, and other pronouncements concerning IFRS accounting and its impact on our financial statements and the ICRMSFR. Failure to adhere to these would present a substantial risk to the compliance of our financial reporting. In addition, the ICRMSFR has both preventive and detective controls, including, for example, automated and non-automated reconciliations, segregated duties with two-person responsibility, authorization concepts in our software systems, and corresponding monitoring measures.

Our Corporate Financial Reporting (CFR) department codifies all accounting and reporting policies in our Group accounting and global revenue recognition guidelines. These policies and the corporate closing schedule, together with our process descriptions, define the closing process. Under this closing process, we prepare, predominately through centralized or external services, the financial statements of all SAP entities for consolidation by CFR. CFR and other corporate departments are responsible for ensuring compliance with Group accounting policies and monitor the accounting work. CFR reviews accounting standards and processes to ensure applicable updates are made to SAP's financial reporting.

We have outsourced some tasks, such as the valuation of projected benefit obligations and share-based payouts, quarterly tax calculations for most entities, purchase price allocations in the context of asset acquisitions and business combinations, and the local statutory financial statements for a few of our subsidiaries. These outsourced tasks are subject to the same stringent requirements that are mandated for all our internally generated financially relevant information.

Based on an analysis of the design and operating effectiveness of our respective internal controls over financial reporting, a committee with leadership representation from Finance, Compliance, Legal, and IT presents the results of the assessment of the ICRMSFR effectiveness with respect to our IFRS consolidated financial statements as at December 31 each year to our Group CFO. The committee meets regularly to set the annual scope for the test of effectiveness, to assess and evaluate any weaknesses in the controls, and to determine measures to address them in good time and adequately. The Audit and Compliance Committee of the Supervisory Board regularly scrutinizes the resulting assessments of the effectiveness of the internal controls over financial reporting with respect to the IFRS consolidated financial statements.

The assessment, conducted by SAP and external audit, of the effectiveness of the ICRMSFR related to our IFRS consolidated financial statements concluded that, on December 31, 2022, the Group had an effective internal control system over financial reporting in place.

Additionally, and in compliance with German commercial law requirements, SAP maintains an internal control system beyond financial reporting. This is supported through automated controls (continuous control monitoring) as part of our business processes.

Supporting Software Solution

We use our own risk management software, namely SAP governance, risk, and compliance (GRC) solutions powered by SAP HANA, to support the governance process. GR&AS risk managers record and track identified risks using our risk management software online and in real time to help create transparency across all known risks that exist in the Group, as well as to facilitate risk management and the associated risk reporting. These GRC solutions also support the risk-based approach of the ICRMSFR. Our continuous control monitoring activities are performed utilizing our GRC software as well. This information is available to managers through direct access to our SAP Fiori application for enterprise risk reporting, and in regularly issued reports, and is consolidated and aggregated for the quarterly risk reports to the Executive Board.

We cannot exclude the possibility that if any one or more of the risks associated with this risk factor were to occur, the impact could be business-critical. We estimate the probability of occurrence to be unlikely, and classify this risk factor as medium.

Legal and IP: Claims and lawsuits against us, such as for IP infringements, or our inability to obtain or maintain adequate licenses for third-party technology, or if we are unable to protect or enforce our own intellectual property, may result in adverse outcomes.

We have in the past, and believe that we will continue to be subject to, claims and lawsuits, including intellectual property infringement claims either as our solution portfolio grows; as we acquire companies with increased use of third-party code including open source code; as we expand into new industries with our offerings, resulting in greater overlap in the functional scope of offerings; and as non-practicing entities that do not design, manufacture, or distribute products assert intellectual property infringement claims.

Moreover, protecting and defending our intellectual property is crucial to our success. The outcome of litigation and other claims or lawsuits is intrinsically uncertain.

We are subject to risks and associated consequences in the following areas, among others: dependency in the aggregate on third-party technology, including cloud and Web services, that we embed in our products or that we resell to our customers; integration of open source software components from third parties into our software and the implications derived from it; inability to prevent third parties from obtaining, using, or selling without authorization what we regard as our proprietary technology and information; and the possibility that third parties might reverse-engineer or otherwise obtain and use technology and information that we regard as proprietary. Moreover, the laws and courts of certain countries might not offer effective means to enforce our legal or intellectual property rights. Finally, SAP may not be able to collect all judgments awarded to it in legal proceedings. The outcome of litigation and other claims or lawsuits is intrinsically uncertain. Management's view of the litigation might also change in the future. Actual outcomes of litigation and other claims or lawsuits could differ from the assessments made by management in prior periods, which are the basis for our accounting for these litigations and claims under IFRS.

SAP has established measures intended to address and mitigate the described risks and adverse effects. For example, we: have various internal programs, such as internal policies, processes, and monitoring in place to assess and manage the risks associated with open source and third-party intellectual property; endeavor to protect ourselves in the respective third-party software agreements by obtaining certain rights in case such agreements are terminated; and are a party to certain patent cross-license agreements with third parties.

We cannot exclude the possibility that if any one or more of the risks associated with this risk factor were to occur, the impact could be major. We estimate the probability of occurrence to be likely, and classify this risk factor as medium.

Data Protection and Privacy: Non-compliance with increasingly complex and stringent, sometimes even conflicting, applicable data protection and privacy laws, or failure to meet the contractual requirements of SAP's customers with respect to our products and services, could lead to civil liabilities and fines, as well as loss of customers.

As a global software and service provider, SAP is required to comply with local laws wherever it does business. One of the relevant European data protection laws is the General Data Protection Regulation. International data transfers to third countries that do not provide for an adequate level of data protection require additional safeguards, including transfer risk assessments, to justify a transfer from the EU to a third country under the new EU standard contractual clauses.

Furthermore, evolving data protection and privacy laws, regulations, and other standards around the world (such as the California Consumer Privacy Act, the Chinese Personal Information Protection Law including data localization requirements, the EU Digital Services Act, and the EU's proposed e-Privacy Regulation) are increasingly aimed at protecting individuals' personal information when it comes to marketing and tracking their online activities. This may impose additional burdens for SAP due to increasing compliance standards that could restrict the use and adoption of SAP's products and services (in particular cloud services) and make it more challenging and complex to meet customer expectations. These changing criteria also impact the compliant use of new technology, such as machine learning and Artificial Intelligence for product development and deployment of intelligent applications.

Non-compliance with applicable data protection and privacy laws by SAP or any of the subprocessors engaged by SAP within the processing of personal data could lead to risks. These include, among others: mandatory disclosure of breaches to affected individuals, customers, and data protection supervisory authorities; investigations and administrative measures by data protection supervisory authorities, such as the instruction to alter or stop non-compliant data processing activities, including the instruction to stop using non-compliant subprocessors; or the possibility of damage claims by customers and individuals, contract terminations, and potential fines.

In addition, the German Federal Office for the Protection of the Constitution and security industry experts continue to warn of risks related to a globally growing number of cybersecurity attacks aimed at obtaining or violating company data including personal data.

Any of these events could have a material adverse effect on our reputation, business, financial performance, competitive or financial position, profit, and cash flows.

SAP has established measures intended to address and mitigate the described risks and adverse effects. For example, we: have implemented internal processes and measures to enable SAP to comply successfully and sufficiently with applicable data protection requirements; anchor data protection requirements in the mandatory product standards of SAP's product development lifecycle; continuously review SAP's existing standards and policies to address changes to applicable laws and regulations; continuously enhance our data center operations worldwide; actively monitor legal developments; engage with political stakeholders and government authorities; and provide clear governance and guidance on data handling, processing standards, and external communication as part of our data management framework, specifically incorporating aspects of new technologies such as those represented in embedded intelligence applications.

We cannot exclude the possibility that if any one or more of the risks associated with this risk factor were to occur, the impact could be major. We estimate the probability of occurrence to be likely, and classify this risk factor as medium.

Corporate Governance and Compliance Risks

Ethical Behavior: Our global business exposes us to risks related to unethical behavior and non-compliance with policies by employees, other individuals, partners, third parties, or entities associated with SAP.

SAP's leadership position in the global market is founded on the long-term and sustainable trust of our stakeholders worldwide. Our overarching approach is one of corporate transparency, open communication with financial markets, regulators, and authorities, and adherence to recognized standards of business integrity. This commitment to recognized standards of business integrity is formalized in SAP's CoEBC and supporting guidelines.

We are subject to risks and associated consequences in the following areas, among others: non-compliance with our policies and violation of compliance related rules, regulations, and legal requirements including, but not limited to, anti-corruption and anti-bribery legislation in Germany, the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, and other local laws prohibiting corrupt conduct; unethical and fraudulent behavior leading to criminal charges, fines, and claims by affected parties; collusion with external third parties; fraud and corruption; public sector transactions in territories exposed to a high risk of corruption; or increased exposure and impact on business activities in highly regulated industries.

Any of these events could have a material adverse effect on our business, reputation, brand, competitive or financial position, share price, profit, and cash flows.

SAP has encountered situations that required clear messaging and strong action on non-compliance in the context of corrupt behavior that has the potential to harm our business and reputation. SAP is continuing to investigate its dealings with the public sector.

SAP has established measures intended to address and mitigate the described risks and adverse effects. For example, we: continuously evolve our comprehensive compliance program based on the three pillars of prevention, detection, and response; improve associated business processes, to prevent further and future violations; review partner business models, to mitigate risks of corruption while meeting agility requirements; conduct internal audits of our compliance programs related to bribery, corruption, and substantial fraud; annually reconfirm commitment to the CoEBC by SAP's workforce (except where disallowed by local legal regulations); implement compliance policies and processes aimed at managing third parties and preventing misuse of third-party payments for illegal purposes, including the performance of compliance due diligence activities prior to the engagement of third parties; and launched a Partner Integrity Initiative aimed at examining the compliance programs of partners in SAP's ecosystem and reviewing the SAP-related deals closed by them. We also introduced a platform called "Speak Out at SAP" for anyone within and outside of SAP to raise confidentially and, if desired, anonymously their concerns on ethics and compliance related to our CoEBC and any law or regulation.

Despite our comprehensive and continuously evolving compliance programs and internal controls, intentional efforts of individuals to circumvent controls or engage in corruption, especially by way of collusion with other involved parties, cannot always be prevented.

We cannot exclude the possibility that if any one or more of the risks associated with this risk factor were to occur, the impact could be major. We estimate the probability of occurrence to be likely, and classify this risk factor as medium.

Operational Business Risks

Sales and Services: Sales and implementation of SAP software and services, including cloud, are subject to several significant risks sometimes beyond our direct control.

A core element of our business is the successful implementation of software and service solutions. The implementation of SAP software and cloud-based service deliveries is led by SAP, by partners, by customers, or by a combination thereof.

We are subject to risks and associated consequences in the following areas, among others: implementation risks caused by insufficient or incorrect information provided by customers, insufficient customer expectation management, including scope, integration capabilities and aspects, and a lack of purposeful selection, implementation, or utilization of SAP solutions; a lack of customer commitments and respective engagements; challenges to achieve a seamlessly integrated, sufficiently automated and aligned service delivery; unrenderable services committed during the sales stage; inadequate contracting and consumption models based on subscription models for services, support, and application management; deviations from standard terms and conditions; or statements concerning solution developments that might be misperceived by customers as commitments on future software functionalities.

Any of these events could have an adverse effect on our business, financial position, profit, and cash flows.

SAP has established measures intended to address and mitigate the described risks and adverse effects. For example, we: integrate risk management processes into SAP's project management methods that are intended to safeguard implementations through coordinated risk and quality management programs; conduct ethical scope reviews and monitoring that are adapted as required as part of a clearly defined change request process together with respective project governance, steering, monitoring and controlling activities; and put in place a policy that clearly outlines communication rules on future functionalities as well as legal requirements for commitments to customers.

We cannot exclude the possibility that if any one or more of the risks associated with this risk factor were to occur, the impact could be major. We estimate the probability of occurrence to be unlikely, and classify this risk factor as medium.

Partner Ecosystem: If we are unable to scale, maintain, and enhance an effective partner ecosystem, revenue might not increase as expected.

An open and vibrant partner ecosystem is a fundamental pillar of our success and growth strategy. We have entered into partnership agreements that drive co-innovation on our platforms, profitably expand our routes to market to optimize market coverage, optimize cloud delivery, and provide high-quality services capacity in all market segments. Partners play a key role in driving market adoption of our entire solutions portfolio, by co-innovating on our platforms, embedding our technology, and reselling or implementing our software.

We are subject to risks and associated consequences in the following areas, among others: failure to establish and enable a network of qualified and fully committed partners; failure of partners to develop sufficient innovative solutions and content on our platforms or to provide high-quality products or services to meet customer expectations; failure of partners to embed our solutions sufficiently enough to profitably drive product adoption; failure of partners to adhere to applicable legal and compliance regulations; failure of partners to transform their business model in accordance with the transformation of SAP's business model in a timely manner; and the failure of partners to comply with contract terms in embargoed or high-risk countries.

If any of these risks materialize, this might have an adverse effect on the demand for our products and services as well as the partner's loyalty and ability to deliver. As a result, we might not be able to scale our business to compete successfully with other vendors, which could have an adverse effect on our reputation, business, financial position, profit, and cash flows.

SAP has established measures intended to address and mitigate the described risks and adverse effects. For example, we: develop and enhance a wide range of partner programs to retain existing and attract new partners; offer training opportunities for our partners; provide safeguarding services to customers and partners; introduced a partner delivery quality framework; and implemented a certification process for third-party solutions to ensure consistent high-quality and seamless integration.

We cannot exclude the possibility that if any one or more of the risks associated with this risk factor were to occur, the impact could be major. We estimate the probability of occurrence to be unlikely, and classify this risk factor as medium.

Cloud Operations: We may not be able to properly protect and safeguard our critical information and assets, business operations, cloud offerings and portfolio presentation, and related infrastructure against disruption or deficient performance.

SAP is highly dependent on the availability, integrity, and reliability of our infrastructure and the software used in our cloud portfolio is inherently complex. We are subject to risks and associated consequences in the following areas, among others: the cloud portfolio or strategic direction of cloud operations may not fully meet customer demands; customers' cloud service demands may not match our data center capacity or control investments; capacity shortages could affect SAP's ability to deliver and operate cloud services as expected by or committed to our customers; scalability demands on infrastructure and operation could lead to cost increases and margin impacts; hyperscaler or infrastructure instabilities and the lack of availability or comprehensive contractual agreements could lead to challenges in meeting service level agreement (SLA) commitments; we might lack sufficient "future skills" for delivering and operating hybrid environments; we might lack the automation, standardization, and tools to manage and optimize operations and infrastructure; local legal requirements or changes to data sovereignty may lead to customers relocating their landscapes to a different data center; the loss of the right to use hardware purchased or leased from third parties could affect our ability to provide our cloud applications; disruptions to SAP's cloud applications portfolio (such as system outages or downtimes, SAP network failure due to human or other errors, security breaches, or variability in user traffic for cloud applications) could affect customer SLAs; hardware failures or system errors might result in data loss or corruption; partner co-location of data centers might not adhere to our quality standards; or we might not comply with applicable certification requirements, such as the Payment Card Industry Data Security Standard (PCI DSS).

Any of these events could have a material adverse effect on our reputation, business, competitive or financial position, profit, and cash flows.

SAP has established measures intended to address and mitigate the described risks and adverse effects. For example, we: consolidated and harmonized our data centers and our data protection measures, which included implementing security information and event management solutions as well as enforcing network access control; invest significantly in infrastructure and processes to ensure consistently secure operations of our cloud solutions while continuously improving resistance, resilience, reusability, and scalability towards a standardized and harmonized portfolio; continuously enhance our infrastructure landscape capabilities and deployment options, including harmonized, efficient, and highly repetitive migration services; adhere to stringent SLAs with hyperscalers to ensure a high-quality customer experience; increase transparency through our continuously enhanced and expanded SAP Trust Center, ensuring an appropriate level of information, for example, regarding planned patching activities and associated downtimes; monitor and invest in the continuous enhancement of our disaster recovery and business continuity capabilities; continuously aim for a homogeneous landscape that supports the complex infrastructure, application, and security requirements so that we can deliver the required service level for cloud services in a cost-effective manner; set up physical access control systems at facilities, multilevel access controls, closed-circuit television surveillance, security personnel in all critical areas, and recurring social engineering tests for SAP premises and data centers; control the access to information and information systems using authorization concepts that include managers and employees being regularly sensitized to the issues and given mandatory security and compliance trainings; adapt our cloud service delivery to local or specific market requirements (such as local or regional data centers) and comply with all local legal regulations regarding data protection and privacy as well as data security; establish contracts and SLAs with our public cloud partners to ensure that data security and privacy measures meet local regulatory and compliance standards and SAP's own standards for data security and privacy; maintain strict internal policies and controls concerning utilization of our partner's cloud infrastructure, including people, process, and technology standards required to ensure compliance and cyber resilience; closely monitor data center utilization, capacity, and pipeline for subsequent investment planning; regularly conduct risks reviews, disclosure requests, and audits to ensure public cloud providers meet SAP's data privacy and security standards; ensure PCI-validated compliance through successful PCI DSS audits; invest in training and certifications concerning hyperscaler and related next-generation technologies; and implement best-of-breed tools for IT operations management and automation.

We cannot exclude the possibility that if any one or more of the risks associated with this risk factor were to occur, the impact could be major. We estimate the probability of occurrence to be unlikely, and classify this risk factor as medium.

Cybersecurity and Security: Cybersecurity attacks or breaches, and security vulnerabilities in our infrastructure or services or those of our third-party partners could materially impact our business operations, products, and service delivery.

SAP delivers a full portfolio of solutions, hosts or manages elements of our customers' businesses in the cloud, processes large amounts of data, and provides mobile solutions to users. While SAP executes each of these areas either directly or through partners and other third parties, our industry continues to experience a complex and threatening cybersecurity landscape. The severity of these cybersecurity threats is amplified due to the increasingly sophisticated and malicious global landscape in which we operate. This includes third-party data, products, and services that we incorporate into SAP products and services, and the increasingly advanced obfuscation, control-circumvention, and related techniques employed by threat actors targeting IT products and businesses. Should we become aware of unauthorized access to our systems or those of our third-party partners, we have action plans in place intended to identify and remediate the source and impact of such events. Like many companies, we and certain of our third-party partners have experienced and expect to continue to experience cyberattacks and other security incidents that affect our business. While we experience cybersecurity incidents of various kinds in the ordinary course of our business, we are not aware of any such incidents that have had a business critical impact on our business.

We are subject to risks and associated consequences in many areas including, but not limited to, an increasing number of global threat actor attacks using ransomware as their preferred method of attack as well as unknown bugs, errors and vulnerabilities in our software and systems. We could experience material exposure to our business operations and service delivery due to disruptions to backups, disaster recovery or business-continuity management processes, or as the result of malicious or inadvertent actions by threat actors, employees, contractors, or a host of other parties. Security threats may also exist due to delayed or insufficient responses to identified issues or other interdependencies such as cloud service providers and those beyond SAP's cybersecurity infrastructure and protocols. Cloud4C, a third-party provider of data centers and related services supporting SAP's cloud customers in certain jurisdictions, recently experienced a ransomware attack that temporarily disrupted Cloud4C's operations. While Cloud4C identified no unauthorized access to customer data, for a brief period of time certain customers were unable to access data that was maintained in Cloud4C's data centers. SAP initiated its incident response protocols and worked with Cloud4C to promptly investigate, contain and remediate the incident. As part of those efforts, SAP issued credits to impacted customers pursuant to existing service-level agreements for which SAP received reimbursement from Cloud4C. While the overall fees and costs incurred by SAP to address the incident were not material, there can be no assurances that similar or more serious attacks impacting SAP or any third-party providers will not occur in future and that the consequences of such attacks would not result in a material adverse effect on SAP. Lack of compliance with security controls and governance to industry standards and regulations by us or third-party partners can impact adherence to external regulatory and customer requirements. Third parties could unknowingly introduce security threats and vulnerabilities without established security evaluation processes. Additionally, failure to integrate or maintain SAP's cybersecurity infrastructure and protocols with network systems obtained through acquisitions could result in loss of data confidentiality and integrity, and system availability.

The foregoing types of events could result in a loss of customers or customer opportunities, a diminished reputation in the marketplace, government investigations or enforcement actions, internal investigations, litigation including class actions, fines, or penalties, increased costs associated with remediation or compliance requirements, required changes to our business model or operations, and a host of other costs and losses, any or all of which could have a material adverse effect on our reputation, business, financial performance, competitive or financial position, profit, and cash flows. In response to the cybersecurity risk environment it is experiencing, SAP is continuously enhancing its cybersecurity program, for example by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and establishing a Cyber Fusion Center (CFC). In addition, the Executive Board and Supervisory Board continue to increase their governance of and involvement in cybersecurity matters, for example by focusing on cybersecurity audit and risk management topics. SAP has established measures intended to address the described risks and adverse effects, such as the continuous adaptation, standardization, and modification of our security procedures. This includes, among others: security risk identification, threat modeling, advanced threat defense, application patches and container security enhancements, and security validation of our critical components and services before shipment. We increased our investments and resources, including various internal initiatives to achieve SAP's objective of ensuring over time that our cybersecurity infrastructure meets or exceeds evolving industry standards. In addition, we enhanced the security capabilities in our hosting environment, cloud platforms, and cloud deployment tools,

(G.3) Other Litigation, Claims, and Legal Contingencies

This Note discloses information about intellectual property-related litigation and claims, tax-related litigation other than income tax-related litigation (see *Note (C.5)*), and anti-bribery matters.

Uncertainty in Context of Legal Matters

The policies outlined in *Note (A.4)* for customer-related provisions, which include provisions for customer-related litigation cases and claims, equally apply to our other litigation, claims, and legal contingencies disclosed in this Note.

The outcome of litigation and claims is intrinsically subject to considerable uncertainty. Management's view of these matters may also change in the future. Actual outcomes of litigation and claims may differ from the assessments made by management in prior periods, which could result in a material impact on our business, financial position, profit, cash flows, or reputation. Most of the lawsuits and claims are of a very individual nature and claims are either not quantified by the claimants or the claim amounts quantified are, based on historical evidence, not expected to be a good proxy for the expenditure that would be required to resolve the case concerned. The specifics of the jurisdictions where most of the claims are located further impair the predictability of the outcome of the cases. Therefore, it is typically not practicable to reliably estimate the financial effect that these lawsuits and claims would have if SAP were to incur expenditure for these cases.

Further, the expected timing of any resulting outflows of economic benefits from these lawsuits and claims is typically uncertain and not estimable, as it depends generally on the duration of the legal proceedings and settlement negotiations required to resolve them.

We are subject to a variety of claims and lawsuits that arise from time to time in the ordinary course of our business, including proceedings and claims that relate to companies we have acquired. We will continue to vigorously defend against all claims and lawsuits against us. The provisions recorded for these claims and lawsuits as at December 31, 2022, are neither individually nor in the aggregate material to SAP.

Among the claims and lawsuits disclosed in this Note are the following classes:

Intellectual Property-Related Litigation and Claims

Intellectual property-related litigation and claims are cases in which third parties have threatened or initiated litigation claiming that SAP violates one or more intellectual property rights that they possess. Such intellectual property rights may include patents, copyrights, and other similar rights.

Contingent liabilities exist from intellectual property-related litigation and claims for which no provision has been recognized. Generally, it is not practicable to estimate the financial impact of these contingent liabilities due to the uncertainties around the litigation and claims, as outlined above. The total amounts claimed by plaintiffs in those intellectual property-related lawsuits or claims in which a claim has been quantified were not material to us as at December 31, 2022 and 2021. Based on our past experience, most of the intellectual property-related litigation and claims tend to be either dismissed in court or settled out of court for amounts significantly below the originally claimed amounts. We currently believe that resolving the intellectual property-related claims and lawsuits pending as at December 31, 2022, will neither individually nor in the aggregate have a material adverse effect on our business, financial position, profit, or cash flows.

Individual cases of intellectual property-related litigation and claims include the following:

In June 2018, Teradata Corporation, Teradata US, Inc. and Teradata Operations, Inc. (collectively "Teradata") filed a civil lawsuit against SAP SE, SAP America, Inc., and SAP Labs, LLC in U.S. federal court in California. Teradata alleged that SAP misappropriated trade secrets of Teradata, infringed Teradata's copyrights (this claim was subsequently withdrawn by Teradata), and violated U.S. antitrust laws. Teradata sought unspecified monetary damages and injunctive relief. In 2019, SAP asserted patent infringement counterclaims against Teradata seeking monetary damages and injunctive relief. In 2020, Teradata initiated a second civil lawsuit against SAP asserting patent infringement, seeking monetary damages and injunctive relief; in February 2021, SAP filed patent infringement counterclaims against Teradata in this second U.S. lawsuit as well as a civil lawsuit against Teradata in Germany asserting patent infringement, seeking monetary damages and injunctive relief. Currently, all claims between the parties have been dismissed. Teradata has appealed the dismissal of its trade secret and antitrust claims; this appeal is expected to be completed by late 2023.

Tax-Related Litigation

We are subject to ongoing audits by domestic and foreign tax authorities. In respect of non-income taxes, we are involved in various proceedings with only a few foreign tax authorities regarding assessments and litigation matters on intercompany royalty payments and intercompany services. The total potential amount in dispute related to these matters for all applicable years is approximately €344 million (2021: €195 million). We have not recorded a provision for these matters, as we believe that we will prevail.

For more information about our income tax-related litigation, see *Note (C.5)*.

Anti-Bribery Matters

SAP has received communications and whistleblower information alleging conduct that may violate anti-bribery laws in the United States (including the U.S. Foreign Corrupt Practices Act (FCPA)), and other countries. The Office of Ethics and Compliance (OEC) of SAP is conducting investigations with the assistance of an external law firm and voluntarily advised the U.S. Securities and Exchange Commission (U.S. SEC) and the U.S. Department of Justice (U.S. DOJ), as well as local authorities where potential violations are being investigated. The investigations and dialogue between SAP and the local authorities and the U.S. SEC and U.S. DOJ are ongoing and neither the outcome of the investigations nor the date when substantiated findings will be available is predictable at this point in time.

The alleged conduct may result in monetary penalties or other sanctions under the FCPA and/or other anti-bribery laws. In addition, SAP's ability to conduct business in certain jurisdictions could be negatively impacted. The comprehensive and exhaustive investigations and the corresponding remediation activities are still ongoing. In South Africa, SAP is seeking resolution of pending civil claims relating to ongoing investigations. Although there could be an unfavorable outcome in one or more of the ongoing investigations, it is impossible at this point in time to make an informed judgment about any possible financial impact.

As a consequence, as at December 31, 2022, no provisions have been recognized for potential anti-bribery law violations in our consolidated financial statements. It is currently also not practicable to estimate the financial effect of any contingent liabilities that may result from these potential violations.

Materiality

Defining Key Priorities for Our Non-Financial Reporting

To select the topics to be included in our integrated reporting, we conducted a comprehensive materiality assessment in 2022, applying the requirements of the German Commercial Code as well as the newly introduced materiality definition of the Universal Standards of the Global Reporting Initiative (GRI): "Material topics are topics that represent an organization's most significant impacts on the economy, environment, and people, including impacts on their human rights."

Below, we have detailed the key stages of the process we followed to assess the significance of each economic, social, and environmental impact.

Identification

We compiled a list of relevant topics that builds on the long list of 2020, using the artificial intelligence (AI) and Big Data solution from Datamaran Limited. To ensure timeliness and completeness, we enriched the list with an analysis of further external sources covering, among others, corporate peer reports as well as mandatory and voluntary regulations for the software sector. To identify key topics and their boundaries, we looked at areas related to our operations and supply chain and at topics related to our solutions. Additional topics identified were added and mapped to the long list.

Prioritization

To assess the significance of each topic on the updated long list, we considered the following two perspectives:

1) Outside-in perspective (impact of the topic on SAP)
2) Inside-out perspective (SAP's impact on the topic)

To assess the outside-in perspective, we evaluated the financial, strategic, and regulatory relevance of each topic to SAP's business success and resilience. To this end, we ranked the topics and applied thresholds.

Next, we assessed the inside-out perspective. In a first step, we qualitatively described positive and negative impact scenarios for each topic on the list based on the results of the impact assessment, using the Value Balancing Alliance (VBA) methodology, through which we can monetarily measure SAP's impact on society and environment across the value chain, see the *Why Holistic Steering and Reporting Matters* section.

Following this, we assessed each negative impact scenario according to its likelihood and severity (scale, scope, remediability), and each positive impact scenario according to its likelihood, scale, and scope. We considered mitigation measures in place in the course of this process, and hence the net risks. During the assessment, we considered the input of several SAP sustainability experts from various units and regions, taking different stakeholders' pespectives[64] into account.

Next, we prioritized the assessed impacts by translating the result of each evaluation category into numeric values, ranking the topics, and applying thresholds to derive the material topics for SAP from the inside-out perspective.

According to section 289c (3) of the German Commercial Code (Handelsgesetzbuch, HGB), the material topics are identified by considering both the inside-out and outside-in perspectives. In contrast, the material topics according to GRI 3 only take into account the inside-out perspective.

[64] Represented stakeholder groups are further explained in section *Stakeholder Engagement*.

Validation

The results of the materiality assessment were reviewed and confirmed by our executive owners for integrated reporting. Our CFO thereafter approved the materiality assessment.

The changes in 2022 compared to 2021 include:

– Due to the introduction of the new Universal Standards of GRI, we applied a completely new approach towards the materiality assessment.

– In 2022, we added “Human rights” as a new material topic according to the HGB, while the number of material topics according to GRI decreased in total. We deleted the topics “Governance,” “Transparency,” “Resource efficiency and waste,” “Responsible supply chain,” “Solutions for an inclusive and circular economy,” and “Product responsibility”.

Review

Feedback on and analysis of our integrated report will be taken into account during future materiality assessments.

Results

In our reporting, we seek to meet the materiality requirements of both the GRI Standards and section 289c (3) of the HGB despite diverging definitions

The following topics are material according to both the HGB and GRI:

Topic	Definitions	Related Non-Financial Matters
Security, privacy, and data protection	Protection of private, confidential, or sensitive information and data, as well as the vulnerability of critical information systems	
Ethics and compliance	Responsible business conduct, including anti-corruption, anti-bribery, fair competition, respect for intellectual property, and responsible tax principles	Anti-corruption and bribery matters
Climate change and air quality	(Non-)greenhouse gas emissions from operations and products, as well as present or potential disruptive impacts of climate change	Environmental matters
Customer responsibility	Responsibility to help ensure customer satisfaction and customer rights, including responsible marketing and selling practices	
Employee engagement	Corporate culture, employee engagement and motivation, and strategic decisions involving workforce changes	Employee matters
Employee rights	Labor rights, including unionization, as well as compensation and benefits offered to employees by their employer	Employee matters
Well-being, health, and safety	Social, economic, psychological, and physical conditions of employees in their workplace, as well as employees' occupational health and safety	Employee matters
Human rights	Fundamental rights of all individuals to live in dignity	Respect for human rights

Additionally, according to the GRI Standards, the following topics are material:

Topic	
Fair and inclusive workplace	Active integration, equal opportunity, as well as fair treatment and remuneration of all employees
Talent and development	Talent attraction, retention, and development
Energy	Energy consumption by operations and products, and the transition to renewable energy

GRI Content Index

SAP SE has reported in accordance with the GRI Standards for the period from January 1, 2022, to December 31, 2022.

The 11 material topics in this GRI Content Index were selected based on the comprehensive *materiality assessment* conducted in 2022 and reflect the requirements of GRI 3 – Material Topics. We have clustered these topics according to the relevant *non-financial matters* set out in the German Commercial Code (Handelsgesetzbuch, HGB) (exception: the material topic “ethics and compliance” is not clustered under “Anti-corruption and bribery matters” as the corresponding GRI standards are defined more broadly).

We present the interconnection between the GRI topic-specific disclosures that are material to SAP and the 17 United Nations Sustainable Development Goals (UN SDGs).

Audit Scope

The content of the column UN SDGs as well as quantitative and qualitative information in relation to GRI 207 Tax were not subject to the independent limited assurance engagement of our external auditor.

General Disclosures

	Links and Content	In scope of External Audit[85]	UN SDGs
2-1	*Strategy and Business Model*	✓	
2-2	*Strategy and Business Model* *About This Report* *https://www.sap.com/about/company/office-locations.html*	✓ ✓	
2-3	*About This Report* *Independent assurance practitioner's report* *Financial Calendar and Addresses*	✓	
2-4	*Non-Financial Notes* In 2022, we did not have any material restatements of information of previous reporting periods.	✓	
2-5	*Independent assurance practitioner’s report* *https://www.sap.com/investors/en/governance/supervisory-board.html*		
2-6	*Strategy and Business Model* *Sustainable Procurement*	✓ ✓	
2-7	*Headcount and Personnel Expense* *Note (B.1) Employee Headcount* *Finance and ESG Data* At SAP, we have a multitude of non-headcount relevant employee categories defined. None of these categories match the GRI definition of “non-guaranteed hours employees.” However, at SAP we have employees who are paid hourly (for example, working students) but who have a reliable minimum number of hours guaranteed. This group represents less than 1.5% of the total SAP workforce.	✓ ✓ ✓ ✓	8, 10

[85] Level of external audit: Limited assurance, reasonable assurance, and statutory audit. For further information regarding the External Audit scope, please refer to the Audit Scope checkboxes in each chapter.

	Links, Content, and Omissions	Boundaries	In scope of External Audit[85]	UN SDGs
	appropriate, perform risk assessments globally. These include cross-business topics and the evaluation of risks related to compliance, bribery, and corruption. Overall, our corporate risk assessments focus on compliance topics. In addition, 53% of all audits concluded in 2022 under the risk-based audit plan are compliance-relevant audits. As part of this process, a regular and dedicated focus is also placed on identifying high-risk countries so as to identify deep dive reviews and necessary mitigations accompanied by regular monitoring. Furthermore, ad hoc audits are performed if there are grounds of suspicion. This regular auditing is a vital component of ensuring compliance worldwide in our business processes and identifying weaknesses or non-compliance to derive adequate measures. Given the holistic approach of our compliance risk assessment, SAP does not report on the number of audits solely related to corruption.			
205-2	The CoEBC provides the primary ethical and legal framework within which SAP conducts business. It also addresses SAP's policies regarding anti-corruption. SAP's Code of Ethics and Business Conduct (CoEBC) is available internally on the Company's intranet and externally on the Internet. All members of the SAP Executive Board and Supervisory Board, all SAP employees, all SAP partners, suppliers, and shareholders, as well as the general public have full access to the CoEBC. We do not collect the data of the geographical distribution and the type of our business partners, who accessed the CoEBC. For a breakdown of the geographical distribution of all SAP employees, see "Finance and ESG Data." The completion rate for mandatory training applicable to all SAP employees[87] on the subject of anti-corruption exceeded 99% in 2022. The numbers of employees per region are listed below: • APJ: 18,698 • Greater China: 5,916 • EMEA: 11,726 (includes five Executive Board Members) • MEE: 32,480 • LAC: 4,954 • North America: 19,582 (includes two Executive Board members) Furthermore, the Group Chief Compliance Officer (GCCO) reports on compliance matters on a quarterly basis to the Executive Board and to the Audit and Compliance Committee of the Supervisory Board.	SAP + external parties	✓	
206-1	*Note (G.3) Other Litigation, Claims, and Legal Contingencies*	SAP	✓	16, 17
207-1	*SAP Global Tax Principles*	SAP		9, 11, 16
207-2	*SAP Global Tax Principles*	SAP		9, 11, 16
207-3	*SAP Global Tax Principles*	SAP		9, 11, 16
207-4	As a German company, we report our tax expense separately for Germany and the rest of the world. We are confident that this information meets our stakeholders'			

[87] Excludes employees on long-term sick leave, parental leave, members of acquired companies, and those in early retirement.

Stakeholder Capitalism Metrics

To support long-term value creation, SAP has committed to applying the World Economic Forum (WEF) Stakeholder Capitalism Metrics and encourages further global standardization and convergence in the ESG reporting landscape. We include the standards in our own reporting and also offer the framework in our core sustainability software solutions.

The following table provides information about the core metrics proposed by the WEF White Paper titled "Measuring Stakeholder Capitalism: Towards Common Metrics and Consistent Reporting of Sustainable Value Creation."

The table refers to the sections of our Management Report, Notes, Form 20-F, and other sources that contain the respective disclosures. Core metrics that have not been identified as material for SAP during our latest materiality analysis have been omitted.

Principles of Governance

Theme	Core Metrics and Disclosures	Links	Comments
Governing Purpose	Setting purpose	*Strategy*	
Quality of Governing Body	Governance body composition	*Corporate Governance Statement* *https://www.sap.com/investors/en/governance/supervisory-board.html* *Form 20-F Item 6* *Note (G.4)*	
Stakeholder Engagement	Material issues impacting stakeholders	*Materiality* *Stakeholder Engagement*	
Ethical Behavior	Anti-corruption	*Business Conduct* *Note (G.3) Other Litigation, Claims, and Legal Contingencies* *SAP Partner Code of Conduct*	Provisions for material corruption cases would be reported together with further details in Note (G.3). Partners are also requested to complete any compliance training available based on their partner type. For more information, see SAP's Partner Code of Conduct.
	Protected ethics advice and reporting mechanisms	*Business Conduct* *Speak Out at SAP*	
Risk and Opportunity Oversight	Integrating risk and opportunity into business process	*Risk Management and Risks* *Expected Developments and Opportunities*	