

Sustainability Statement



Sustainability Statement - General



Reporting principles

BP-1 Basis for preparation

F-Secure is a Finnish and globally operating cyber security company. The parent company of the Group is F-Secure Corporation incorporated in Finland and domiciled in Helsinki, Finland. This statement has been prepared from the Group perspective (unless stated otherwise) and on consolidated basis to be published as part of the Board of Directors' report. This sustainability statement has been prepared in accordance with the Accounting Act Chapter 7 and European Sustainability Reporting Standards (ESRS).

The scope of this sustainability statement is the same as for the financial statement and complies with the EU European Sustainability Reporting Standard (ESRS). It includes information on the material Impacts, Risks and Opportunities (IROs) connected with the direct and indirect business relationships in the upstream and downstream value chain of F-Secure as described under SBM-1 section.

F-Secure has not omitted any specific information corresponding to intellectual property, know-how or the results of innovation. F-Secure has not used the exemption from disclosure of impending development in the course of negotiation, as provided for in articles 19a(3) of the directive 2013/34/EU of the European Parliament and of the Council.

BP-2 Disclosures in relation to specific circumstances

The specific circumstances applicable to F-Secure and their effect on sustainability reporting are listed in this section of the sustainability statement.

Planning horizon

F-Secure defines short-, medium- and long-term time horizons in accordance with table 1. The reason for deviating from ESRS is caused by the alignment of definitions with F-Secure's financial planning horizons and how we provide guidance to investors on topics such as growth and profitability.

Time horizons	Years	Alignment of definitions
Short term	0 - 1	Standard F-Secure strategy and planning period.
Medium term	1 - 3	Standard F-Secure strategy and planning period.
Long term	3 +	Standard F-Secure strategy and planning period.

Table 1. F-Secure planning horizon definitions .

Value chain estimation

The main value chain-related data is related to GHG emissions. F-Secure has calculated its GHG emissions in accordance with the GHG Protocol and used value chain estimations to complete the model where actual data is not available.

The quantification of GHG emissions of F-Secure emissions is systematical and any uncertainties have been reduced as far as practical. Consistent methodology has been used to allow for meaningful comparisons of emissions over time. Any changes to the data, inventory boundary, methods, or any other relevant factors are documented. It is usual that estimations and sector averages are used in GHG calculation in cases where actual data is not available.

In coming years, changes of varying degrees may occur in the company's operations, which, in turn, may affect the created GHG emissions. All relevant and significant changes or abnormalities will be enclosed in the current GHG report to enhance the transparency of the calculation results.

At any time when a change occurs, F-Secure will review whether the change is significant enough to trigger the base year calculation. In addition, F-Secure will aim to improve the quality of the data included in the calculation, moving away from estimations to actual emission data where possible. The improvement of the data will be conducted in collaboration with the stakeholders in F-Secure's value chain.

Sources of estimation and outcome uncertainty

F-Secure's GHG emissions calculation contains a degree of uncertainty, especially regarding scope 3. In Scope 1, leased cars data is limited and the calculations have been done based on estimating contract kilometers and average consumption of car models. In Scope 2, there was limited site-specific consumption data available for energy consumption in some of the offices, including electricity, heating and cooling.

It is typical that in scope 3, many estimations and assumptions are made due to limited availability of actual emission data, for example, from suppliers. The estimations and assumptions include:

The category 1 calculations are all spend-based and the emission factors of the purchased services were inflation-adjusted. Category 5 emissions were calculated by estimating the amount of office waste generated in F-Secure's facilities. Categories 7 and 11 were calculated based on proxy data and estimations, which increases the degree of uncertainty in the results. Electricity usage of home and coworking spaces was also estimated. Furthermore, there are uncertainties for objectivity in cyber security metrics as stated under S4 Consumers and End-users section. Finally, the measurement of the metrics in this Sustainability Statement have not been validated by an external body apart from the assurance of this sustainability statement unless specifically stated otherwise under disclosure requirement section of such metrics.

Forward-looking statement

This Sustainability Statement contains forward-looking statements that reflect the current views and assumptions of F-Secure. Accordingly, the statements should be considered with caution and the understanding that they are not historical facts or promises. Such statements are subject to risks and uncertainties, most of which are difficult to predict and are generally beyond the control of F-Secure. Some of the factors that might influence our ability to achieve our objectives include (but are not limited to) the progress of our strategy implementation, stronger-than-expected competition, macroeconomic developments, technological innovations, market consolidation, legal proceedings, government actions, and regulatory developments, each and all of which may have an adverse effect (which may be material) on our results. Further, the economic downturn in our markets may also impact our business development and the availability of financing on favorable conditions. If these or other risks and uncertainties materialize, or if the assumptions underlying any of these statements prove incorrect, our actual performance may materially differ from the performance expressed or implied by forward-looking statements. We offer no assurance that our estimates or expectations will be correct or accurate and, therefore, our results may differ significantly from those set out in any forward-looking statements as a result of various factors.

Disclosures stemming from other legislation or reporting pronouncements

F-Secure has included in the sustainability statement disclosures in section S4 Consumers and End-users related to the following legislation, standards and international principles:

1. Cyber security policy-related metrics and targets including cyber security training, cyber security incidents and bug bounty program based on
 - a. EU General Data Protection Regulation
 - b. ISO 27001 information security management standard
2. Code of Conduct policy- and practice-related metrics, anti-corruption incidents and code of conduct training also based on (see section ESRS S4-1 for further details)
 - a. OECD Guidelines for multinational enterprises
 - b. United Nations Global Compact
 - c. United Nations Guiding principles on Business and Human rights
 - d. United Nations Convention against Corruption
 - e. International Bill of human rights
 - f. The Declaration of the International Labour Organisation on Fundamental Principles and Rights at Work

Incorporation by reference

Incorporation by reference outside the sustainability statement has not been conducted.

Omitted information

F-Secure's employee count does not exceed the average number of 750 employees during the 2024 financial year. We have decided to omit some of the information required by ESRS E1 and ESRS S1 in accordance with Appendix C of ESRS 1. F-Secure has opted to comply with ESRS 2 SBM-3 paragraph 48(e) by reporting only qualitative disclosures for the first 3 years of preparation of its sustainability statement. In addition, F-Secure has decided to omit in our 2024 statement matters related to "E1-9 Anticipated financial effects from material physical and transition risks and potential climate-related opportunities". Related to our own workforce (S1), we've omitted "S1-7 Characteristics of non-employees in the undertaking's own workforce" in full and "S1-14 Health and safety metrics" partially.

Governance

Gov-1 The role of the administrative, management and supervisory bodies

In this Sustainability Statement, 'supervisory bodies' refer to the F-Secure Board of Directors and its Audit Committee and Personnel and Nomination Committee. 'Management body' is to be understood as the F-Secure Leadership Team including the CEO and the leadership team members. The Board of Directors oversees the administration of the company and appoints the CEO, who oversees the daily administration of the company in accordance with the instructions and orders given by the Board.

The highest decision-making body in F-Secure is the General Meeting of Shareholders, which elects the members of the Board of Directors. The Board of Directors is responsible for the administration of F-Secure Group and appropriate organization of its operations. The duties and responsibilities of the Board of Directors of F-Secure are, inter alia, defined according to the Articles of Association of F-Secure, the Finnish Companies Act and other applicable laws and regulations. As such, the Board oversees F-Secure's business conduct and compliance, and approves the most significant governance-related policies, such as the Anti-Bribery and Corruption Policy.

The Board of Directors appoints the CEO. The CEO, assisted by the Leadership Team, is responsible for managing the company's business and implementing its strategic and operational targets. Both the CEO and the Leadership Team also play a significant role in ensuring that employees comply with the relevant policies and procedures, including those related to business conduct.

To enhance the efficiency of its work, the Board of Directors has established an Audit Committee and a Personnel and Nomination Committee. The Audit Committee functions as a preparatory body, and the matters it addresses are brought to be decided on by the Board of Directors. The Audit Committee monitors and evaluates risk management, internal controls, IT strategy and practices, sustainability, and financial reporting, as well as auditing. The majority of members of the Audit Committee shall be independent of the company and at least one member shall be independent of the company's significant shareholders. Additionally, any substantiated investigations of incidents related to corruption or bribery are reported to the Audit Committee for evaluation. The Personnel and Nomination Committee prepares material and instructs on issues related to the composition and compensation of the Board of Directors and remuneration of the other members of the top management of the company. The Committee prepares proposals for

shareholders related to the Board composition and remuneration. The duties of the Personnel and Nomination Committee include actively seeking and identifying new individuals qualified to become members of the Board.

The Board of Directors and the Leadership Team are supported by the Legal Team that maintains the business conduct-related policies and procedures, as well as offers internal training on such issues.

Expertise related to business conduct matters

The Board members have international experience in different roles in global companies operating in different businesses and geographical market areas. Additionally, the company ensures that all members of the Board of Directors have access to sufficient information about F-Secure's business operations, operating environment, and financial position, and that new members are properly introduced to the operations of F-Secure.

Members of the Audit Committee must have broad business knowledge, as well as sufficient expertise and experience concerning the committee's area of responsibility and the mandatory tasks relating to auditing, including risk management related to business conduct issues. The Audit Committee invites experts to its meetings when necessary for the issues to be discussed. External auditors are permanent invitees to the meetings of the Audit Committee.

When seeking and identifying new individuals qualified to become members of the Board, the Personnel and Nomination Committee takes into account the expertise on business conduct matters of such individuals to ensure that all Board members have sufficient experience and knowledge of business conduct matters.

The Leadership Team members are chosen based on their expertise and experience suitable to their respective roles. The Leadership Team members also supervise the implementation of business conduct-related policies and procedures in their respective business functions.

The number of executive and non-executive members

As of 31 December 2024, F-Secure had 9 executive members in its management body and 6 non-executive members in its supervisory body (Board of Directors), while noting that the latter figure used in this statement also includes F-Secure employee Board member.

Representation of employees and other workers

One member of the Board of Directors is elected from among F-Secure personnel. An election is arranged annually for F-Secure personnel and each permanent employee is eligible to stand as a candidate. The representatives of the Board of Directors interview three to four persons who have obtained the highest number of votes in the elections and choose a candidate from amongst them to be proposed for election as a member of the Board by the Annual General Meeting. The term of office of members of the Board of Directors ends at the close of the Annual General Meeting of shareholders following their election.

Experience relevant to the sectors, products and geographic locations of the company

F-Secure's Board members have international experience and diverse backgrounds from international companies in business sectors and geographical markets (including Europe, North America, APAC and Japan) relevant to F-Secure:

- Pertti Ervi is a seasoned international IT-business leader and Board professional with over 30 years of experience. As Co-President of Computer 2000 AG, Europe's largest IT distributor, he managed global operations across 38 countries. Pertti has extensive Board experience with publicly listed companies like F-Secure, Comptel, Teleste and Efecte, and has worked closely with tens of growth companies, providing expertise in strategy, internationalization, and corporate development. He co-founded Mintly Oy and has successfully led numerous high-value exits. A Finnish citizen living in France, Ervi holds a B.Sc. in Electronics and has completed advanced business studies at INSEAD and Hanken.
- Risto Siilasmaa is the founder of F-Secure and WithSecure Corporations and the Chair of the Board of Directors of WithSecure having served as President and CEO of the company in 1988-2006. He is also an active venture capital investor with over 30 active investments via First Fellow Partners, a fund management company where he is both a general partner and the only limited partner. Previously Risto was the Chair of the Board of Directors of Nokia Corporation in 2012-2020 and of Elisa Corporation in 2008-2012. Risto is the Chair of the Board of Upright and a Board member of F-Secure, Futurice, Pixieray, Quanscient, Hamina Wireless and CybExer Technologies. Since 2019 Risto has been a member of the International Advisory Board at IESE Business School, University of Navarra.
- Thomas Jul is a seasoned Danish executive with over 30 years of global leadership in high-tech, telecom, and fintech sectors. With a history of driving growth and transformation, he held prominent roles at Ericsson and Nokia, including President & CEO of Ericsson Indonesia and West Europe Region Head

at Nokia. As co-founder of MATTA Group and former CEO of payments scale-up Inpay, Thomas continues to excel in leading innovative organizations. Currently, he serves as Group CEO of Danish IT leader KMD. Thomas holds an M.Sc. in Software Engineering and has completed advanced business programs at Henley, Wharton, Columbia, Harvard, and London Business Schools.

- Petra Teräsaho is a senior finance executive and Board professional with wide international experience from various industries: forest, telecom, mining, IT, automotive/electric batteries & consumer goods. In addition to finance, Petra has held leadership positions in marketing, strategy and business development. Besides Finland, Petra has worked and lived in India, Belgium, France and Sweden. Her current main occupation is CFO of Transmeri Group. Her earlier employers are UPM, Nokia, Outotec, Stora Enso, Enfo Group and Valmet Automotive. Petra is Board member and Audit committee chair in F-Secure and Paulig Group. She is a Finnish citizen and holds a Masters Degree in Accounting & Finance.
- Tommi Uitto has worked in Nokia's network equipment business for thirty years, from 2G/GSM to 5G/NR and early research of 6G. He is currently leading Nokia's Mobile Networks Business Group, the largest of Nokia's four businesses, and is a member of Nokia Group Leadership Team. He also serves in the Board of Directors and Working Committee of the Board of Technology Industries of Finland (TIF). At Nokia, he has held various executive and managerial positions across several functions from business unit management to sales and region management, from product management to product development, and from production planning to quality management. Before Nokia, he worked in forestry equipment manufacturing. Besides Finland, he has lived in France and the United States.
- With extensive experience in quality assurance, software development management, and portfolio governance, Katja Kuusikumpu is a respected leader in the IT industry. As the Director of Portfolio Governance & Operations at F-Secure, she oversees strategic product initiatives and drives the company's portfolio transformation. She is also currently a Member of the Board of Directors at F-Secure, contributing to the company's strategic direction. Previously, Katja has held several R&D leadership roles at F-Secure and in other Finnish and international companies. Katja is a Finnish citizen and holds a Master of Science degree from Aalto University.

Percentage by gender and other aspects of diversity

According to Diversity Principles established by the Board of Directors, an optimal mix of diverse backgrounds, expertise and experience strengthens the Board's performance and promotes the creation of long-term shareholder value.

The Diversity Principles of the Board of Directors strives towards appropriately balanced gender distribution. At the Annual General Meeting in 2024 six members representing two different nationalities were elected to the Board. The age structure of the Board members is 47–67 years. Two Board members are female and four are male, giving a ratio of 2:4 (female/male) and thus females represent 33.3% and males 66.7% of all members of the Board.

Percentage of independent board members

The majority of the 2024 Board members are independent from the company and from its major shareholders. Two Board members are considered not independent on grounds of share ownership or working for the company meaning ~67% are independent.

Responsibilities for IRO oversight

At F-Secure, ESG covers all layers of the organization as described in the figure below:¹⁾

¹⁾A Culture, health and well-being committee and an Environment committee were established in Q3 2024 and before that the topics were covered by the ESG Council. Oversight of each topic will remain with the ESG Council and the administrative bodies. Also, donations and sponsorships are ultimately approved by the CEO.



Figure 1. ESG governance at F-Secure

Our ESG Policy outlines our commitments to environmental stewardship, social responsibility, and ethical governance. Thereby, it provides clear guidance on how the business addresses ESG challenges and monitors progress.

F-Secure's CEO supported by the Leadership Team establishes a company strategy that is approved by the Board of Directors. ESG is tightly integrated into the company strategy and our daily operations rather than approved as a separate "ESG strategy". The Board of Directors also approves remuneration policies including alignment with sustainability topics. The Board of Directors is furthermore updated at a minimum annually on ESG progress by the management in addition to updates from the Audit Committee.

The Audit Committee monitors and evaluates risk management, internal controls, ESG reporting, as well as independent assurance. The Audit Committee is regularly updated on ESG topics and related progress, and reports progress on ESG topics to the Board of Directors. The Audit Committee also reviews the preparation of the sustainability statement, including the identification of the material topics to be covered by the statement and the implementation of sustainability statement assurance with an external auditor. The Audit Committee presents the results of the sustainability statement to the Board of Directors with specifications on how the external assurance has increased the credibility of the statement and what the Audit Committee's role has been in the assurance process.

Our ESG Council is responsible for facilitating, implementing and tracking our ESG activities, including alignment with the company strategy process and other necessary company processes such as risk management, and drives the creation of the annual sustainability statement. All ESG activities are company strategy-driven and based on our values, Code of Conduct, and ESG-related policies and processes. The ESG Council also drives regular reviews of our sustainability topics, including reviewing the relevancy and accuracy of our DMA and IROs.

We've also established ESG Committees with nominated leads to drive forward committee-specific agendas, for example, diversity or well-being. Moving to 2025, ESG Committees participate in IRO analysis, are informed on the analysis results and support developing required actions and executing the plans towards set targets. We track the effectiveness of the impacts in the ESG Council and communicate the actions taken on an annual basis as part of our sustainability statement.

Management role in assessing and managing IROs

While ESG ownership resides with the Corporate Development function, which is part of the Leadership Team, we've established a cross-functional ESG Council that is responsible for the identification and assessment of impacts, risks, and opportunities (IRO) at minimum twice a year. Results are shared with the Audit Committee for review and oversight including internal controls, while targets related to material topics are approved by the Board of Directors.

Oversight on target setting and monitoring progress

F-Secure has targets and metrics set for strategically important ESG topics, which have been identified in the Double Materiality Assessment. The targets are time-bound and outcome-oriented and we report on our progress as part of our annual sustainability report. The targets are developed by internal and external (when needed) subject matter experts and reviewed by the ESG Council and Leadership Team, noting that some of them have been established for the reporting year 2024. The targets and progress towards them are presented to the Audit Committee and Board of Directors at minimum on an annual basis.

Controls and procedures and integration with internal functions

We continuously develop our ESG reporting process and controls in terms of data and reporting quality, transparency, and accountability. For ESG-related data, F-Secure has identified relevant functions and owners for the data, as well as implemented ESG-related controls on data collection and management practices similar to F-Secure's financial reporting. We've assigned owners for each control that range across functions such as HR, IT, Legal and Product Management. When a new measure or target is implemented the need for a new control is assessed and implemented if risks related to data management are identified.

Availability of appropriate skills and expertise to oversee sustainability matters

The Board of Directors has received ESG training 2024 to build appropriate skills and expertise to oversee sustainability matters. The training included information about the relevant EU-related regulations and the related responsibility of the Board of Directors. In addition, the training included information about the Double Materiality Assessment and third-party assurance of the sustainability statement.

In conjunction with the training, the Board was updated on F-Secure's sustainability targets, governance and related activities.

Additionally, a member of the Board who is also the current Chair of the Audit Committee has previous expertise in establishing sustainability-related reporting practices. Our financial assurer has the option to participate in Audit Committee meetings when ESG topics are reviewed, providing further access to ESG knowledge to F-Secure Audit Committee. F-Secure has also established an ESG Council to drive the ESG agenda across the company with the Chair having previous experience in ESG-related matters while our Chief People Officer similarly has previous experience in ESRS reporting.

GOV-2 Information provided to and sustainability matters addressed by F-Secure administrative, management and supervisory bodies

The F-Secure Board has ESG on the agenda at minimum once a year, while during 2024 the F-Secure Audit Committee had ESG on the agenda in 4 out of 5 meetings. Updates on ESG topics to the Board, the F-Secure Leadership team, and the Audit Committee have been presented by the SVP of Corporate Development responsible for creating and implementing F-Secure ESG plans, policies and targets and report on their progress as well as implementation of due diligence, based on input from the ESG Council and its members.

The F-Secure ESG Council typically meets monthly including the CFO, CPO, Legal Counsel, SVP of Corporate Development, and the ESG function lead reporting to the SVP of Corporate Development. In addition, the ESG Council includes participants from other functions for further collaboration like sales and product management while the ESG Committee leads provide updates on progress, when topical. Moving to 2025, Committees will also participate in the bi-annual assessment of the DMA/ IROs and will track the effectiveness of actions and metrics related to them.

Consideration of IROs when overseeing company strategy and risk management

Sustainability-related risks and adverse impacts are managed as part of F-Secure's risk management process. In short, the primary goal of F-Secure's risk management policy is to enable the organization to identify and manage risks more effectively. The risk management process monitors the potential negative impact and likelihood of various situations arising from the company's operations, its markets, its customers, or its partners.

F-Secure encourages continuous risk assessment by the company's personnel. The relevant operational risks identified through the risk management process

are regularly reviewed by each function, including the twice-a-year review with the President and CEO, the Leadership Team, and the Audit Committee. Positive impacts and opportunities, on the other hand, are embedded into the strategy process and considered when reviewing F-Secure's operating plans and related objectives, developing plans and allocating resources to execute said plans.

Evaluating trade-offs related to IROs is an important part of the strategy process, as it involves making decisions about where to allocate resources and prioritize initiatives. This involves weighing the costs and benefits of different options and making choices that align with the organization's overall goals and stakeholder expectations. This ensures that trade-offs are considered relative to the company objectives, while weighing the potential risks and opportunities associated with different options.

Furthermore, during 2024, updates on the DMA including IROs have been presented to the ESG Council and Audit Committee. These impacts, risks and opportunities include topics listed below and are addressed by the administrative, management and supervisory bodies described earlier:

- Protecting consumers' digital moments
- Attracting, developing, and retaining talent
- Company working conditions and employee well-being
- Critical strategic competencies and DEI (equal treatment and opportunities for all)
- Privacy and security related to, e.g., how we use and protect consumer or partner data
- Cyber security threats related to end-customers, partners, and our operations
- Business-conduct topics including anti-bribery, anti-corruption and whistleblowing channels
- Development and launching of a new company culture
- Climate change mitigation risks, roadmap and strategy

GOV-3 Integration of sustainability related performance in incentive schemes

The F-Secure Leadership Team is eligible for the non-sales Short-Term Incentive (STI) Plan. The purpose of the STI Plan is to reward participants for achieving the financial and operational objectives of the Company, to focus on execution of the business plan, and to foster a performance culture.

The Leadership Team is also eligible for the share-based long-term incentives (LTI) to align the interests of the shareholders and the Leadership Team. Part of our administrative and supervisory bodies' remuneration is tied to LTIs similar to the Leadership Team.

Role of sustainability-related targets in incentive schemes

The goals of F-Secure's 2024 non-sales STI Plan included the Company Business Results (combined growth % and profitability %) and the Company Employee Engagement (eNPS). These STI elements are tightly connected to our material sustainability drivers as growth is a proxy number for the number of consumers that we protect globally ("building trust in digitality and society"), while eNPS represents the importance of our employee well-being and satisfaction.

The non-sales STI Plan is included in the remuneration policy, and the goals of the non-sales STI Plan as described here are approved by the Board annually. Similarly, performance against the targets is reviewed regularly while any pay-outs take place annually.

Share-based LTI programs can be based on long-term financial and/or strategic performance or on the company's share value increase. In performance-based LTI programs, the criteria for the performance period are based on strategic financial targets.

STI or LTI plans do not contain any climate-related targets.

Proportion of variable remuneration dependent on sustainability-related targets and approvals

The non-sales STI consists of the Business Results (combined growth % and profitability %) with 60-80% weight, a function-specific target with 0-20% weight that may link to sustainability related targets and the Company Employee Engagement (eNPS) goal with 20% weight. The Long-Term Incentive criteria for the performance period are based on strategic financial targets.

The annual non-Sales STI design and the company-level targets are approved by the Board of Directors based on a proposal made by the Leadership Team. For the LTI programs, the Board of Directors decides on the terms and conditions for the plans and the possible performance criteria and objectives for each performance/ vesting period.

GOV-4 Statement on Due Diligence

As part of F-Secure due diligence we identify, mitigate, and account for how we have addressed actual and potential negative impacts connected to our business, our operations and value chain, our offering and business partners. Due Diligence is an ongoing practice that responds to and may trigger changes in our ESG governance, strategy, business model, activities and processes, business partners, operations, or sourcing. For further details, also see chapter on ESG governance and the role of administrative, management and supervisory bodies and the section on Governance.

Engagement with stakeholders

Through mapping all relevant stakeholders and conducting regular stakeholder engagement, F-Secure ensures an effective corporate sustainability due diligence process. The mapping includes employees, customers, suppliers, investors, and government bodies. We will review the stakeholder map when significant changes in the business model and strategy occur or if new impacts are identified as part of our IRO reviews and as described further under IRO-1 section.

On adverse impacts

Addressing and taking action on adverse impacts is conducted in alignment with F-Secure's risk management policy, where risks have an owner to drive mitigation activities. F-Secure uses risk modeling and quantification methods to identify and manage risks effectively. Risks are mitigated and proactively monitored, also building strategic resilience in the Company and its business operations where applicable. F-Secure has not identified any adverse impacts as described under the "F-Secure impacts on people and the environment" section.

Risk management is an integrated part of F-Secure's governance and management, and the risk management process is aligned with the ISO-31000:2018 guidelines. Each function is responsible for tracking the effectiveness of the mitigation activities and aligning with relevant internal or external stakeholders. The Leadership Team and Audit Committee review the risks bi-annually, while the Audit Committee regularly evaluates the effectiveness of the risk management process (internal controls).

GOV-5 Risk management and internal controls over sustainability reporting

Control over sustainability matters is organized and formalized through policies, procedures, and processes, as described in this sustainability statement. ESG-related policies and procedures are proposed and developed by the ESG Council

or relevant functions and approved by the CEO, the Board or a member of management depending on the policy. The Audit Committee reviews the policies presented to the Board and the Code of Conduct is approved by the Board.

F-Secure has internal control operating procedures in place which apply to the entire company. Principles and recommendations introduced in the Finnish Corporate Governance Code for listed companies are reflected in our Internal Control Framework. Based on risk assessment the key processes are identified. For the identified processes key risks and related internal control points have been defined and documented in internal control matrices. ESG has been identified as one of the key processes and we've developed internal controls for material ESG topics. Internal Control definition as adopted by F-Secure consists of e.g. policies, procedures, control activities, and monitoring, executed by F-Secure's Board of Directors supported by the Audit Committee, the CEO, F-Secure's Leadership Team and other operative management, and all F-Secure employees, designed to provide assurance regarding the achievement of F-Secure's objectives.

Monitoring helps ensure that internal control activities are carried out properly and in a timely manner, thus ensuring that F-Secure's objectives relating to internal control are achieved. Through effective monitoring, F-Secure can identify and correct internal control problems on a timely basis, produce more accurate and reliable information for use in decision-making, and prepare accurate and timely financial and sustainability statements.

Internal control monitoring in F-Secure consists of the following interlinked components:

- Annual risk assessment
- Catalogue updates and gap follow-up
- Internal control self-assessments
- Internal control reporting

Sustainability-related risks are managed as part of F-Secure's risk management process and in alignment with F-Secure's Risk management policy. The primary goal of F-Secure's risk management policy is to enable the organization to identify, prioritize and manage risks more effectively. This includes having

- Established risk acceptance criteria and when risk assessment should be performed
- Systematic means to collect, analyze and learn from risks

- A clear understanding of roles and responsibilities regarding risk management
- Continuous, systematic and structured means to identify, analyze, evaluate the impact of, monitor, and control risks including
 - assessing and scoring risks based on impact, probability (likelihood) and overall risk level
 - creating a risk matrix, where high-impact quadrant risks are prioritized for company-level mitigation planning
 - evaluating different time horizons and taking into consideration the severity of the impact and probability
 - evaluating risks against risk acceptance criteria and prioritizing risks for risk treatment

Main risks, mitigation plans and controls

F-Secure has analyzed the risks for each material topic including sub and sub-sub-topics as part of updating our Double Materiality Assessment at the beginning of 2024. The risks have been reviewed by the ESG Council and integrated into the company's risk assessment process. Table 2 presents F-Secure's main risks, both potential and actual, and their mitigation strategies, including internal controls.

GOV-5 The main risks identified

The main risks identified	Management and mitigation	Controls and tracking
Environment		
Fail to meet level of climate change reduction ambition and reporting requirements from partner or investor point of view	Annual stakeholder surveys to ensure level of ambition is sufficient Review transition risks and mitigation roadmap	Review stakeholder feedback and compare with F-Secure ambition level
Social		
Loss of key persons or inability to acquire new talent	Part of Leadership Team monthly reporting meeting agenda Analysis of critical strategic competences Improving talent acquisition process	Number of people leaving F-Secure rising in comparison to previous year
Partner retention and acquisition related to DEI requirements	Establishment of DEI Committee Setting DEI targets for both gender, nationality and age	Review stakeholder feedback and compare with F-Secure ambition level
Consumer willingness to pay	Willingness to pay is verified annually by Product organization through a global survey F-Secure Total ARPU development is tracked by both Product and Sales organization.	Input from consumer survey Direct business ARPU decrees
Significant agreement changes or loss of a major Service Provider account, or Direct Business decline	New wins tracked and reported by Sales organization Loss analysis is done for major accounts as account losses are not a regular occurrence due to long contract lifetimes	Track number of wins/losses
Create, deliver and maintain Tier 1 partnerships in a profitable way	Transforming the Company and its operating model with its growth strategy For major embedded security opportunities and as per F-Secure process a bid review is organized	Track embedded security contribution margin
Security of vendors and partners	Dependency on suppliers and partners may increase our vulnerabilities.	Reported major security incidents
Cyber security attacks negatively impact reputation and business	Public security incident announcements follow the F-Secure Security Incident Management Procedure As part of the procedure each security incident is categorized per severity and if deemed major and requiring public communications	Reported major security incidents
Workload and wellbeing	eNPS results from Fellow survey regarding workload and wellbeing	eNPS level
Governance		
Risk of bribery or corruption: Partnership business, use of agents and other intermediaries	Code of conduct training conducted by 98% of personnel (valid for two years)	Training completion level
Detection of bribery and corruption	Global banking system stops any suspicious transactions and each case is investigated by finance team	Control part of overall financial processes

Table 2. The main risks identified.

Integration of risk assessment and controls with company processes

The purpose of internal control is to ensure that operations are effective and aligned with the strategy and that sustainability reporting and management information is reliable and in compliance with applicable regulations and operating principles.

Internal control consists of applicable guidelines, policies, processes, practices, and relevant information about the organizational structure that helps ensure that the sustainability reporting complies with applicable regulations. The purpose of internal control is also to ensure that the sustainability information provides a true and accurate reflection of the activities and sustainability status of the company.

The company regularly monitors its key sustainability-related processes and metrics linked to, for example, environment, employees, consumer and partner satisfaction, cyber security, and Code of Conduct. If any inconsistencies appear, the issues are handled without delay. The company's Corporate Development function is responsible for the consistency and reliability of internal control methods. The Corporate Development team in tandem with the ESG Council works in close cooperation with businesses, providing relevant data to support and drive sustainability actions within the company. As this is the first year of sustainability reporting, the team will regularly assess and monitor the reliability of the reporting and target setting moving to 2025.

Furthermore, every employee at F-Secure is responsible for risk management activities. Therefore, each function runs a continuous risk management process to identify new risks and ensure mitigation activities are progressing as planned, and an owner has been defined for each risk. Risk assessment, including mitigation plan reviews, is carried out monthly or at least once a quarter in each function.

Material risks identified through the risk management process are regularly reviewed by the CEO and the Leadership Team. The Leadership Team reviews risks at a minimum bi-annually. The Audit Committee regularly conducts a review of top operational risks, inc. cyber risks, at a minimum of 1–2 times annually. The ESG governance, in conjunction with the risk management policy and internal controls, ensures that the relevant internal functions remain aware of the topics and that actions are taken effectively, and progress is monitored.

Strategy

SBM-1 Strategy, business model and value chain

Product and services offering

F-Secure offers holistic, engaging and easy-to-use cyber security products and services to consumers to protect their digital moments. This includes our Security Suite offering (F-Secure Total), an all-in-one app, including end-point security, scam protection, privacy protection, password management, and identity protection. Notable new protection capabilities launched during 2024 focused especially on protecting consumers against various scams.

Our Embedded Security capabilities – software development kits, application programming interfaces and browser plug-ins – protect consumers’ digital moments typically by embedding cyber security capabilities into our partners’ apps, devices and services that consumers already have and know how to use, without the need to install a separate security application. Embedded Security solutions can also be used to create entirely new, custom security applications to meet the requirements of service providers looking to create a unique security experience of their own.

In addition, we offer our Service Provider partners a wide range of Customer Engagement Services to support their go-to-market activities such as Marketing & Sales Enablement, and Lifecycle Messaging Services. Combined with our cloud-based Security Business Platform that provides self-service capabilities for partners’ app developers, sales & marketing, and customer care teams we can deliver successful business outcomes with security services to our partners.

Markets and customer groups served

F-Secure’s end-customers are consumers, who are worried about their online security, looking for a holistic, easy-to-use security solution that addresses today’s threat landscape and thereby a sense of security. We serve all consumers directly and indirectly via a global network of 200+ Service Provider partners including communication service providers, retailers, banks, and insurance companies.

We’re a partner-first company, which is also visible in our 2024 revenue split which is 81% through our partners and 19% directly. In terms of geographical regions, the revenue splits between Europe, North America and the Rest of the World (mainly APAC and Japan) as highlighted in Table 3.

Regions	2024 Revenue
Nordic countries	42.0
Rest of Europe	48.1
North America	45.5
Rest of the world	10.6
Total	146.3

Table 3. Revenues per region.

The ESRS sector to which F-Secure belongs is Technology - Software & IT Services. F-Secure’s revenue 2024 is 146.3 M€. Our operations and profitability are reported as a single operating segment, which is consistent with internal reporting and the way that operative decisions and assessment of performance are made by F-Secure’s Leadership Team. Since F-Secure Group only has one operating segment, there is also only one reportable segment.

Country	Headcount
Denmark	2
Finland	270
France	5
Germany	5
India	70
Italy	1
Japan	5
Malaysia	74
Netherlands	7
Norway	1
Poland	15
Slovakia	19
Spain	2
Sweden	7
United Kingdom	13
United States of America	33
Grand Total	529

Table 4. Headcount per country.

Sustainability-related goals

We believe that understanding human behavior first is fundamental to effective security, which is why delivering experiences is the cornerstone of our innovation. Our solutions are designed for all consumers across age groups on their terms: an individually personalized and contextually relevant trusted companion protecting consumers in moments when it really matters.

Therefore, we've moved away from providing point solutions like separate End-Point Protection or VPN apps and now offer an all-in-one consumer security application or

embed protection capabilities as part of our partners' apps or services as described earlier in this section. This portfolio strategy and focus on "brilliantly simple security and customer experiences" allows us to protect consumers' digital moments and continuously improve our product satisfaction scores (Net Promoter Score, NPS), which are critical sustainability-related goals to F-Secure.

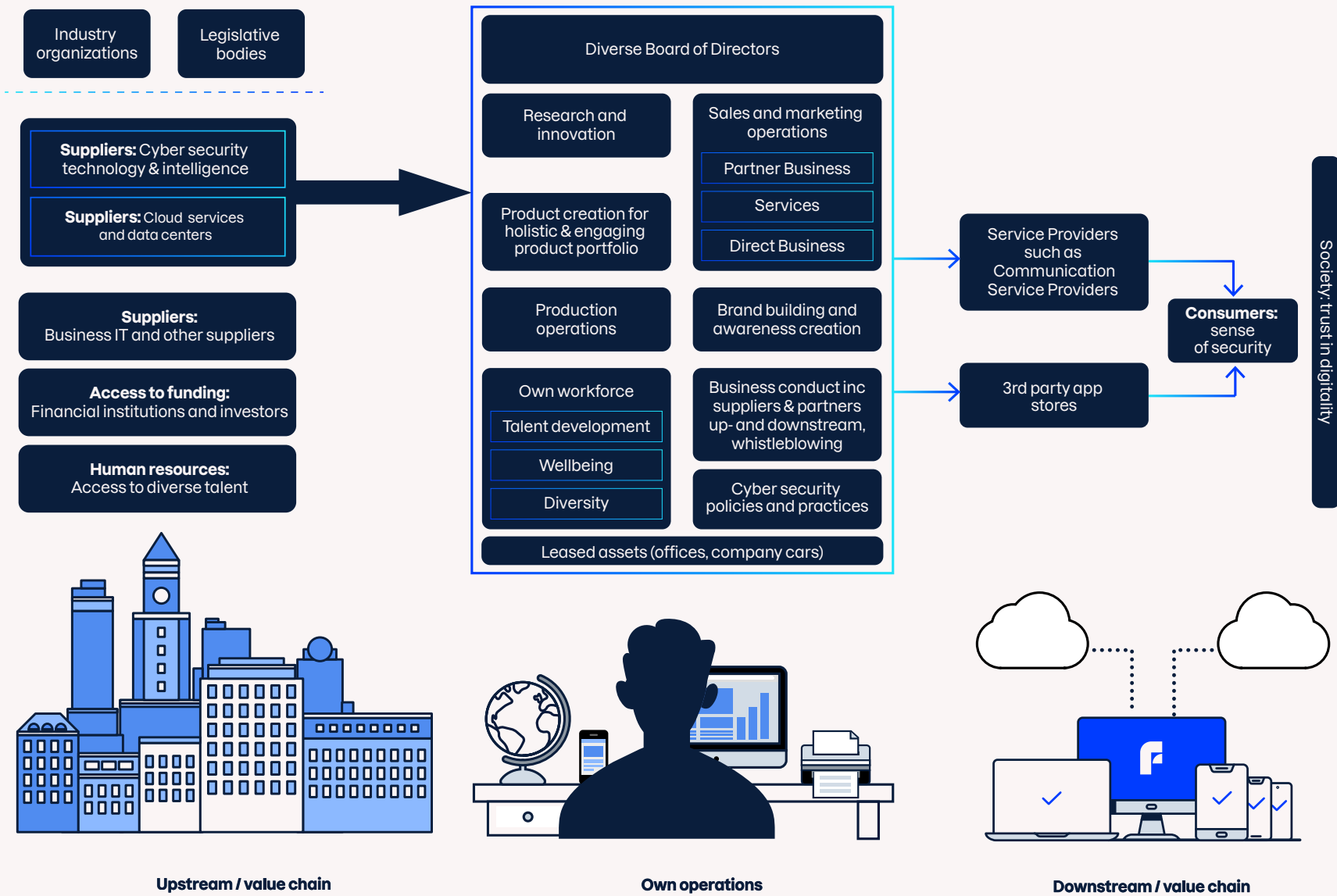
Furthermore, to realize our purpose of making every digital moment more secure for everyone, our go-to-market model is primarily channel-based and through Service Providers allows us to reach hundreds of millions of consumers behind these partners in our focus regions in Europe, North America and APAC/Japan. Additionally, after the acquisition of Lookout Life in 2023 we've expanded our offering to new partner segments, namely the world's largest Communication Service Providers ("Tier 1s"). With this in mind, during 2024 we've further invested in serving such partners, including service delivery, partner support and meeting other Tier 1-related contractual commitments.

F-Secure's channel model emphasizes the importance of win-win relationships measured both in terms of revenue and partner satisfaction while ensuring we do so with the highest business ethics and conduct. Measuring our partner satisfaction is another critical sustainability-related goal to realize our purpose and protect consumers' digital moments as described in more detail in the chapter "Consumers and End-users".

Business model and value chain

Our business model is based on delivering subscription-based consumer cyber security software products and services directly through our own e-com activities and app stores, as well as through our channel partners such as Communication Service Providers and financial institutions (banks or insurers). Our high-level value chain, including notable actors, operations and stakeholders are visualized in *the Value Chain and Actors* figure below.

Figure 2. F-Secure Value Chain.



The most notable inputs (upstream) supporting our business include:

1. Securing the right talent: Expertise in the cyber security industry is scarce and highly sought after. It's critical to build a strong employer value proposition, hire diverse new talent and help them reach their full potential at F-Secure.
2. Access to cyber security technology and threat intelligence: As is common in the cyber security industry, protection is a combination of own core protection capabilities complemented by 3rd party solutions such as threat intelligence. F-Secure always evaluates whether a particular protection functionality is core to our strategy and if we should make it, buy it or partner around it.
3. Industry organizations: We work, for example, with Amtso, Coalition Against Stalkerware, Internet Watch Foundation and GASA, as well as with academia such as Aalto University to increase cyber security awareness.
4. Suppliers: F-Secure is a cloud-based company and works with various suppliers and partners. This includes suppliers to our production environment, business IT, CRM, finance, and other related business systems.
5. Financial institutions: The market where we operate, and our recurring subscription-based business model provides the opportunity for F-Secure to grow profitably. This in turn gives us credibility with financial institutions and investors. All combined makes it possible to pay dividends to our shareholders and drive growth that can positively impact our share price, while strong cash flow allows us to manage our debt and supports future potential M&A activity.
6. For legislative purposes and as a listed company, we continue to track and evaluate regulatory impacts on F-Secure operations across our regions. This includes, for example, evolving ESG regulation, legislation on the use of AI and data privacy.

Our material own operations consist of the below activities and actors:

1. Product creation and related operations: Product management functions lead the creation of a compelling and differentiating portfolio vision, offering and roadmap. Our R&D function implements roadmaps and also drives security research and innovation agenda to stay ahead of the threat landscape evolution.
2. Sales and marketing: Service Provider channel is F-Secure's primary go-to-market model where partners promote and sell security services and support their end-customers (consumers). F-Secure has a dedicated partner sales organization that focuses solely on driving sales through Service Providers.
3. Sales and marketing: Direct channel provides us with direct access to consumers in our focus regions and a source of revenue but also critical insights into what

resonates with consumers in terms of the product offering, value proposition and pricing.

4. Services organization supports both our direct and partner channel activities in terms of delivery, customer care and providing a wide range of partner success services that help our partners grow their security business.
5. F-Secure's business is based on trust. All data needs are handled securely and respecting e.g. consumers' right to privacy. We ensure that our employees follow our Code of Conduct and take business ethics into account in all they do, including training on cyber security-related policies and activities.
6. Developing our own employees and hiring new talent is critical for F-Secure's growth. This also includes how we maintain and increase well-being and diversity at F-Secure to create a safe working environment where everyone can reach their full potential.
7. Business support: Finance, HR, legal, CISO, and Corporate Development provide business support activities to all functions such as support in hiring, accounting and financial reporting, invoicing, ensuring company-level cyber security, and support in strategy process and M&A activities.
8. The Board of Directors plays a crucial role in the governance of a company by providing strategic direction and oversight. The Board is responsible for approving the company's overall vision, strategy and long-term goals, and ensuring that management acts in the best interests of shareholders and other stakeholders. The Board also oversees financial performance, risk management, and compliance with legal and regulatory requirements. See the section on Governance for further information on the Board's role and responsibilities at F-Secure.

Through our strategy and business model, we deliver concrete outcomes and benefits to our key stakeholders as described above. See the section on "upstream" on our impact on investors and lenders.

Our material downstream operations consist of the below activities and actors:

1. We support our partners in selling and promoting cyber security services and deliver concrete business outcomes where security becomes a new core service. Consumer cyber security also has a positive impact on their other core businesses such as fiber or 5G broadband sales, increasing customer retention and overall relevancy of their brand in consumers' everyday lives.
2. App stores: In addition to our own e-Commerce platform, we make available and promote our services in Apple's and Google's app stores.

SBM-2 Interest and views of stakeholders

Through ongoing dialogue and engagement with our stakeholders, we strive to understand our stakeholder positions, requirements, concerns, and expectations in more detail. This continuous interaction provides input to our strategy and ESG-related policies, actions, and processes, allowing us to align with the interests and views expressed by our stakeholders. The insights gained from these continuous dialogues serve as the baseline for our due diligence processes and concluding the Double Materiality Assessment.

As described in more detail under General Information and the IRO-1 section, during the F-Secure Double Materiality Assessment, we've engaged in a dialogue with our key stakeholders to understand their expectations, including financial institutions (inc. analysts, investors, lenders), our own workforce, end-customers (consumers), the Board of Directors (via the Audit Committee), and channel partners. In addition, we analyzed selected suppliers and regulatory compliance. F-Secure has conducted several different surveys that have helped identify material themes in these stakeholder groups. Finally, with selected Service Provider partners we've had 1:1 meetings to deep-dive into their sustainability-related needs and expectations, and we'll continue to do so in 2025. Please see Figure 3, F-Secure stakeholder map for further details.

SBM-2 Stakeholder map







	Stakeholder expectations	How engagement is organized	F-Secure actions and outcome from engagement in 2024
Investors and financial institutions 	Consistent growth and progression Clear and attainable goals Transparency in sustainability reporting Good Business conducts and data protection Ability to pay, liquidity	ESG surveys, calls and emails ESG ratings Capital market day Regular meetings with banks and analysts	Renewing relevant ESG ratings ESG investor webpages available
Employees (Fellows) 	Caring employer Securing retention and incentivizing compensation Opportunities for professional development Good business ethics and capability to protect our customers Global DEI agenda	Employee surveys Personal development dialogues DEI Committee and Health, Wellbeing and Culture Committee Employee-elected board member Townhalls and trainings	ESG training, including code of conduct and cybersecurity DEI Policy development Increase internal ESG communication Improvement of personal development dialogues Learning and development policy development Update requirement process Launch of Culture, wellbeing and health committee
Partners 	Securing digital moments, together Reducing GHG emissions Good margins and shared values Reporting and targets on relevant ESG topics ESG policies aligned with partners policies	Partner survey and discussions Engagement with Sales ESG ratings	Renewing relevant ESG ratings Improvement on reporting ESG webpages available ESG training of sales improving dialogue with partners Launch of Environment committee
Consumers 	High level of protection for good price Understanding customer needs Knowledge about cybercrime Reliable and simple solution	Customer support and guidance Surveys	Product improvements ESG webpages available Increase cybersecurity awareness through campaigns
Policymakers and regulators 	Regulatory compliance Transparency in sustainability reporting Addressing ESG Risks and opportunities	Answering public consultations Participating in feedback rounds concerning new regulations and legislations	Further aligning business strategy with ESG requirements Value creation and risk mitigation ESG targets developed
Suppliers 	Favorable payment terms Good business ethics and conduct Climate change and human rights Trust and transparency	Cybersecurity examination of suppliers conducted by CISO office Basic supplier onboarding process Basic review of main suppliers ESG priorities	Development of supplier code of conduct covering main ESG topics

Figure 3. F-Secure stakeholder map.

While the outcome of the DMA did not result in material changes in our strategy or business model, we expect the relationship with some of the stakeholders to further strengthen through regular dialogue and complementary ESG agendas, especially our Service Provider partners. We also aim to build on the trust placed in us by continuing to act in a transparent way and following through on our goals. In addition, the standardization of measures will create more common metrics and activities which may serve as a further catalyst for collaboration with our stakeholders.

Informing internal stakeholders on stakeholder interests

Stakeholder feedback has also been presented to the management, administration and supervisory bodies as part of the DMA. F-Secure will continue to consider stakeholder feedback as part of our risk management process and annual strategy reviews. Our ESG Council will continue to review and update DMA and IROs regularly, and the management, administration and supervisory bodies will be informed if there are any significant changes in stakeholder feedback, or new potential or actual impacts are emerging affecting the strategy and business model.

Consumer interests

For clarity, within the context of this Sustainability Statement, terms “consumer” and “end-user” should be treated as synonyms unless explicitly stated otherwise.

Related to consumer interests, views and rights, F-Secure is in the business of protecting consumers against online threats and it is critical to understand consumer needs and concerns around cyber security. F-Secure conducts regular consumer and market surveys to ensure its product and protection roadmaps are aligned with consumer needs. As an example, F-Secure recognized consumer's right to privacy online and implemented a consumer VPN offering several years ago.

Additionally, several other channels serve as input to our product management processes and developing new protection capabilities, such as our own customer care operations or feedback from our Service Providers like Communication Service Providers. Equally important is to have in-depth views of how the threat landscape evolves to provide effective protection to consumers and educate consumers on surfacing threats. Our promise is to provide frictionless user experiences, which means we also involve our end-customers in product usability and accessibility testing.

The above market studies and consumer insights not only allow F-Secure to ensure its product strategy addresses real and relevant consumer needs in an

elegant and simplified manner but also serve as input to our channel strategy. According to consumer feedback, approximately 81% of consumers expect internet service providers to provide security services, which has influenced our channel strategy. Furthermore, consumers find cyber security complicated, which is one of the reasons we're now embedding security as part of our partner's existing app or services so there is no need for a consumer to download and learn a new application.

Finally, we are continuously monitoring evolving legislation in our key markets that impact consumers. This includes, for example, EU GDPR and its impacts on the extent we collect consumer data and how it is processed at F-Secure.

Own Workforce interests

F-Secure has involved its workforce when conducting the Double Materiality Assessment and defining IROs. Additionally, we regularly gauge our employees' well-being and obtain their feedback on current events and company strategy, for example. These results are reviewed also by the Leadership Team and each function to drive related actions (where needed). Furthermore, we

- Ensure that we work according to our Code of Conduct, which includes respecting human rights
- Actively communicate company direction and priorities. This allows every employee to understand how their roles contribute to the broader company goals, thus making them feel connected to the company's direction
- Emphasize F-Secure's cultural values and how things are done at F-Secure to encourage employees to align their actions with shared values. Values are also used as part of our performance management (“how” things got done in addition to “what”).

Value chain workers' interests

F-Secure is committed to respecting the human rights of its value chain workers and takes actions to ensure fair labor practices, safe working conditions, and the right to freedom of association and collective bargaining. F-Secure has a supplier Code of Conduct and agreements with certain partners, which seek to ensure that they meet the company's standards for responsible business conduct, including the treatment of their workers.

SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model

F-Secure has identified several actual positive impacts related to social sustainability, which is closely linked to our strategy and business model. Through our actions and the portfolio of consumer cyber security products and services, we protect people against cyber security threats. Additionally, we make free tools and educational information about the threats available to everyone, helping raise awareness of cyber threats in society at large.

Additionally, we focus on the well-being of our employees, providing equal treatment and opportunities for professional development. Through these activities, we have an actual positive impact on our workforce and support them to be the best professionals they can be. We encourage our employees to speak up, which is also enforced by our recently renewed culture and through our whistleblower channel where any business conduct matter can be raised without fear of retribution.

Related to the environmental topic we see that there is a potential positive impact to be had in the future, which is linked to green coding practices. While we today deploy our solutions in climate-neutral platforms like AWS, we see the use of AI becoming more widespread, and as we protect more consumers, more energy will be needed to run our products, emphasizing the need for green coding and similar practices.

Environment

Potential positive impact (OO)

- Implementation of green coding principles and practices can reduce battery use in consumer devices or computational power needed in a cloud environment

Social

Actual positive impact (OO)

- Protect consumers' digital moments by providing relevant, effective, engaging and easy-to-use cyber security solutions against modern cyber threats directly and through partners
- Create awareness about cybercrimes: Increase consumer awareness about cyber security and cybercrime through marketing campaigns, events, free tools, and content

- Number of annual holidays: We offer more days off than some countries require, such as the US
- Promoting gender equality: Recruit and advance women and under-represented groups, mitigate the gender pay gap
- Inclusive culture with a speak-up culture: Ensure that we have an inclusive culture where the workplace is a safe environment for everyone through our company culture. We foster a speak-up culture ("dare to care").

Governance

Actual positive impact (OO)

- Whistleblower channel available: Protection of whistleblowers encourages and enables all stakeholders to speak up. F-Secure has a whistleblower channel available to all our employees and business partners. Internal awareness is raised about it in mandatory training internally.

We've additionally identified Risks and Opportunities as per the Double Materiality Assessment as described in the IRO-1 section and covered in more detail in the topic-specific sections.

Environment-related risks and opportunities

- RISK: Failure to meet climate change mitigation targets (OO) may have a negative impact on our channel business as some Service Providers expect meeting the 42% CO2 reduction target
- OPPORTUNITY: Continue to enforce policy regarding e- and hybrid leasing vehicles Continue to enforce our policy for e-vehicles over time to reduce our CO2 emissions (OO)

Social-related risks and opportunities

- OPPORTUNITY: Protecting consumers against the evolving threat landscape is seen as an opportunity (VC) for both F-Secure and our channel partners as scams continue to become more widely spread and consumers are seeking solutions to stay protected.
- OPPORTUNITY: Use data and AI in security applications to provide more effective protection against online threats and improve the user experience (OO)

- OPPORTUNITY: Identifying critical strategic competencies that are needed for our long-term success (OO) with related opportunities in providing learning and development opportunities to our employees (OO)
- OPPORTUNITY: Expand the use of worktime tracking on the EU level (OO)
- OPPORTUNITY: Employer reputation: Improving the employer brand image can attract especially younger generations through DEI activities (OO). On the other hand, there may be a RISK that our DEI activities are not sufficient, especially for major Service Providers with extensive DEI requirements (VC)
- RISK: F-Secure's go-to-market model is primarily based on channel sales and a significant agreement change or existing partner loss can negatively impact our future outlook
- RISK: Tier 1 partnerships: To drive growth, F-Secure works with the world's largest Service Providers and we may be unable to create and deliver solutions to these partners with sufficient profitability levels or meet extensive contractual obligations
- RISK: Consumer willingness to pay: Intensifying competition and a negative macro-economic situation may hurt consumer willingness to pay for premium security (VC)
- RISK: Failure in talent acquisition and retention (OO)
- RISK: Security of suppliers and partners: As is customary in the cyber security industry we work with several suppliers and partners and the reliance on these suppliers or partners may subject us to vulnerabilities (OO)
- RISK: Cyber security: We may become targets of a cyber security attack negatively impacting our reputation and business (OO)
- RISK: Workload and mental well-being: We acknowledge our industry is demanding for our employees and increasing workloads and negative impacts on mental well-being constitute a risk (OO)

Governance-related risks and opportunities

- OPPORTUNITY: F-Secure launched its new culture program in 2024 to support and accelerate our ESG agenda including the speak-up culture described above (OO)
- RISK: Partner business, use of agents and other intermediaries may increase the risk of bribery and corruption in cases where middlemen are used (VC)
- RISK: Bribery and corruption risks may rise as a result of M&A transactions due to limited understanding of the target (OO)

The positive impacts related to consumers and end-users are directly linked to F-Secure's business model and strategy. We are in the business of protecting consumers' digital moments against cyber threats directly and through our partners and doing this in a business-responsible manner with our employees.

F-Secure's ambition is to increase the positive impact further based on our growth strategy of protecting consumers' digital moments while increasing reach and scale through our Service Provider partners. These partners that generate most of F-Secure's revenue continue to see protecting their end-customers as a major part of their brand promise and a business opportunity as a new core service. Together with our partners, we can expand the reach and adoption of security in our key markets among consumers, which, in turn, enables us to increase our actual positive impacts further over time.

Similarly, other potential or actual impacts related to green coding (lower electricity use in end-user devices and cloud), only leasing electric vehicles reducing CO2 emissions, activities around employee well-being, such as more holidays than mandatory, our inclusive corporate culture encouraging speaking up and not tolerating any harassment, and anonymous whistleblowing channel related impacts are directly related to F-Secure's strategy and business model.

The positive social sustainability- and governance-related impacts have already materialized, and we see them having an increasingly positive impact also in the long term, as well as per company strategy and priorities. The potential positive impacts related to green coding will grow over time and we expect an actual impact to materialize in the long term.

Effects of IROs on strategy and decision making

Our most material actual positive impact is related to *protecting consumers' digital moments* against online threats, increasing consumer trust in digitality and hence society. For consumers, this translates to peace of mind and psychological safety using digital services, in addition to protecting against financial losses. We already have this positive impact today based on our own operations directly and through our channel partners, and we expect it to remain our material impact also in the long term. Protecting consumers' digital moments continues to guide and inform the company strategy, decision making and execution, notably including

1. Allocating product and technology investments to provide relevant, engaging and effective protection capabilities to consumers against modern threats.

This also includes investments in innovation, threat research and research in consumer needs.

2. Ensuring that in our go-to-market model that is primarily channel sales driven, we can meet the needs of each partner segment operationally and through our product and services portfolio. This “fit to channel” and being a “partner-first” company further ensures we can reach a sizable number of consumers behind our partners whether providing an all-in-one consumer cyber security application, network security or SDK/API-based security solutions to our partners to protect their end-customers (consumers) and other partner-facing services that support their business growth. These in turn help mitigate the *risk of not meeting our Tier 1 partners' needs*.

When protecting consumers' digital moments, the *constantly evolving threat landscape* has been identified as a growth opportunity for F-Secure and our channel partners both in the short and long term. This is because scams have become commonplace and cybercriminals are switching to using AI to create more credible scams, such as fake online shops. Additionally, we see the *use of AI as an opportunity* for innovating new protection capabilities and improving customer experience.

To take advantage of these opportunities, our portfolio, customer experience and protection roadmaps are now focused on scam protection. This includes providing new protection capabilities such as messaging scam protection, where implementing AI capabilities provides effective protection and ensures an engaging user experience. We expect our scam protection focus to have a positive effect on our financial performance already today while supporting our long-term growth strategy as our offering becomes more attractive to consumers and our partners. Furthermore, providing relevant and engaging scam protection also helps address risks around *consumer willingness to pay for security* and a potential *loss of an existing partner*.

Additionally, protecting consumers' digital moments means supporting all consumers, whether they are using F-Secure's products or not. Therefore, we're both directly and through our channel partners having an actual positive impact while *increasing consumer awareness about cyber security and cybercrime*. Consumers are keen to learn about online threats and how to stay protected, and we address this need today by providing free tools, as well as engaging, digestible, easy-to-action content and communication through our experts that is relevant to consumers. These activities are having a positive impact on consumers already today and we plan to continue providing such services to consumers during our strategy period (2025-2027).

Our employees turn our vision and strategy into actions, and we've identified *opportunities to identify and develop strategic competencies* that are critical for our long-term competitiveness, especially in the cyber security industry where access to talent can be scarce. Related to this opportunity, attention has been put on our *learning and development initiatives*, including competencies across the company such as sales skills, product development and research, AI, and leadership development that supports living up to our culture, the daily work and the well-being of our employees.

We also believe we're making an actual positive impact on our work-life balance and well-being as we've decided to *offer more days off than some countries require*, such as the US, additionally supported by our plans to expand the *use of worktime tracking on the EU level*. Combined with developing strategic competencies and leadership development we can also reduce the risks related to workload and mental illnesses.

In addition to developing our workforce, hiring new talent is critical for our long-term success. *Employer reputation* and our employer brand image are crucial in these activities, especially when attracting the younger generations through DEI activities, which has influenced us to support activities such as Women in Tech.

Furthermore, by *promoting gender equality* and advancing women and under-represented groups as well as mitigating the gender pay gap we can directly make an actual positive impact on our employees. We've already made gender pay gap-related adjustments during 2024 and will continue to do so during our strategy period 2025-2027 and in the future, to the extent needed. Additionally, to support diversity and equality at F-Secure, in 2024 we've decided to define and launch *our new inclusive culture with a speak-up culture* to support our growth ambition, which directly has an actual positive impact creating an inclusive culture where the workplace is a safe environment for everyone. This includes our new values, defining wanted and unwanted behaviors, as well as leadership principles and Employee Value Proposition (EVP), all aligned with the company vision and feedback from our employees.

The impact of our new culture applies to all employees at F-Secure and we're seeing a positive impact in our employee NPS results already today and expect our culture to further develop and strengthen over the long term as this development is a journey. We believe these actions will help mitigate risks related to certain regions and *partner retention and acquisition related to Service Providers may have extensive DEI requirements*. Similarly, their combined effect helps mitigate the *risk of losing key people or not being able to acquire new talent*.

Trust is critical in the cyber security industry. Therefore, we recognize that there is a risk that *cyber security attacks negatively impact our reputation and business while working with external suppliers and partners can introduce layers of vulnerabilities*. This has led to the decision to improve our product-related vulnerability management processes and develop secure software, as well as overall protection against cyber attacks by successfully running and completing ISO27001 certification that further improved the maturity of our security practices across the company.

The majority of F-Secure's revenue originates from channel business, which may increase *risks of bribery and corruption* in cases where middlemen are used. Being a cyber security company, ethical business practices are critical for our success, hence we address these risks raising awareness and understanding of our Code of Conduct, anti-bribery, and supplier Code of Conduct-related topics. A similar risk potentially applies to future *M&A transactions* as understanding of the target can be limited and the risk will be addressed when topical and as part of the M&A Due Diligence process.

Additionally, through our *whistleblower channel*, we see a direct positive impact where the protection of whistleblowers encourages and enables all stakeholders to speak up. F-Secure has made whistleblower channels available to all employees and business partners, and internal awareness is raised through mandatory training. This ensures that any misconduct or risks can be raised without repercussions as discussed later in this statement. The whistleblowing channel has been available since the demerger from WithSecure in mid-2022 and continues to be available in the future as per our policies.

Related to climate change, F-Secure has a relatively small CO2 footprint being a software company but it is committed to the Paris Climate Change Agreement reduction target, which is also important to our stakeholders like Service Providers. Therefore, as our business is primarily channel-driven, should we *fail to reach our reduction target* it may negatively affect relationships, especially with those Service Providers who are committed to reducing emissions by 2030. With this in mind, F-Secure is mitigating the risk by developing reduction pathways across Scope 1–3 emissions with a special focus on engaging with our suppliers as described under the Climate Change section, in addition to the opportunity to switch *to electric or hybrid vehicles*, and expect these activities to continue until 2030 when the target has been reached and as described under the Climate Change reduction pathways section.

We also recognize that implementing *green coding principles and practices* can have a potential positive impact in the medium to long term as we can reduce the impact of our protection offering e.g. further optimizing the footprint in consumer devices and minimizing the impact on battery use, as well as improving cloud computing efficiency even if we run on top of carbon-neutral platforms like Amazon Web Services. These impacts would be directly originating from and related to F-Secure's operations and we expect to see the benefits materializing in the medium to long term.

Effects on F-Secure's financial position

Management has not recognized any sustainability-related material uncertainties related to our operations and for which there is a significant risk of a material adjustment within the current (2024) or next annual reporting period to the carrying amounts of assets and liabilities reported in the related financial statements. Material R&D related expenses to protect consumers are described in F-Secure's 2024 Board of Directors' Report.

Resilience addressing material IROs

F-Secure's strategy and business model are considered resilient to address material impacts and risks, and leverage opportunities as identified as part of our 2024 strategy process for the next strategy period (2025–2027), which is F-Secure's definition of the mid-term period (1–3 years). This included both qualitative and quantitative analysis, expert assessments and external consultation. Additionally, F-Secure is a highly profitable company with a strong cash flow, providing the ability to invest in our growth initiatives. Furthermore, our dynamic strategy process where we regularly assess our progress as opposite to an annual one-off corporate strategy planning project also provides the capability to rapidly react to market changes and new opportunities.

Overall, we see that the benefits from our positive impacts and opportunities outweigh the risks that we've identified further increasing our resilience. Most importantly, we continue to have an actual positive impact on consumers' everyday lives, protecting their digital moments, which is very much in demand according to our surveys. This is evidenced also by the fact that we operate in a large and growing consumer cyber security market. All combined, help mitigate risks related to competition and consumer willingness to pay for cyber security becoming lower.

We also see an opportunity to grow further based on the evolving threat landscape, especially providing scam protection. Therefore, during 2024, we've shifted our

research, technology and product creation-related investments to address this “scam pandemic”.

Our confidence in company resilience is further based on

1. Our business model is based on recurring subscriptions while our channel strategy further increases our resilience against risks and market disruptions as partners include security in their core offering
2. Our contracts with partners are typically long and should a contract end, there is typically a long tail of revenue generated for a period of time. This combined with building a compelling offering for our partners and building connections with our partners' C-level helps mitigate the risk of losing a partner.
3. We work with the world's largest Service Providers such as Communication Service Providers that have demanding requirements and addressing these needs increases our resilience across our entire business. We've also made significant changes to our operating model and investments to support such Tier 1 partners, ensuring we can win and support these partners.
4. We continue investing in our talent development, well-being and inclusive company culture to support our employees and our growth strategy, which helps mitigate risks related to attracting and retaining talent, and overall employee well-being

For resilience against climate change, refer to the Climate Change section for transition and physical-related risks.

Entity-specific IROs

F-Secure has identified some entity-specific impacts, risks and opportunities related to social topics, which is where F-Secure makes the largest contribution. The descriptions in the entity-specific section include contextual information and any assumptions made when calculating the measure or target. When developing entity-specific measures and targets F-Secure has considered how they can support reducing negative outcomes and increasing positive outcomes for people. The measures and targets have been developed for IROs where we have identified material impacts, risks or possibilities in the short, medium or long term that exceeds the threshold for financial impact (see the section IRO-1).

In short, and based on our double-materiality analysis, these entity-specific disclosure requirements apply to section S4 Consumers and End-Users, covering:

	Material impact, risk or opportunity	Description
Personal safety of consumers and/or end-users		
Security of a person - Protecting our customers		
Opportunity (OO)	Use of AI in security applications	AI-powered (network) monitoring tools can observe user behavior, detect anomalies, and react accordingly.
Opportunity (OO)	Evolving threat landscape	Scams have become more commonplace. Opportunities for F-Secure to offer engaging and relevant protection services.
Risk (OO)	Consumer willingness to pay	Intensifying competition and negative macro-economic situation may have negative impact on consumer willingness to pay.
Risk (VC)	Channel strategy	Significant agreement changes or loss of a major Service Provider account, or Direct Business decline
Risk (VC)	Tier 1 partnerships	F-Secure may be unable to create, deliver and maintain Tier 1 solutions with sufficient profitability levels (over time) inc. meeting support commitments
Actual positive impact (OO)	Protecting digital moments	According to our product questionnaire our consumers are worried about their online protection. F-Secure provides solution to these threats through its offering.
Risk (VC)	Security of vendors and partners	The reliance on external vendors, especially vendors who are one step removed in the supply chain, adds layers of vulnerability.
Risk (OO)	Cyber security	Cyber security attacks negatively impact reputation and business
Health and safety		
No IROs identified.		
Protection of children		
No IROs identified.		

	Material impact, risk or opportunity	Description
Social inclusion of consumers and/or end-users		
Non-discrimination		
No IROs identified.		
Access to products and services		
No IROs identified.		
Responsible marketing practices		
No IROs identified.		
Information-related impacts for consumers and/or end-users		
Privacy		
No IROs identified.		
Freedom of expression		
No IROs identified.		
Access to (quality) information (Awareness and education)		
Actual positive impact (VC)	Create awareness about cybercrimes	Increase the consumers awareness about cybersecurity and cybercrime through marketing campaigns and events.

Table. 5 Entity-specific IROs.

Impact, risk and opportunity management

IRO-1 Identify and assess material impacts, risks and opportunities

F-Secure completed its first Double Materiality Assessment (DMA) in November 2022 and in 2023–2024 further refined its DMA process and methodology, aligning them with the final version of the European Sustainability Reporting Standards and EFRAG guidance, which resulted in an updated view of material topics, sub-topics, and IROs.

When assessing sustainability matters, the following principles and approaches were applied:

1. ESG matters assessed were selected based on EFRAG sustainability standards while SFRD and NFI regulations were also reviewed
2. Sector and entity-specific disclosure topics were assessed whenever identified as relevant, for example related to cyber security
3. The assessment was conducted as double materiality, considering sustainability matters' impacts on F-Secure and F-Secure's impacts on sustainability matters
4. Assessment of IROs was based on appropriate quantitative and/or qualitative thresholds
5. Engagement with affected stakeholders was conducted and inputs were used to inform the materiality assessment process
6. Acknowledge that cross-cutting matters are to be reported irrespective of the outcome of the materiality assessment, and a topic was considered material if an impact, risk or opportunity was identified that exceeded the thresholds

The critical input for the assessment has been dialogue with our key stakeholders to understand their material needs and topics. During the process, F-Secure has engaged with its Service Provider partners, investors and bankers, own workforce as well as consumers and taken into account requirements from its suppliers and regulators as described under 1.3.2 SBM-2 Interest and views of stakeholders.

To complete the analysis, we applied guidance available from EFRAG, combined with our own and 3rd party sustainability expert interpretation of the standards, and developed an assessment process and scoring matrices allowing us to identify the material sustainability matters as shown in the Table 6, *Material ESG topics*.

IRO-1 Material ESG topics

Topic	Sub-topic	Materiality
Environment		
	Climate change adaptation	No
Climate change	Climate change mitigation	Yes
	Energy	No
Social		
	Working conditions	Yes
Own workforce	Equal treatment and opportunities for all	Yes
	Other work-related rights	No
	Information-related impacts for consumers and/or end-users	Yes
Consumers and end-users	Personal safety of consumers and/or end users	Yes
	Social inclusion of consumers and/or end users	No
Governance		
	Corporate culture	Yes
	Protection of whistle blowers	Yes
Business conduct	Animal welfare	No
	Political engagement	No
	Management of relationships with suppliers including payment practices	No
	Corruption and bribery	Yes

Table 6. Material ESG Topics.

When conducting the materiality assessment F-Secure as a software-based company has not identified any pollution, water or marine resource, biodiversity and ecosystem or resource use and circular economy-related impacts, risks or opportunities. Furthermore, as F-Secure does not have physical product manufacturing, pollution from the value chain is considered small, and resource use and the circular economy are irrelevant. F-Secure has a recycling policy in place covering the whole organization's waste. However, no impacts, risks or opportunities were identified, which would make resource use and circular economy material.

F-Secure does not have operations or sites in or near biodiversity-sensitive areas which could lead to deterioration of natural habitats and disturbance of species in protected areas or affect threatened species. F-Secure has not identified any activities that would have a negative impact related to land degradation,

desertification or soil sealing. See a more detailed approach to the process later in this chapter.

When assessing IROs, we applied guidance available from EFRAG, combined with our own and 3rd party sustainability expert interpretations of the standards, and developed an assessment process and scoring matrices allowing us to identify material impacts, risks and opportunities. Results were reviewed with the F-Secure Leadership Team members and ESG Council.

We focus on areas where impacts, risks and opportunities are deemed likely to arise, based on the nature of the activities, business relationships, geographies, or other factors concerned. Indication whether the impacts and risks are in our own operations (OO) or value chain (VC) is illustrated in the tables under each topic. We also indicate whether our impacts are positive or negative. The risk management, including negative impacts, is conducted in accordance with F-Secure's Risk management policy and as part of F-Secure's risk review. In addition to assessing risks and negative impacts, positive impacts and opportunities are also embedded into the strategy process including all material sustainability matters.

Material impacts, risks and opportunities were considered material if one or more of the following thresholds were exceeded: Strong stakeholder request, exceedance of financial impact, scope and scale of event impact global and/or severe and/or irremediable in nature as well as likelihood. The Table 7, *Description of assessment methodology* contains the threshold values for scope, scale and financial impact. A topic was considered material if it scored '3' in any category or met the financial impact threshold. Additionally, whenever relevant, studies about global risks and megatrends were utilized to assess further material topics.

IRO-1 Thresholds

Scope	Scale	Financial impact
1 = Impact on group of people which is relatively small in the context of company's value chain, or impact on local natural area	1 = Impact with short-term effects which may be either negative or positive. Impacts are temporary in nature.	Financial impact (revenue threshold 5 % of revenue, costs threshold 3% of business costs and EBIT-margin threshold 2%)
2 = Impact on a community, several groups of people, region or broader natural area	2 = Impact with medium-term effects which might be either negative or positive. Impacts are temporary in nature but to recover there needs to be investments or programs to remediate the negative impacts. In case of positive impacts, beneficiary can benefit from the impact relatively long time	
3 = Impact on a global or multiregional scale on nature, people or society	3 = Impact is severe and either positive or negative. Either large groups of people, nature or larger communities are impacted or can benefit from the impact. Impact is long-term in nature and benefits are replacing inefficient existing processes or negative existing impacts with significant potential to improve the lives of people and/or the planet.	

Table 7. Description of assessment methodology.

IROs related to climate change issues

In line with the Disclosure Requirement ESRS E1-6 and F-Secure Double Materiality Assessment the following impacts, risks and opportunities have been identified.

	Material impact, risk or opportunity	Description
Climate change mitigation		
Opportunity (OO)	Set policy for e-cars	F-Secure has a small number of leasing cars in Finland, however the amount will rise over time (taken in consideration F-Secure growth target)
Risk (OO)	Fail to meet mitigation targets or not enough ambition. F-Secure emission reduction heavily reliant on suppliers.	Investing and finance linked to ESG ambition and targets of the company. Some partners not willing to continue business if not sufficient climate ambition.
Potential positive impact (OO)	Implementation of green coding principles	Through implementing green coding, we can reduce the impact of our end-product. Including optimizing device performance, battery use and cloud computing.
Energy		
No significant IROs identified		
Climate change adaptation		
No significant IROs identified		

Table 8. Climate IROs list.

The process involved collecting and evaluating GHG emissions across all scopes, using scenario analysis, and integrating findings into strategic planning while regular monitoring and reporting will ensure transparency and accountability.

F-Secure has also applied climate-related scenario analysis and their assessment of transition risks and opportunities are disclosed in the Climate Change section.

Climate-related physical risks in own operations or in the value chain

No significant physical risks were identified related to climate in own operations or value chain and no assets were identified in high-risk regions or there are sufficient guardrails in place like geographical redundancies. The physical risks were not seen as material as they are unlikely for the majority of employees and do not pass the threshold for materiality.

Climate-related transition risks and opportunities in own operations and in the value chain

Through climate-related scenario analysis, the only material risk identified is a transition risk related to reputation. This risk would materialize if F-Secure fails to meet mitigation targets aligned with the Paris Agreement, affecting stakeholders' expectations. Over 90% of F-Secure's emissions are from Scope 3 categories, making emission reduction heavily dependent on the supply chain.

A transition plan with mitigation actions is in place, and no significant negative impacts have been identified. Continuous monitoring and methodology development are essential to capture climate risks accurately. The only opportunity identified is setting a car policy on hybrid and e-vehicles, which could reduce Scope 1 emissions. Also, by 2030 we expect a shift to an all-electric vehicles policy.

Climate-related transition events

F-Secure has identified several key transition events that could impact its operations and value chain by considering scenarios that limit global warming to 1.5°C. Driving forces are mostly external to F-Secure and will affect both F-Secure and its stakeholders with negative impacts. The driving forces identified in F-Secure's climate change scenario analysis have been identified below.

Social & Reputation	Technology	Economic	Market & Environment	Political
Increased stakeholder concerns	Green coding and substitution of existing services with lower emission options	Macroeconomic trend Economic loss due to not reaching climate goals or not having sufficient targets in place	Transition to green energy and electrical cars	Enhanced emissions-reporting obligations Increased pricing of GHG emissions

Table 9. Key transition events.

Assets and business activities that may be exposed to climate-related transition events

The following drivers may expose F-Secure to climate-related transition events:

Social & Reputation: F-Secure may need to validate its GHG reduction target through SBTi or similar framework due to stakeholder concerns and partner requests. Setting a climate neutrality target is also likely in the short to medium term.

Technological: A significant portion of F-Secure's emissions come from purchased goods and services. Larger suppliers are expected to provide better emission data and reduce emissions. An in-depth analysis of smaller suppliers will likely lead to an emission reduction plan, and data improvements and supplier emission reductions are anticipated over the next decade.

Economic: The inability to address the climate change topic may lead to F-Secure facing some economic losses assuming sufficient climate targets are not set and reached as per stakeholder expectations. There may be fines in the medium or long term if such targets are not met.

Market & Environment: By 2030 for Scope 1&2 emissions it is medium-likely that the transition to green energy is possible in all F-Secure offices and that all leased cars are electric. F-Secure will apply green energy as a requirement for new office spaces and request changes in the current locations, where feasible. By 2050 for scope 1&2 emissions it is highly likely that the transition to green energy is possible in all F-Secure offices.

Political/Policy/Legislation: Climate change policy and legislation is one of the main drivers for companies to assess and reduce their climate-related impacts. F-Secure will continue to monitor policy changes and react accordingly.

Process to identify material IROs relative to business conduct matters

F-Secure is focused on areas where impacts, risks and opportunities are deemed likely to arise, based on the nature of the activities, business relationships, geographies, or other factors concerned. The business conduct assessment was conducted on a global level and when assessing the impacts, risks and opportunities we also considered special circumstances such as M&As. The assessment was conducted on sub-topics level, and we indicate in our statement whether the impacts and risks are in our own operations (OO) or value chain (VC). We also show whether our impacts are positive or negative.

F-Secure is operating with large international partners with clear business codes of ethics and practices decreasing the risk of any anti-business conduct behavior. As F-Secure's operations are global, there are countries in which F-Secure has operations and where risks related to corruption and fraud are elevated.

To estimate and understand the risks in the value chain, F-Secure has considered various aspects and operations and their risks of and related magnitude of any unethical behavior. In case any event would take place, it is still estimated to have a rather insignificant financial impact on F-Secure in the long term and would rather be short term and local in nature, with a low likelihood of happening.

Stakeholder feedback was also considered in the assessment. Business ethics are essential for attracting investors and retaining partners, in addition, ethical practices create a positive and productive workplace. This is reflected in the stakeholder surveys and the level of importance the stakeholders place on the topic.

F-Secure impacts on people and the environment

Through analyzing F-Secure's business model and strategy, discussions with leadership and different functions, reviewing already existing company risks, and reaching out to stakeholders for input we were able to create an understanding of where we might have a heightened risk of adverse impacts.

As a result of the analysis, no adverse impacts have been recognized, however we have recognized risks that might lead to adverse impacts if realized. The impacts have not been included in the materiality analysis as the likelihood that these risks would materialize is more unlikely than likely. Assessment and prioritization of risks were made based on the threshold set for determining materiality as described in the Table *Description of assessment methodology*.

During the process of identifying and assessing physical risks, F-Secure has considered climate-related hazards and screened whether its assets or business activities may be exposed to these hazards.

F-Secure applied the same method for identifying and prioritizing material impacts for reporting purposes as for risks and opportunities. An impact was considered material once one or more of the following thresholds were exceeded. See the Table *Description of assessment methodology* presented earlier that contains the threshold values for scope, scale and financial impact.

Positive impacts have not been further prioritized and are included in the reporting scope (see summary under "*Material impacts, risks and opportunities and their interaction with strategy and business model*"). Any potential negative impacts identified during the project but not meeting the threshold values will be managed as part of F-Secure's risk management process, where applicable.

Risks and opportunities with potential financial effect

The assessment of risks and opportunities with potential financial effect was based on thresholds for financial materiality (magnitude) and likelihood as described earlier. The risks are included in the company's risk management process where the company-level risks are prioritized based on risk impact and likelihood, while opportunities are managed as part of the company's strategy and function-specific execution plans.

Risk management is a continuous process within F-Secure. On company level, F-Secure maintains a top 10 risk map including mitigation actions and the risk map also includes ESG risks, where applicable. F-Secure's risk management framework is based on the ISO 31000 Risk Management guidelines that provide principles, a framework and a process for managing risks. Transparency to identified risks and their mitigation plans are done within a company-wide risk management tool.

F-Secure has also considered how our actual or potential impacts relate to risks and opportunities. This includes, for example, how protecting digital moments is directly connected with i) the opportunity that we see with the changing threat landscape, use of AI and protecting consumers against scams, ii) how such focus also helps mitigate risks around consumer willingness to pay for security and iii) having a compelling and relevant scam protection offering mitigates risks related to loss of a channel partner. Similarly, our impacts around gender equality, new culture and providing more holidays in regions like the US, in turn, help mitigate risks related to the well-being and satisfaction of our own workforce, loss of existing talent, and new hires. We have considered these in our strategy, business model and function plans.

Decision-making process and internal control procedures

F-Secure has established an ESG Council containing members from F-Secure's Leadership Team (CPO, CFO, SVP Corporate Development) and key stakeholders from various functions to drive the ESG agenda at F-Secure as described under ESRS 2 GOV-1.

The ESG Council is responsible for regularly re-assessing our DMA, as well as our impacts, risks and opportunities. F-Secure's ESG function under Corporate Development develops required internal controls in collaboration with the topic owner and updates of new controls will be presented to the ESG Council and Director of Financial Controlling who is the owner of the company-wide internal controls procedure. The ESG Council will be informed if the control has failed and present risk mitigation actions. Depending on the nature of the control, the Audit Committee will also be informed about the status and further mitigation actions being taken.

Integration of managing IROs and the risk management process

F-Secure has implemented a process of continuous risk management in its operations and functions. Each function will monthly or at minimum quarterly, review the risks, the related progress of mitigation plans while the Leadership Team reviews risks bi-annually. Each Leadership Team member (function lead) is accountable for executing the risk management process in their functions.

The input parameters include stakeholder feedback, F-Secure's own insights and estimations for each threshold value. The estimations are made based on the best available information at the time.

Our Risk Management Policy explicitly requires evaluating the short-, mid- and long-term time horizons taking into consideration the severity of the impact (scale, scope, remendability) and probability for any ESG-related risks including actual and potential negative impacts, and in the case of a potential negative human rights impact, the severity of the impact takes precedence over its likelihood.

The coordination of the DMA process and keeping our DMA up-to-date and relevant bi-annually is handled through F-Secure's ESG Council. Any actual or potential negative impacts or risks found during the assessment would be assigned and owned by each respective function to mitigate the risk or negative impact as part of our risk management process, while actual or potential positive impacts, as well as opportunities are integrated as part of F-Secure's strategy and relevant function execution plans.

While 2024 is the first reporting period applying ESRS, DMA and IRO lead reporting structure, the assessment process related to ESG impacts, risks and opportunities has been further developed as part of the F-Secure Double Materiality Assessment finalization. This includes further stakeholder engagement, sub-sub topic analysis and formally assigning specific impacts, risks and opportunities to specific functions. Possible future revisions of our DMA are subject to our annual DMA review by the ESG Council and as per our risk management process. Our next planned DMA review will take place no later than Q2/2025.

IRO-2 Disclosure requirements

F-Secure has included the following disclosure requirements in our sustainability statement as outlined in the following table.

Topic	Disclosure requirements	Index
General disclosure		
Basis for preparation	BP-1 – General basis for preparation of sustainability statements	29
Basis for preparation	BP-2 – Disclosures in relation to specific circumstances	29-30
Governance	GOV-1 – The role of the administrative, management and supervisory bodies	31-36
Governance	GOV-2 – Information provided to and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies	36-36
Governance	GOV-3 - Integration of sustainability-related performance in incentive schemes	36-37
Governance	GOV-4 - Statement on due diligence	37-37
Governance	GOV-5 - Risk management and internal controls over sustainability reporting 3. Strategy	39-40
Strategy	SBM-1 – Strategy, business model and value chain	37

Topic	Disclosure requirements	Index
Strategy	SBM-2 – Interests and views of stakeholders	45
Strategy	SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model	48-54
Impact, risk and opportunity management	IRO-1 - Description of the processes to identify and assess material impacts, risks and opportunities	55
Impact, risk and opportunity management	IRO-2 – Disclosure requirements in ESRS covered by the undertaking's sustainability statement	61-69

Topic	Disclosure requirements	Index
Environment		
Climate change	GOV-3 Integration of sustainability related performance in incentive schemes	36-37
Climate change	E1-1 Transition plan for climate change mitigation	81
Climate change	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	48-54
	IRO-1 Description of the processes to identify and assess material climate-related impacts, risks and opportunities	55-56
Climate change	E1-2 Policies related to climate change mitigation	82
Climate change	E1-3 Actions and resources in relation to climate change policies	82-83
Climate change	E1-4 Targets related to climate change mitigation	83-84
Climate change	E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions	84
Social		
Own workforce	GOV-3 Integration of sustainability-related performance in incentive schemes	36-37
Own workforce	SBM-2 Interests and views of stakeholders	45-46
Own workforce	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	48-54
Own workforce	S1-1 Policies related to own workforce	95-97
Own workforce	S1-2 Processes for engaging with own workers and workers' representatives	97-98
Own workforce	S1-3 Processes to remediate negative impacts and channels for own workers to raise concerns	98
Own workforce	S1-4 Taking action on material impacts on own workforce, and approaches to mitigating material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions	98-103
Own workforce	S1-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	103-104
Own workforce	S1-6 Characteristics of the undertaking's employees	106-106
Own workforce	S1-9 Diversity metrics	109
Own workforce	S1-13 Training and skills development metrics	109
Own workforce	S1-14 Health and safety metrics	110
Own workforce	S1-15 Work-life balance metrics	110
Own workforce	S1-16 Remuneration metrics	111
Own workforce	S1-17 Incidents, complaints and severe human rights impacts	111
Consumers and end-users	SBM-2 Interests and views of stakeholders	112-124

Topic	Disclosure requirements	Index
Consumers and end-users	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	112
Consumers and end-users	S4-1 Policies related to consumers and end-users S4-2 – Processes for engaging with consumers and end-users about impacts	116
Consumers and end-users	S4-3 Processes to remediate negative impacts and channels for consumers and end-users to raise concerns	119
Consumers and end-users	S4-4 Taking action on material impacts on consumers and end-users, and approaches to mitigating material risks and pursuing material opportunities	119-122
Consumers and end-users	S4-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	122-124
Governance		
Business conduct	GOV-1 The role of the administrative, supervisory and management bodies	31-36
Business conduct	IRO-1 Description of the processes to identify and assess material impacts, risks and opportunities Impact, risk and opportunity management	126
Business conduct	G1-1 Corporate culture and business conduct policies	127-129
Business conduct	G1-3 Prevention and detection of corruption or bribery	129-130
Business conduct	G1-4 – Confirmed incidents of corruption or bribery	131-131

Table 10. Disclosure requirements.

Disclosure Requirement and related datapoint	SFDR reference ¹⁾	Pillar 3 reference ²⁾	Benchmark Regulation reference ³⁾	EU Climate Law reference ⁴⁾	Index
ESRS 2 GOV-1 Board's gender diversity paragraph 21 (d)	Indicator number 13 of Table #1 of Annex 1		Commission Delegated Regulation (EU) 2020/1816, Annex II ⁵⁾		33
ESRS 2 GOV-1 Percentage of board members who are independent paragraph 21 (e)			Delegated Regulation (EU) 2020/1816, Annex II		33
ESRS 2 GOV-4 Statement on due diligence paragraph 30	Indicator number 10 Table #3 of Annex 1				37
ESRS 2 SBM-1 Involvement in activities related to fossil fuel activities paragraph 40 (d) i	Indicators number 4 Table #1 of Annex 1	Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Table 1: Qualitative information on Environmental risk and Table 2: Qualitative information on social risk ⁶⁾	Delegated Regulation (EU) 2020/1816, Annex II		Not applicable to F-Secure
ESRS 2 SBM-1 Involvement in activities related to chemical production paragraph 40 (d) ii	Indicator number 9 Table #2 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II		Not applicable to F-Secure
ESRS 2 SBM-1 Involvement in activities related to controversial weapons paragraph 40 (d) iii	Indicator number 14 Table #1 of Annex 1		Delegated Regulation (EU) 2020/1818, Article 12(1); Delegated Regulation (EU) 2020/1816, Annex II ⁷⁾		Not applicable to F-Secure
ESRS 2 SBM-1 Involvement in activities related to cultivation and production of tobacco paragraph 40 (d) iv			Delegated Regulation (EU) 2020/1818, Article 12(1); Delegated Regulation (EU) 2020/1816, Annex II		Not applicable to F-Secure
ESRS E1-1 Transition plan to reach climate neutrality by 2050 paragraph 14				Regulation (EU) 2021/1119, Article 2(1)	81
ESRS E1-1 Undertakings excluded from Paris-aligned Benchmarks paragraph 16 (g)		Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Template 1: Banking book Climate Change transition risk: Credit quality of exposures by sector, emissions and residual maturity	Delegated Regulation (EU) 2020/1818, Article 12.1 (d) to (g), and Article 12.2		81

Disclosure Requirement and related datapoint	SFDR reference ¹⁾	Pillar 3 reference ²⁾	Benchmark Regulation reference ³⁾	EU Climate Law reference ⁴⁾	Index
ESRS E1-4 GHG emission reduction targets paragraph 34	Indicator number 4 Table #2 of Annex 1	Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Template 3: Banking book – Climate change transition risk: alignment metrics	Delegated Regulation (EU) 2020/1818, Article 6		83
ESRS E1-5 Energy consumption from fossil sources disaggregated by sources (only high climate impact sectors) paragraph 38	Indicator number 5 Table #1 and Indicator n. 5 Table #2 of Annex 1				Not material
ESRS E1-5 Energy consumption and mix paragraph 37	Indicator number 5 Table #1 of Annex 1				Not material
ESRS E1-5 Energy intensity associated with activities in high climate impact sectors paragraphs 40 to 43	Indicator number 6 Table #1 of Annex 1				Not material
ESRS E1-6 Gross Scope 1, 2, 3 and Total GHG emissions paragraph 44	Indicators number 1 and 2 Table #1 of Annex 1	Article 449a; Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Template 1: Banking book – Climate change transition risk: Credit quality of exposures by sector, emissions and residual maturity	Delegated Regulation (EU) 2020/1818, Article 5(1), 6 and 8(1)		84
ESRS E1-6 Gross GHG emissions intensity paragraphs 53 to 55	Indicators number 3 Table #1 of Annex 1	Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Template 3: Banking book – Climate change transition risk: alignment metrics	Delegated Regulation (EU) 2020/1818, Article 8(1)		88
ESRS E1-7 GHG removals and carbon credits paragraph 56				Regulation (EU) 2021/1119, Article 2(1)	Not material
ESRS E1-9 Exposure of the benchmark portfolio to climate-related physical risks paragraph 66			Delegated Regulation (EU) 2020/1818, Annex II Delegated Regulation (EU) 2020/1816, Annex II		Omitted 2024

Disclosure Requirement and related datapoint	SFDR reference ¹⁾	Pillar 3 reference ²⁾	Benchmark Regulation reference ³⁾	EU Climate Law reference ⁴⁾	Index
ESRS E1-9 Disaggregation of monetary amounts by acute and chronic physical risk paragraph 66 (a) ESRS E1-9 Location of significant assets at material physical risk paragraph 66 (c)		Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 paragraphs 46 and 47; Template 5: Banking book – Climate change physical risk: Exposures subject to physical risk.			Omitted 2024
ESRS E1-9 Breakdown of the carrying value of its real estate assets by energy-efficiency classes paragraph 67 (c)		Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 paragraph 34; Template 2: Banking book – Climate change transition risk: Loans collateralised by immovable property – Energy efficiency of the collateral			Omitted 2024
ESRS E1-9 Degree of exposure of the portfolio to climate related opportunities paragraph 69			Delegated Regulation (EU) 2020/1818, Annex II		Omitted 2024
ESRS E2-4 Amount of each pollutant listed in Annex II of the EPRTR Regulation (European Pollutant Release and Transfer Register) emitted to air, water and soil, paragraph 28	Indicator number 8 Table #1 of Annex 1	Indicator number 2 Table #2 of Annex 1	Indicator number 1 Table #2 of Annex 1	Indicator number 3 Table #2 of Annex 1	Not material
ESRS E3-1 Water and marine resources paragraph 9	Indicator number 7 Table #2 of Annex 1				Not material
ESRS E3-1 Dedicated policy paragraph 13	Indicator number 8 Table 2 of Annex 1				Not material
ESRS E3-1 Sustainable oceans and seas paragraph 14	Indicator number 12 Table #2 of Annex 1				Not material
ESRS E3-4 Total water recycled and reused paragraph 28 (c)	Indicator number 6.2 Table #2 of Annex 1				Not material
ESRS E3-4 Total water consumption in m3 per net revenue on own operations paragraph 29	Indicator number 6.1 Table #2 of Annex 1				Not material
ESRS 2- SBM3 - E4 paragraph 16 (a) i	Indicator number 7 Table #1 of Annex 1				Not material
ESRS 2- SBM3 - E4 paragraph 16 (b)	Indicator number 10 Table #2 of Annex 1				Not material

Disclosure Requirement and related datapoint	SFDR reference ¹⁾	Pillar 3 reference ²⁾	Benchmark Regulation reference ³⁾	EU Climate Law reference ⁴⁾	Index
ESRS 2- SBM3 - E4 paragraph 16 (c)	Indicator number 14 Table #2 of Annex 1				Not material
ESRS E4-2 Sustainable land / agriculture practices or policies paragraph 24 (b)	Indicator number 11 Table #2 of Annex 1				Not material
ESRS E4-2 Sustainable oceans / seas practices or policies paragraph 24 (c)	Indicator number 12 Table #2 of Annex 1				Not material
ESRS E4-2 Policies to address deforestation paragraph 24 (d)	Indicator number 15 Table #2 of Annex 1				Not material
ESRS E5-5 Non-recycled waste paragraph 37 (d)	Indicator number 13 Table #2 of Annex 1				Not material
ESRS E5-5 Hazardous waste and radioactive waste paragraph 39	Indicator number 9 Table #1 of Annex 1				Not material
ESRS 2- SBM3 - S1 Risk of incidents of forced labour paragraph 14 (f)	Indicator number 13 Table #3 of Annex I				Not material
ESRS 2- SBM3 - S1 Risk of incidents of child labour paragraph 14 (g)	Indicator number 12 Table #3 of Annex I				Not material
ESRS S1-1 Human rights policy commitments paragraph 20	Indicator number 9 Table #3 and Indicator number 11 Table #1 of Annex I				96
ESRS S1-1 Due diligence policies on issues addressed by the fundamental International Labor Organisation Conventions 1 to 8, paragraph 21			Delegated Regulation (EU) 2020/1816, Annex II		95-97
ESRS S1-1 processes and measures for preventing trafficking in human beings paragraph 22	Indicator number 11 Table #3 of Annex I				Not applicable to F-Secure.
ESRS S1-1 workplace accident prevention policy or management system paragraph 23	Indicator number 1 Table #3 of Annex I				97
ESRS S1-3 grievance/complaints handling mechanisms paragraph 32 (c)	Indicator number 5 Table #3 of Annex I				98
ESRS S1-14 Number of fatalities and number and rate of work-related accidents paragraph 88 (b) and (c)	Indicator number 2 Table #3 of Annex I		Delegated Regulation (EU) 2020/1816, Annex II		Omitted 2024

Disclosure Requirement and related datapoint	SFDR reference ¹⁾	Pillar 3 reference ²⁾	Benchmark Regulation reference ³⁾	EU Climate Law reference ⁴⁾	Index
ESRS S1-14 Number of days lost to injuries, accidents, fatalities or illness paragraph 88 (e)	Indicator number 3 Table #3 of Annex I				Omitted 2024
ESRS S1-16 Unadjusted gender pay gap paragraph 97 (a)	Indicator number 12 Table #1 of Annex I		Delegated Regulation (EU) 2020/1816, Annex II		111
ESRS S1-16 Excessive CEO pay ratio paragraph 97 (b)	Indicator number 8 Table #3 of Annex I				111
ESRS S1-17 Incidents of discrimination paragraph 103 (a)	Indicator number 7 Table #3 of Annex I				111
ESRS S1-17 Nonrespect of UNGPs on Business and Human Rights and OECD paragraph 104 (a)	Indicator number 10 Table #1 and Indicator n. 14 Table #3 of Annex I		Delegated Regulation (EU) 2020/1816, Annex II	Delegated Regulation (EU) 2020/1818 Art 12 (1)	111-111
ESRS 2- SBM3 – S2 Significant risk of child labour or forced labour in the value chain paragraph 11 (b)	Indicators number 12 and n. 13 Table #3 of Annex I				Not material
ESRS S2-1 Human rights policy commitments paragraph 17	Indicator number 9 Table #3 and Indicator n. 11 Table #1 of Annex 1				47
ESRS S2-1 Policies related to value chain workers paragraph 18	Indicator number 11 and n. 4 Table #3 of Annex 1				Not material
ESRS S2-1 Nonrespect of UNGPs on Business and Human Rights principles and OECD guidelines paragraph 19	Indicator number 10 Table #1 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II	Delegated Regulation (EU) 2020/1818, Art 12 (1)	Not material
ESRS S2-1 Due diligence policies on issues addressed by the fundamental International Labor Organisation Conventions 1 to 8, paragraph 19			Delegated Regulation (EU) 2020/1816, Annex II		Not material
ESRS S2-4 Human rights issues and incidents connected to its upstream and downstream value chain paragraph 36	Indicator number 14 Table #3 of Annex 1				Not material
ESRS S3-1 Human rights policy commitments paragraph 16	Indicator number 9 Table #3 of Annex 1 and Indicator number 11 Table #1 of Annex 1				47

Disclosure Requirement and related datapoint	SFDR reference ¹⁾	Pillar 3 reference ²⁾	Benchmark Regulation reference ³⁾	EU Climate Law reference ⁴⁾	Index
ESRS S3-1 non-respect of UNGPs on Business and Human Rights, ILO principles or and OECD guidelines paragraph 17	Indicator number 10 Table #1 Annex 1		Delegated Regulation (EU) 2020/1816, Annex II Delegated Regulation (EU) 2020/1818, Art 12 (1)		Not material
ESRS S3-4 Human rights issues and incidents paragraph 36	Indicator number 14 Table #3 of Annex 1				Not material
ESRS S4-1 Policies related to consumers and end-users paragraph 16	Indicator number 9 Table #3 and Indicator number 11 Table #1 of Annex 1				Not material
ESRS S4-1 Non-respect of UNGPs on Business and Human Rights and OECD guidelines paragraph 17	Indicator number 10 Table #1 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II Delegated Regulation (EU) 2020/1818, Art 12 (1)		117
ESRS S4-4 Human rights issues and incidents paragraph 35	Indicator number 14 Table #3 of Annex 1				121
ESRS G1-1 United Nations Convention against Corruption paragraph 10 (b)	Indicator number 15 Table #3 of Annex 1				Not material
ESRS G1-1 Protection of whistle-blowers paragraph 10 (d)	Indicator number 6 Table #3 of Annex 1				128-128
ESRS G1-4 fines for violation of anti-corruption and anti-bribery laws paragraph 24 (a)	Indicator number 17 Table #3 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II		131
ESRS G1-4 Standards of anti-corruption and anti-bribery paragraph 24 (b)	Indicator number 16 Table #3 of Annex 1				131

1) Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector (Sustainable Finance Disclosures Regulation) (OJ L 317, 9.12.2019, p. 1).

2) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (Capital Requirements Regulation "CRR") (OJ L 176, 27.6.2013, p. 1).

3) Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (OJ L 171, 29.6.2016, p. 1).

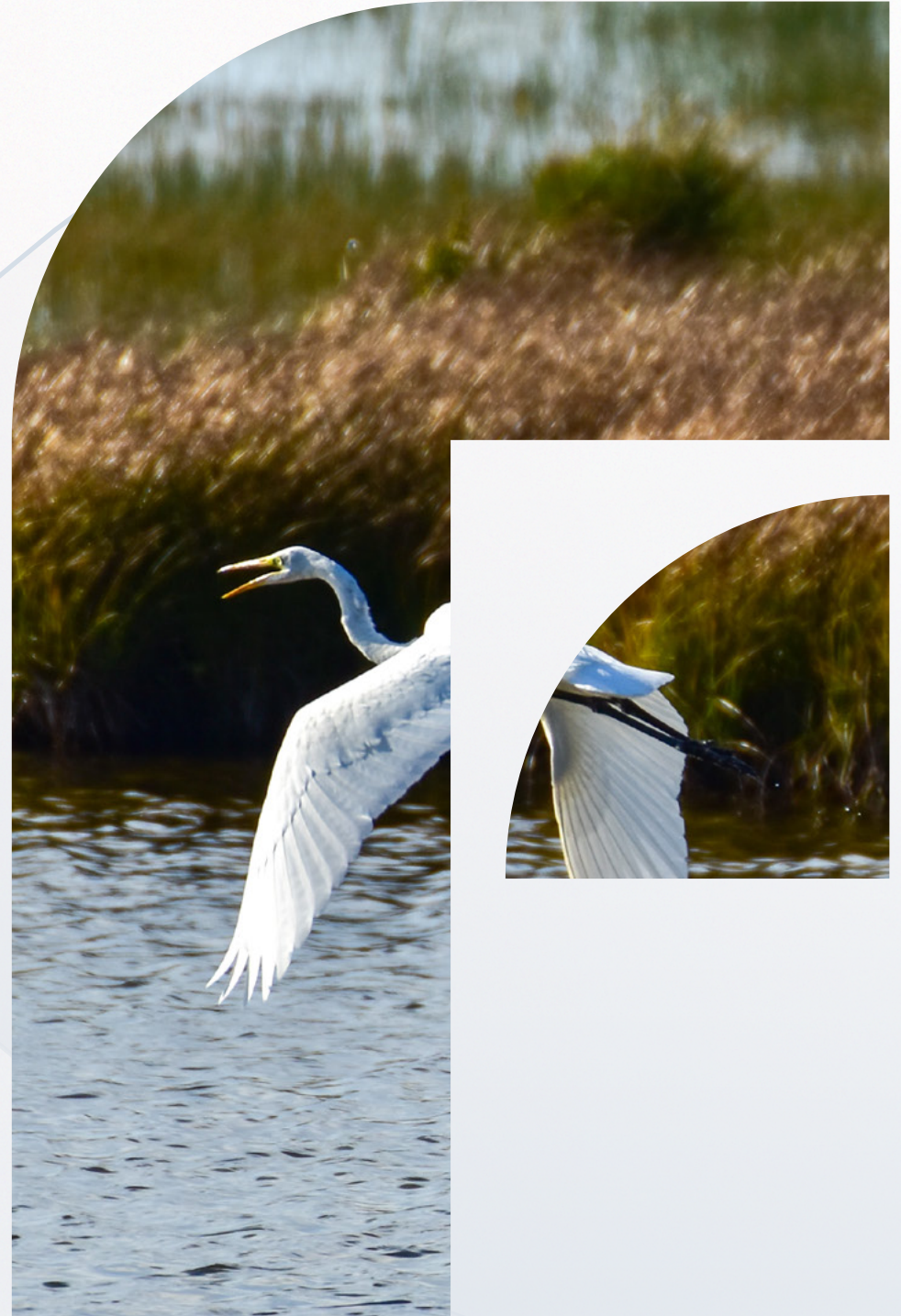
4) Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 ('European Climate Law') (OJ L 243, 9.7.2021, p. 1).

5) Commission Delegated Regulation (EU) 2020/1816 of 17 July 2020 supplementing Regulation (EU) 2016/1011 of the European Parliament and of the Council as regards the explanation in the benchmark statement of how environmental, social and governance factors are reflected in each benchmark provided and published (OJ L 406, 3.12.2020, p. 1).

6) Commission Implementing Regulation (EU) 2022/2453 of 30 November 2022 amending the implementing technical standards laid down in Implementing Regulation (EU) 2021/637 as regards the disclosure of environmental, social and governance risks (OJ L 324, 19.12.2022, p.1).

7) Commission Delegated Regulation (EU) 2020/1818 of 17 July 2020 supplementing Regulation (EU) 2016/1011 of the European Parliament and of the Council as regards minimum standards for EU Climate Transition Benchmarks and EU Paris-aligned Benchmarks (OJ L 406, 3.12.2020, p. 17).

Sustainability Statement - Environment



EU Taxonomy

Taxonomy reporting

F-Secure has assessed the taxonomy-eligibility and taxonomy-alignment of its economic activities according to the EU Taxonomy Regulation (EU) 2020/852, the Climate Delegated Acts (EU) 2021/2139 and (EU) 2023/2485, the Environmental Delegated Act (EU) 2023/2486, the Disclosures Delegated Act (EU) 2021/2178 and other related guidance from the European Commission.

The analysis has been performed in collaboration between the F-Secure financial controlling and sustainability function and reviewed by an external sustainability consultant.

A taxonomy-non-eligible activity is defined as an activity not listed in Commission Delegated Regulations (EU) 2021/2139 and (EU) 2023/2485 or Commission Delegated Regulation (EU) 2023/2486. F-Secure operates in the field of cybersecurity software, which is a business area currently not covered by the EU Taxonomy and is therefore not taxonomy eligible. While Commission Delegated Regulation (EU) 2021/2139 (Climate Delegated Act) endorses computer programming as a taxonomy eligible activity (8.2 Computer programming, consultancy and related activities), the description of the activity is broad and does not specify whether or not the activity needs to be associated with software and consulting relevant to climate change adaptation or mitigation. It is also evident based on Section 8.2 in Annex II that it concerns expert services rather than the type of activities F-Secure offer. As F-Secure's business activities are clearly not aimed towards climate change adaptation or mitigation and climate change adaptation has been identified as not material in a recent double materiality assessment for the company, we do not consider our business activities to be taxonomy-eligible and we provide the tables for turnover, capex and opex with only taxonomy-non-eligible information (*part B* of the tables). F-Secure has taken into account the 4 other climate and environmental objectives (water and marine, circular economy, pollution, biodiversity and ecosystem) and they do not lead to potentially eligible economic activities in this section. Furthermore, F-Secure is not involved with any nuclear energy-related activities or fossil gas-related activities as disclosed in section *Involvement with nuclear energy and fossil gas related activities*.

We closely follow further developments of the taxonomy reporting requirements and will update the assessments when new legislation is published or when new information regarding its application becomes available. New activities, with new

environmental targets in future versions of the taxonomy might be more relevant for F-Secure and trigger a need of re-assessing both eligibility and alignment.

Turnover

Taxonomy-eligible turnover is defined as the proportion of net turnover derived from products or services, including intangibles, associated with taxonomy-eligible economic activities. As F-Secure has not recognized any taxonomy-eligible economic activities, only the turnover on taxonomy-non-eligible activities is disclosed.

Turnover

Financial year 2024		2024		Substantial contribution criteria						DNSH criteria											
Economic Activities		Code(s)	Turnover	Proportion of Turnover 2024	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Minimum safeguards	Proportion of Taxonomy-aligned (A.1) or -eligible (A.2) turnover 2023	Category (enabling activity)	Category (transitional activity)	
Text			EUR 1 000	%	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	%	E	T	
A.	TAXONOMY-ELIGIBLE ACTIVITIES																				
Environmentally sustainable activities (Taxonomy-aligned)																					
A.1																					
Turnover of environmentally sustainable activities (Taxonomy-aligned) (A.1)			0 €	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%			
Of which enabling			0 €	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%	E		
Of which transitional			0 €	0.0 %	0.0 %													0%		T	
A.2		Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)																			
					EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL											
					EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL								0%			
Turnover of Taxonomy-eligible but not environmentally sustainable activities (not-Taxonomy-aligned activities) (A.2)			0 €	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%			
A.		Turnover of Taxonomy-eligible activities (A.1 + A.2)		0 €	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%			
B.		TAXONOMY-NON-ELIGIBLE ACTIVITIES																			
Turnover of Taxonomy-non-eligible activities			146,258 €	100.0 %																	
TOTAL			146,258 €	100.0 %																	

Operating expenditure

The operating expenses (1,879 MEUR) included in the taxonomy assessment are defined as direct non-capitalised costs that relate to research and development, building renovation measures, short-term lease, maintenance and repair, and any other direct expenditure relating to the day-to-day servicing of assets of property, plant and equipment by the undertaking or a third party to whom activities are outsourced that are necessary to ensure the continued and effective functioning of such assets (2021/2178). In F-Secure's calculation, the operating expenses related to rental of premises (including depreciations for leased premises accounted for under IFRS 16 standard) and maintenance of premises, as well as other expenses related to the functioning of the leased property, plant and equipment are included. After the end of the transitional service period (at the end of 2023), F-Secure has transitioned to third-party cloud platforms of Amazon Web Services (AWS) and Microsoft Azure for majority of its operations. Cloud hosting costs are not included in the operating expenses subject to taxonomy assessment.

As F-secure has not recognized any taxonomy-eligible economic activities, only the OpEx of taxonomy-non-eligible activities is disclosed.

Operating expenditure

Financial year 2024		2024		Substantial contribution criteria						DNSH criteria										
Economic Activities		Code(s)	OpEx	Proportion of OpEx 2023	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Minimum safeguards	Proportion of Taxonomy-aligned (A.1) or -eligible (A.2) OpEx 2023	Category (enabling activity)	Category (transitional activity)
Text			EUR 1000	%	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	%	E	T
A.	TAXONOMY-ELIGIBLE ACTIVITIES																			
Environmentally sustainable activities (Taxonomy-aligned)																				
A.1	OpEx of environmentally sustainable activities (Taxonomy-aligned) (A.1)		0 €	0%	0%	0%	0%	0%	0%	0%								0%		
	Of which enabling		0 €	0%	0%	0%	0%	0%	0%	0%								0%	E	
	Of which transitional		0 €	0%	0%													0%		T
A.2	Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)																			
					EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL										
					EL	EL	N/EL	N/EL	N/EL	N/EL								0%		
OpEx of Taxonomy-eligible but not environmentally sustainable activities (not-Taxonomy-aligned activities) (A.2)			0 €	0%	0%	0%	0%	0%	0%	0%								0%		
A.	OpEx of Taxonomy-eligible activities (A.1 + A.2)		0 €	0%	0%	0%	0%	0%	0%	0%								0%		
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES																				
OpEx of Taxonomy-non-eligible activities			1,879 €	100%																
TOTAL			1,879 €	100%																

Capital expenditure

The capital expenses included in the taxonomy assessment are defined as additions to tangible and intangible assets during the financial year, considered before depreciation, amortization and any re-measurements, including those resulting from revaluations and impairments, for the relevant financial year and excluding fair value changes (2021/2178). F-Secure's capital expenses (11.158 MEUR) include capitalizations of development expenditure on new products or product versions with significant new features, partially or completely internally developed intangible assets which relate e.g. to platforms and software licenses. These are intangible assets according to IAS 38 accounting standard. A minor part of capital expenses relates to capitalization of employee laptops and other hardware, as well as office renovation expenses. As F-secure has not recognized any taxonomy-eligible economic activities, only the CapEx of taxonomy-non-eligible activities is disclosed.

Capital expenditure

Financial year 2024		2024			Substantial contribution criteria						DNSH criteria									
Economic Activities		Code(s)	CapEx	Proportion of CapEx 2023	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Minimum safeguards	Proportion of Taxonomy-aligned (A.1) or -eligible (A.2) CapEx 2023	Category (enabling activity)	Category (transitional activity)
Text			EUR 1000	%	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y; N; N/EL	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	%	E	T
A.	TAXONOMY-ELIGIBLE ACTIVITIES																			
Environmentally sustainable activities (Taxonomy-aligned)																				
A.1		CapEx of environmentally sustainable activities (Taxonomy-aligned) (A.1)		0 €	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
		Of which enabling		0 €	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%	E	
		Of which transitional		0 €	0.0 %	0.0 %												0%		T
A.2		Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)																		
					EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL										
					EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL	EL; N/EL								0%		
		CapEx of Taxonomy-eligible but not environmentally sustainable activities (not-Taxonomy-aligned activities) (A.2)		0 €	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
A.		CapEx of Taxonomy-eligible activities (A.1 + A.2)		0 €	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
B.		TAXONOMY-NON-ELIGIBLE ACTIVITIES																		
		CapEx of Taxonomy-non-eligible activities		11,158 €	100.0 %															
		TOTAL		11,158 €	100.0 %															

Involvement with nuclear energy and fossil gas related activities.

Row	Nuclear energy related activities	
1	The undertaking carries out, funds or has exposures to research, development, demonstration and deployment of innovative electricity generation facilities that produce energy from nuclear processes with minimal waste from the fuel cycle.	NO
2	The undertaking carries out, funds or has exposures to construction and safe operation of new nuclear installations to produce electricity or process heat, including for the purposes of district heating or industrial processes such as hydrogen production, as well as their safety upgrades, using best available technologies.	NO
3	The undertaking carries out, funds or has exposures to safe operation of existing nuclear installations that produce electricity or process heat, including for the purposes of district heating or industrial processes such as hydrogen production from nuclear energy, as well as their safety upgrades.	NO
Fossil gas related activities		
4	The undertaking carries out, funds or has exposures to construction or operation of electricity generation facilities that produce electricity using fossil gaseous fuels.	NO
5	The undertaking carries out, funds or has exposures to construction, refurbishment, and operation of combined heat/cool and power generation facilities using fossil gaseous fuels.	NO
6	The undertaking carries out, funds or has exposures to construction, refurbishment and operation of heat generation facilities that produce heat/cool using fossil gaseous fuels.	NO

E1 – Climate change

SBM-3 Material impacts, risks and opportunities

Climate change list of IROs

	Material impact, risk or opportunity	Description
Climate change mitigation		
Opportunity (OO)	Set policy for e-cars	F-Secure has a small number of leasing cars in Finland, however the amount will rise over time (taken in consideration F-Secure growth target)
Risk (OO)	Fail to meet mitigation targets or not enough ambition. F-Secure emission reduction heavily reliant on suppliers.	Investing and finance linked to ESG ambition and targets of the company. Some partners not willing to continue business if not sufficient climate ambition.
Potential positive impact (OO)	Implementation of green coding principles	Through implementing green coding, we can reduce the impact of our end-product. Including optimizing device performance, battery use and cloud computing.
Energy		
No significant IROs identified		
Climate change adaptation		
No significant IROs identified		

Table 15. Climate change IROs.

Interaction with strategy and business model

F-Secure's material climate change-related IROs are summarized under F-Secure's resilience analysis covers both the upstream and downstream value chain, as well as own operations. F-Secure has covered relevant physical risks, as well as transition-related risks in its resilience analysis.

The physical risks covered in the analysis are listed in the Table 7, *Physical Climate Risks* below. Transition-related risks, derived from material IROs, are integral to the resilience analysis. Transition risks are described in chapter "Description of the process to identify and assess material IROs". These material IROs are evaluated in terms of their impact on F-Secure's strategy and business model, ensuring that the scope of the analysis comprehensively addresses potential vulnerabilities and opportunities for adaptation.

Climate SBM-3 physical risks

Chronic		Acute	
	Temperature-Related		
x ¹⁾	Changing temperature (air, freshwater, marine water)	x	Heat wave
x	Heat stress	x	Cold wave/frost
x	Temperature variability	x	Wildfire
	Permafrost thawing		
	Wind-Related		
	Changing wind patterns	x	Cyclone, hurricane, typhoon
		x	Storm (including blizzards, dust and sandstorms)
		x	Tornado
			Glacial lake outburst
	Water-Related		
x	Changing precipitation patterns and types (rain, hail, snow/ice)	x	Drought
	Precipitation and/or hydrological variability	x	Heavy precipitation (rain, hail, snow/ice)
	Ocean Acidification	x	Flood (coastal, fluvial, pluvial, ground water)
	Saline intrusion		
	Sea level rise		
	Water stress		
	Solid Mass-Related		
	Coastal erosion		Avalanche
	Soil degradation	x	Landslide
	Soil erosion	x	Subsidence
	Solifluction		

¹⁾ x = hazard included in the assessment

Table 16. Climate related physical risks.

Transition assumptions

The transition to a lower-carbon and resilient economy will likely influence macroeconomic trends by driving economic growth through green technologies and sustainable practices. Energy consumption will shift towards renewable sources like solar and wind, reducing reliance on fossil fuels. Technology deployment, including energy-efficient software solutions and innovations in carbon capture, will support this transition and enhance economic resilience. National and international policies will be crucial in promoting GHG emission reductions and supporting renewable energy adoption.

Time horizons, climate scenarios and reduction targets

F-Secure has considered Task Force on Climate-related Financial Disclosures Guidance on Scenario Analysis for Non-Financial Companies (2020) in the development of the climate-related scenario analysis. F-Secure has not used TCFD's future climate scenarios but created its own, since the timescale of the business activities (including contracts with facility owners, partners and suppliers) are shorter than the climatic comparison period (20-30 yr.) in areas, where they may be exposed to material hazards. Therefore, it is sufficient to estimate the current climate risks and update the analysis regularly.

F-Secure has set a long-term GHG reduction target for 2030 and made a transition plan where a reduction pathway has been defined and reduction actions identified on an annual level. The focal question of F-Secure's scenario analysis revolves around whether F-Secure will reach its climate reduction target or not, namely as F-Secure's emission reductions are heavily supply chain-dependent. If F-Secure does not reach its long-term climate change mitigation target of reducing emissions of Scope 1, 2 and 3 by 42% by 2030 there could be reputational damage, and our partners might choose to do business with other companies instead, all of which could be reflected in F-Secure's stock price. Furthermore, and over time, there could be changes in legislation defining fines for companies not reaching climate targets in line with the Paris Agreement.

F-Secure uses scenarios as a tool to analyze its environmental resilience. The time horizons for the scenarios are 2030 and 2050. As a result, F-Secure has included the following climate scenarios in the analysis:

Scenario 1: F-Secure meets its long-term climate mitigation target by 2030 and becomes climate neutral by 2050. The scenario is in line with limiting global warming to 1.5°C.

Scenario 2: F-Secure fails to meet the mitigation targets. Society's emission reductions (including F-Secure's supply chain) are not fast or effective enough and therefore the operating environment prevents F-Secure from meeting its climate goal.

Anticipated financial effects

The estimated anticipated financial effects from material physical and transition risks, as required by Disclosure Requirement E1-9, were not thoroughly evaluated in our resilience analysis due to the omission of E1-9. However, regarding material transition risks related to supply chain dependency, it is likely that F-Secure may

face some economic losses if sufficient climate targets are not set in alignment with stakeholder expectations. Additionally, in the medium to long term, companies may face financial penalties or fines for not meeting climate mitigation targets. The mitigation actions and resources, as disclosed under Disclosure Requirement E1-3, have been integrated into our strategic planning.

Results of the resilience analysis

F-Secure is considered a climate change-resilient company due to the nature of our business. Our resilience analysis shows that there are no significant risks identified related to climate change physical hazards, climate change in our own operations, and no assets identified in higher risk regions, as F-Secure is a software company.

There are areas of uncertainty, particularly regarding supplier emissions and the long-term carbon target. There is uncertainty in obtaining actual emission data from suppliers and ensuring they meet their climate targets. Additionally, uncertainties exist regarding the impact of various drivers on setting and achieving a potential carbon neutrality target.

In terms of considering assets and business activities at risk, F-Secure aims to meet legal and partner expectations on climate change without negatively impacting the business. We are updating our supplier selection processes to include climate requirements. F-Secure focuses on obtaining emission data from suppliers, ensuring suppliers meet climate targets, and monitoring spend categories like travel to align with their reduction pathway. We are also conducting assessments to understand the requirements for achieving carbon neutrality in the long term. While it is likely that F-Secure will set such a target in the coming years, we have conducted an initial assessment to understand the requirements and high-level actions needed to achieve it.

Ability to adapt the strategy and business model to climate change

F-Secure's ability to adjust or adapt the strategy is embedded in our strategy process, which allows us to regularly assess our progress and rapidly react to market changes and new opportunities. This includes integrating climate considerations into our strategic planning over the short, medium and long term. The ability to adapt to climate change in the business model and strategy is covered more in ESRS 2 E1 IRO-1.

E1-1 Transition plan for climate change mitigation

During 2024, F-Secure has developed a detailed transition plan for climate change mitigation including Scope 1, 2 and 3, and all the relevant categories included in Scope 3. We have also updated our GHG model and reviewed the emission factors used in the model.

Reference to GHG emission reduction targets: Paris Agreement

In reference to E1-4, F-Secure has set key greenhouse gas (GHG) emissions reduction targets in line with the Paris Agreement limiting global warming to 1.5 °C. The Greenhouse Gas Protocol (GHG Protocol) and CSRD are adopted as the framework for measuring and managing emissions. The targets cover reducing GHG emissions by 42% between 2024 and 2030 in our own operations and across our value chain (Scope 1 & 2 and 3) whereas the base year set for our emission reduction targets is 2024. Also, the emission reduction targets are based on the IPCC 1.5°C Pathways. Sectoral decarbonization is not available for IT and Software companies, yet.

Reference to GHG emission reduction targets: E1-3 and E1-4

In reference to Disclosure Requirements E1-3 and E1-4, we have identified three primary decarbonization levers regarding material IROs: fuel switching, supply chain decarbonization and efficient coding principles. To meet our 2030 emission reduction targets, we have outlined a series of actions we plan to implement in these decarbonization levers.

1. Fuel switching: to reduce the climate impact of our fleet, we will lease only hybrid and electric vehicles.
2. Supply chain decarbonization consists of i) improving GHG emissions data quality related to our suppliers, ii) ensuring that our travel policy reflects our climate ambitions, and prioritizing virtual meetings to minimize travel. Also partnering with zero-emission solution providers will ensure that the overall emission profile remains unchanged despite increased energy use while adopting new technologies, for example AI models.
3. Efficient or "green" coding principles, we focus on creating efficient solutions that minimize electricity usage and implement coding standards that reduce energy consumption during software execution in the downstream value chain.

For 2050, a specific emission reduction target has not yet been set but could include working with carbon-neutral suppliers to further reduce indirect emissions and promote sustainable practices.

Reference to climate change mitigation actions

As per disclosure requirement E1-3, F-Secure does not have taxonomy-compliant activities, and therefore no linked investments and financing that would support its transition plan. See more under the EU Taxonomy section.

Locked-in GHG emissions

Carbon lock-in is generally associated with physical infrastructure and long-term investments in carbon-intensive technologies. While there are some aspects where carbon lock-in can be relevant to software, the topic is not seen as material as the impacts are small due to actions already taken by F-Secure. The implementation of green coding further reduces locked-in GHG emissions.

Economic activities and benchmark regulation (Pillar 3)

A taxonomy-non-eligible activity is defined as an activity not listed in Commission Delegated Regulation (EU) 2021/2139 or Commission Delegated Regulation (EU) 2023/2486. F-Secure operates in the field of cyber security software, which is a business area currently not covered by the EU Taxonomy and is, therefore, not taxonomy eligible. See our EU Taxonomy statement for more details. F-Secure is not excluded from the EU Paris-aligned Benchmarks.

Transition plan alignment with F-Secure's strategy and financial planning

ESG is not a separate strategy at F-Secure but is incorporated into the company's strategy and is part of normal business operations. Similarly, the transition plan actions will be implemented by appropriate functions including taking actions into account in their annual budgets to meet set goals, and progress will be tracked by F-Secure's Environment Committee and our ESG Council.

The 2024 priority was to establish it as our baseline year for GHG reductions. During the year, an Environment Committee has been set up in Q3 2024 to implement the transition plan and owners for each category have been defined. In addition, climate change-related topics are considered in the renovation of the new headquarters project (planning 2024 and execution 2025) and in new leasing agreements. During 2024, we have defined and approved our climate change policy and the supplier Code of Conduct includes relevant environmental topics. Further developments and updates of our GHG emissions model and transition plan have also been conducted to build the foundation to execute the plan. Our detailed transition plan is being defined based on the scope described under the Climate Change section and will be reviewed and approved by the Board during 2025.

Impact, risk and opportunity management

E1-2 Policies

F-Secure has the ambition to deliver sustainable security experiences to our partners and consumers. To ensure we deliver on our climate change targets F-Secure has a separate Climate change policy approved by the CEO covering climate change mitigation, climate change adaptation and renewable energy deployment. The main objective is to manage and prioritize emissions in operations and the value chain, covering all geographies.

The policy outlines F-Secure's climate change mitigation principles, covering targets and main activities across Scopes 1, 2, and 3. For climate change adaptation, it emphasizes identifying climate impacts, risks, and opportunities to inform planning, including conducting risk assessments and integrating climate considerations into the strategy. Regarding renewable energy deployment, the policy focuses on using renewable energy in office spaces, integrating climate considerations into office decisions, utilizing low-emission hosting services, and implementing green coding practices. F-Secure acknowledges its climate change-related impacts, risks, and opportunities, and the process to identify these includes conducting risk assessments, scenario analyses, and integrating these considerations into the strategy and operations.

E1-3 Actions and resources

To achieve Climate change policy targets and mitigate emissions, there are three decarbonization levers linked to the environmental IROs.

The IRO opportunity set policy for e-vehicles has decarbonization lever fuel switching. In 2024, F-Secure decided that all new cars leased from May 1st onwards would be either hybrid or electric vehicles. A few cars were already replaced with hybrid or electric models during 2024, and this transition will continue as leasing contracts are renewed. In the future, we aim to update our car policy to ensure that by 2030, all leasing cars are electric.

Regarding the IRO risk that F-Secure's emission reduction is heavily reliant on suppliers, the key decarbonization lever is supply chain decarbonization. We have started actions towards mitigating emissions in our value chain. For example, the decision on new VPN technology was finalized, the travel booking system was updated and supplier analysis was initiated to identify the sources of emissions to guide future actions. There are no quantitative emission reductions for these actions in 2024, and in 2030 a 42% reduction is expected.

The IRO potential positive impact of the implementation of green coding principles has decarbonization lever efficient coding principles. Emissions for sold products are calculated based on the number of products sold annually, which may increase unless changes are made. No quantitative emission reductions are expected in 2024, and the material impact is low. By 2030, no emission reductions are expected as the number of sold products is projected to grow while we optimize energy consumption.

In addition to decarbonization levers, F-Secure operates two major offices with over 50 employees each: one in Helsinki and one in Kuala Lumpur. The long-term plan is to ensure that all large offices, as well as smaller facilities where energy contracts can be controlled, use 100% renewable energy.

For more specific expected emission reductions, see *Disclosure Requirement E1-4 – Targets related to climate change mitigation and adaptation*. No significant monetary amounts CapEx and OpEx have been required to implement the actions.

Metrics and targets

E1-4 Targets

F-Secure describes its sustainability-related baseline measures and targets in Table E1-4 *Climate targets & progress*. 2024 is established as a baseline year and progress will be reported annually moving forward.

Methodologies for tracking emission reduction targets vary. Scope 1 emissions are calculated using fuel consumption data and leasing contracts. Scope 2 emissions use both market-based and location-based methods, collecting data from sites. Scope 3 emissions primarily use the spend-based method, with some data obtained directly from suppliers. More details are in E1-6 – Gross Scopes 1, 2, 3 and Total GHG emissions.

The 2024 emission calculation methodology was reviewed by an external consultant. Financial values were audited during regular finance processes. Metrics were selected based on addressing legislative requirements, material ESG topics, and stakeholder feedback. ESG targets were internally reviewed and approved by the Board of Directors.

E1-4 Climate targets & progress

	2024 base year	2030 target
Gross Scope 1 & Scope 2 (market-based) (tCO2eq)	220	42% emission reduction
Gross Scope 3 (tCO2eq)	8330	42% emission reduction

Table 17. Climate targets and progress

We track our actions' effectiveness using total GHG emissions (tons of CO2e), emissions intensity per revenue, and their impact. Our GHG emissions reduction target aligns with the Paris Agreement, aiming to limit global warming to 1.5 °C, and aim for a 42% reduction in Scope 1, 2, and 3 emissions by 2030, using 2024 as the baseline year. This target is absolute and measured in tons of CO2e.

We disclose combined GHG emission reduction targets for Scope 1 and Scope 2 emissions, covering direct and indirect emissions from operations and purchased energy. Scope 2 emissions are calculated using market-based and location-based methods, with market-based used for the 2030 target. There is a separate target for Scope 3 emissions, including upstream and downstream activities, applying globally. The targets align with GHG inventory boundaries.

Our emission reduction targets do not include GHG removals, carbon credits or avoided emissions as a means of achieving the GHG emission reduction targets.

E1-4 Progress towards targets

Current base year and baseline value

2024 is chosen as the base year for emissions to ensure an accurate view and to avoid external influences. For example, 2023 includes the acquisition of Lookout Life midyear and also comes with a sizable impact on IACs. After 2030, the base year is set every five years. The 2024 baseline values are described in chapter E1-6 later in this statement.

Framework and methodology for target setting

F-Secure has established GHG emission reduction targets that are compatible with limiting global warming to 1.5°C. Therefore, F-Secure aims to decrease emissions in Scope 1&2 and in Scope 3 by 42% by 2030. This means that in 2030 Scope 1&2 emissions aim to be 127 tons of CO₂e and Scope 3 emissions aim to be 4831 tons of CO₂e. To achieve this, the Greenhouse Gas Protocol (GHG Protocol) and IPCC's cross-sector pathway are adopted as the framework for measuring and managing emissions. This ensures accurate tracking and reporting of GHG emissions across all operations. Emission reduction targets are based on the IPCC 1.5°C Pathways. SBTi or a similar framework is under evaluation as per stakeholder requirements but has not yet been applied. The current view is that such a framework would not materially change our overall GHG emissions.

Additionally, future developments have been carefully considered when setting these targets. Technological advancements, regulatory changes, and shifts in market dynamics could significantly impact the targets and progress toward them. For instance, the transition to renewable energy and the adoption of AI technologies are anticipated to influence F-Secure's ability to achieve its emission reduction targets. F-Secure is dedicated to continuously reviewing and adjusting its strategies to ensure they remain aligned with the latest scientific and industry standards, thereby maintaining the integrity and feasibility of its emission reduction goals.

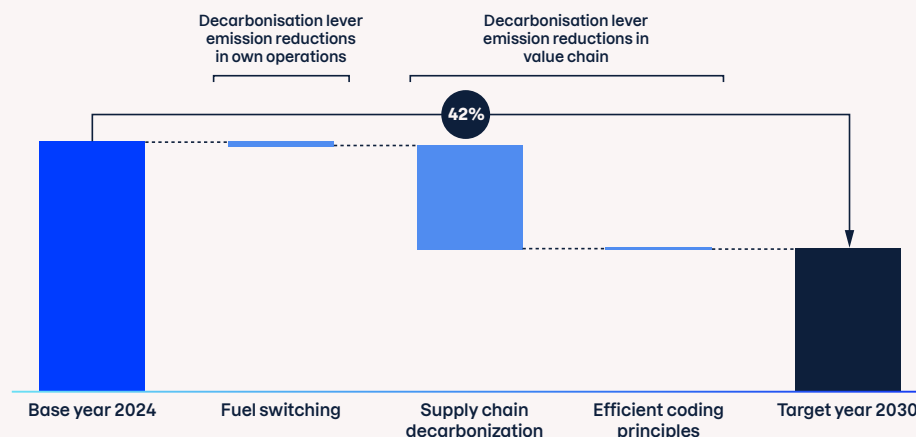
Decarbonization levers and their contributions to achieve reduction targets.

Expected decarbonization levers based on IRO analysis are fuel switching, supply chain decarbonization and efficient coding principles.

- Fuel switching: F-Secure plans to lease only hybrid and electric vehicles to reduce the impact of its fleet on climate change. The estimate is that the amount of leasing vehicles will stay the same of which 50% will be electric vehicles and 50% hybrid vehicles. Hybrid vehicle emissions are estimated to be 50% of regular fuel

vehicles. We estimate that emissions will be within the 42% decrease target by 2027. Emissions in Scope 1 and Scope 2 in 2024 were 220 tCO₂e.

- Supply chain decarbonization: Energy-efficient practices are promoted among suppliers. This lever includes Scope 3 categories 1 and 6. In 2024 these categories covered over 95% of emissions in Scope 3. By collaborating with key suppliers and following policies, a 42% decrease in emissions from the value chain is anticipated. Emissions in Scope 3 in 2024 were 8330 tCO₂e.
- Efficient coding principles: We're not expecting a material reduction in the emissions due to these activities as we expect our end-customer base to grow at the same time (sold products). This lever covers Scope 3 category 11 and is around 1% of emissions. Emissions in Scope 3 in 2024 were 8330 tCO₂e.



Graphical pathway waterfall shows the development of emissions over time.

E1-6 Gross scopes 1, 2, 3 and Total GHG Emissions

In GHG emission calculations, the GHG Protocol Corporate Standard has been considered for principles, requirements and guidance. In our efforts to measure and manage our Scope 3 greenhouse gas (GHG) emissions, we have utilized both primary data and emission factors. Currently, Amazon Web Services (AWS) is the only supplier providing primary data that is used in emission calculation, which represents less than 1% of our total Scope 3 emissions. The remaining emissions have been calculated using standardized emission factors.

E1-6 Gross scopes and total emissions are summarized in the table below.

	Retrospective				Milestones and target years			
	Base year 2024	Comparative	2024	% N / N-1	2025	2030	(2050)	Annual % target / Base year
Scope 1 GHG emissions								
Gross Scope 1 GHG emissions (tCO ₂ eq)	31	-	31	-	-	18 ¹⁾	-	8.70% ²⁾
Percentage of Scope 1 GHG emissions from regulated emission trading schemes (%)	0%	-	0%	-	-	-	-	-
Scope 2 GHG emissions								
Gross location-based Scope 2 GHG emissions (tCO ₂ eq)	233	-	233	-	-	-	-	-
Gross market-based Scope 2 GHG emissions (tCO ₂ eq)	189	-	189	-	-	110 ¹⁾	-	8.70% ²⁾
Scope 3 GHG emissions								
Total Gross indirect (Scope 3) GHG emissions (tCO ₂ eq)	8330	-	8330	-	-	4831	-	8.70% ³⁾
1. Purchased goods and services (excluding data centre services)	6466	-	6466	-	-	-	-	-
Sub-category: Cloud computing and data centre services	43	-	43	-	-	-	-	-
3. Fuel and energy-related activities	49	-	49	-	-	-	-	-
5. Waste generated in operations	2	-	2	-	-	-	-	-
6. Business travel	1675	-	1675	-	-	-	-	-
7. Employee commuting	23	-	23	-	-	-	-	-
8. Upstream leased assets	11	-	11	-	-	-	-	-
11. Use of sold products	61	-	61	-	-	-	-	-
Total GHG emissions								
Total GHG emissions (location-based) (tCO ₂ eq)	8594	-	8594	-	-	-	-	-
Total GHG emissions (market-based) (tCO ₂ eq)	8550	-	8550	-	-	4958	-	8.70% ³⁾

1) Scope 1 and Scope 2 target is combined and not measured separately.

2) Value is based on a linear progression. Our impact is not expected to follow a linear pattern. Scope 1 and Scope 2 target is combined and not measured separately.

3) Value is based on a linear progression. Our impact is not expected to follow a linear pattern.

Table 18. Gross scopes and total emissions.

To create an accurate emission calculation the most relevant data and methodologies have been used.

Scope 1: Emissions of Fuels of cars or machines owned or used by the company: Non-electric vehicles.

- F-Secure's Scope 1 emissions come from fuel combustion in company vehicles. Emissions are calculated based on fuel consumption data from our leasing car system in Finland and country representatives elsewhere. Data forms vary by country, leading to different calculation methods. When car models are unknown, average values are used.
- The emission factors, sourced from Statistics Finland, convert fuel data into GHG emissions in metric tons of CO₂e. These emission factors were selected as they represent the most accurate emission factor for the calculation. F-Secure has most of its vehicles in Finland.

Scope 2: Emissions of purchased electricity, heat and cooling

- F-Secure uses both market-based and location-based methodologies for Scope 2 calculations. Data on purchased electricity is collected from six sites via country representatives. In terms of limitations and assumptions, for January 2024, Kuala Lumpur's electricity consumption was estimated based on other months. Emissions from heating (except Finland) and cooling are calculated using the office area and heating/cooling factors. Kuala Lumpur's office is assumed not to require heating due to its tropical climate.
- Emission factors are from multiple authorities, including the Energy Authority, Carbon Footprint, GreenTech Malaysia, Statistics Finland, Forum Energii, Umweltbundesamt, and the European Commission.

Scope 3: The most significant GHG emission categories in Scope 3 are Category 1 (Purchased goods and services) and Category 6 (Business travel). These categories account for the majority of our GHG emissions across all scopes. We use methodologies and principles from the GHG Protocol Corporate Value Chain (Scope 3) Accounting and Reporting Standard (Version 2011). In scope 3 category 1 and category 6, spend-based calculations were used.

Category 1: Purchased goods and services (excluding data center services)

- Values are derived from our financial reports, representing the expenditure on these goods and services. Emissions from some vendors are calculated separately by comparing their emissions to their revenue, and these vendor expenses are excluded from the financial report data to avoid double counting. Assumptions and limitations include that vendor-specific emissions are based on data from the previous reporting year due to reporting schedules. Also, data for company computer/laptop purchases was only available for Europe and the US, so other regions were extrapolated based on the employee count.
- Used emission factors come from Lenovo and Exiobase.

Category 1 sub category: Data center services

- There is a 3-month delay in retrieving figures in AWS (Amazon Web Services). VPN energy usage is primarily provided by Ficolo, our Finnish VPN server provider. Other VPN providers are unable to provide our electricity usage and Finnish server electricity usage is used to extrapolate emissions based on the known traffic used in each of our server sites, which is then mapped onto the emissions model in their respective country's emissions factor.
- Emission factors used are AWS, EEA (European Environment Agency), the Australian government, Carbon Footprint, the Government of Canada, Ficolo, Climate Transparency, the Singapore government, EPA (United States Environmental Protection Agency), the Vietnam government, and GreenTech Malaysia.

Category 6: Business travel

- In Category 6, flight data comes from two travel systems and company HR systems. For the HR system, the destination and arrival airports were obtained, and emission calculators were used to get either emissions or flight lengths. Assumptions were made to get flight lengths for all flights.
- Emission factors used are from Defra.

Categories 3, 5, 7, 8 and 11:

- In Category 3, fuel- and energy-related activities are calculated based on Scope 1 and Scope 2 values. Emission factors used are GLEC (The Global Logistics Emissions Council), Defra and the UK Government.
- In Category 5, no waste amounts were available, so waste generated in the office is estimated by extrapolating general waste amounts and types generated in a conventional office. Laptop and monitor -data was collected from the Finnish offices and extrapolated to other offices based on personnel per office. Emission factors used are Lenovo and the Environmental Protection Agency: GHG emission factors hub.
- In Category 7, data for work travel distance and type of travel was based on external data sources and are estimations. Office workdays were calculated

based on Helsinki and Oulu office data for other sites. Emission factors used are from Defra, Statistics Finland, GreenTech Malaysia, Carbon Footprint, and EEA.

- In Category 8, the emissions from home offices and coworking spaces are assumed to come from electricity consumption from the use of ICT equipment since no specific data from the used spaces were available. Home offices and coworking spaces are not separated for the analysis as they work similarly. Emission factors used are Carbon Footprint, EPA and Climate Transparency Report India.
- In Category 11, it is assumed that all sold products are taken into use. Emission factor used is from Statistics Finland.

Categories included and excluded from F-Secure's Scope 3 calculations are enclosed in the Table 19, *Scope 3 categories*.

Scope 3 category	Categories included in F-Secure Oyj's calculations
1. Purchased goods and services	x
2. Capital goods	Not relevant, F-Secure has not purchased or acquired capital goods
3. Emissions from fuels and energy that are not included in scope 1 or scope 2 emissions	x
4. Upstream transportation and distribution	Not relevant, F-Secure does not have upstream transportation or distribution
5. Waste generated in operations	x
6. Business travel	x
7. Employee commuting	x
8. Upstream leasing-commodities	x
9. Downstream transportation and distribution	Not relevant, F-Secure does not have downstream transportation or distribution
10. Processing of sold products	Not relevant, F-Secure does not have processing of sold products as our product is software
11. Use of sold products	x
12. End-of-life treatment of sold products	Not relevant, no physical products are sold by F-Secure
13. Downstream leasing-commodities	Not relevant, F-Secure does not lease any assets
14. Franchisee's emissions	Not relevant, F-Secure does not have operation of franchises
15. Investments	Not relevant, F-Secure does not have investments that falls into this category

Table 19. Scope 3 categories.

F-Secure has no operational control of associates, joint ventures or unconsolidated subsidiaries, nor do we have operational control of contractual arrangements in joint arrangements that are not structured through an entity.

The emission factors used are carbon dioxide equivalents, except for any specifically mentioned exceptions. This means that in addition to carbon dioxide, other greenhouse gases listed in the Kyoto Protocol, such as CH₄, N₂O, HFCs, PFCs, SF₆, and NF₃ are also included. Additional greenhouse gases may be considered when significant. The equivalents have been calculated using a 100-year time horizon to calculate CO₂eq emissions of non-CO₂ gases.

E1-6 GHG intensity based on net revenue

E1-6 GHG Intensity

F-Secure calculates GHG intensity based on net revenue by dividing total GHG emissions (t CO₂eq) by net revenue (€). Values are represented both in market-based and location-based methods. Net revenue is based on our financial statement [\(Cross-reference to financial section 3. Revenue\)](#) and our E1-6 GHG intensity is presented in the table below.

GHG intensity per net revenue	2024 base year
Total GHG emissions (location-based) per net revenue in millions (tCO ₂ eq/MEUR)	58.76
Total GHG emissions (market-based) per net revenue in millions (tCO ₂ eq/MEUR)	58.46
Net revenue used to calculate GHG intensity	
Total net revenue (in financial statements) MEUR	146.3

Table 20. GHG intensity per net revenue.

Sustainability Statement - Social



S1 – Own workforce

SBM-3 Material impacts, risks and opportunities

F-Secure acknowledges the value of its workforce and has identified key impacts, risks, and opportunities (IROs) related to working conditions, equal treatment, and career development.

By fostering an inclusive culture, promoting equality, and ensuring a healthy work-life balance, we create an environment where employees can thrive. The risks, such as discrimination, burnout, and inequitable opportunities, are addressed by opportunities like strengthening diversity and inclusion, implementing wellness programs, and enhancing career development and succession planning.

These opportunities not only mitigate the associated risks but also create positive outcomes for both employees and the business. The relationship between risks and opportunities is interconnected, as focusing on opportunities helps reduce risks and strengthens the company's overall strategy. Our risk management strategies are designed to ensure that risks are taken into account in our business model, and aligning with our long-term goals for employee satisfaction, retention, and business success.

F-Secure has identified the following risks and opportunities related to our impacts and overall dependencies with our workforce as described in the table below.

Own workforce list of IROs

	Material impact, risk or opportunity	Description
Working conditions		
Working time		
Opportunity (OO)	Expand use of worktime tracking on EU level	Use of work tracking system on EU level
Adequate wages		
No IROs identified.		
Social dialogue		
No IROs identified.		
Freedom of association, the existence of works councils and the information, consultation and participation rights of workers		
No IROs identified.		
Collective bargaining, including rate of workers covered by collective agreements		
No IROs identified.		
Work-life balance		
Actual positive impact (OO)	Number of annual holidays	F-Secure offers more days off than some (for example US) countries require.
Health and safety		
Risk (OO)	Workload and mental wellbeing	Rising trend in mental health related absences detected.

	Material impact, risk or opportunity	Description
Equal treatment and opportunities for all		
Gender equality and equal pay for work of equal value		
Actual positive impact (OO)	Promoting gender equality	Recruiting and advancing women and under-represented groups and mitigate the gender pay gap.
Training and skills development		
Opportunity (OO)	Learning and development	Opportunity to further ramp up strategic learning and development activities and track investment into learning activities. (Transparency on budget and result)
Opportunity (OO)	Critical strategic competences	Understand which are the critical competences internally which are critical for our strategy.
Risk (OO)	Talent acquisition and retention	Loss of key persons or inability to acquire new talent
Employment and inclusion of persons with disabilities		
No IROs identified.		
Measures against violence and harassment in the workplace		
Actual positive impact (OO)	Inclusive culture with a speak up-culture	We ensure through our company culture that we have an inclusive culture where the workplace is a safe environment for everyone. We foster a speak-up culture ("dare to care").
Measures against violence and harassment in the workplace		
Opportunity (OO)	Employer reputation	Especially younger generations value DEI topics and we would need to ensure that F-Secure meet expectations.
Risk (VC)	Partner retention and acquisition related to DEI requirements	In our growth markets (example US) DEI is of increasing importance and requirements will grow and may become critical in retaining and acquiring partners

	Material impact, risk or opportunity	Description
Other work-related rights		
Child labor		
Due to the nature of F-Secure employees that are highly educated specialists the risk of Child labor is considered extremely low. No opportunities or impacts identified.		
Forced labor		
Due to the nature of F-Secure operations the risk is considered low. No opportunities or impacts identified.		
Adequate housing		
Not material as housing is not part of F-Secure contracts. No opportunities or impacts identified.		
Privacy		
Due to the nature of F-Secure operations the rights to privacy are not at risk. No opportunities or impacts identified.		

Table 21. Own workforce IROs.

Interaction with strategy and business model

Risks and opportunities and our strategy and business model

The relationship between the material risks and opportunities arising from the impacts and dependencies on our workforce is integral to F-Secure's strategy and business model. Risks such as employee burnout, discrimination, and high turnover are addressed through initiatives aimed at improving employee well-being, career development, and diversity. These efforts are crucial to retaining talent and maintaining productivity, which are vital components of our strategy for sustainable growth.

By focusing on opportunities like career development, diversity, and work-life balance, F-Secure strengthens its workforce, which in turn supports the company's business objectives of growth. The risks and opportunities are not only managed but actively shape and adapt our strategy and business model, ensuring a positive relationship between the workforce's impact and the company's long-term success.

Disclosure scope

All employees who can be materially impacted by F-Secure are included in the scope of this disclosure. This includes impacts that are connected with our own operations and value chain.

Types of employees

F-Secure measures full-time employees by FTEs (full-time equivalent) and has no "non-guaranteed hours" - employees. Our "other" – category includes individuals with facility access but no system access, like Board members, facility services and cleaners.

The company's employees are in permanent or fixed-term employment with the F-Secure company in their country of residence. Most of the employment relationships are full-time, adhering to current laws and regulations of the respective country or region. The company also employs subcontractors, who may be independent contractors or individuals provided by a third party. Each subcontractor has a contract with the company either directly or through a third party.

- Permanent employees: Employed with no predefined end date to their contract.
- Fixed-term employees: Hired for a specific duration with defined end dates and for specific projects/reasons, after which the employment relationship is either extended/terminated/converted to permanent status.
- Contractor: All non-employees are called Contractors (alternatively Contingent workers or subcontractors)

The types of non-employees include "Employee-like", "Consultant" and "Other" as described in more detail next.

Employee-like (also called "Fellowlike"):

- Integral part of F-Secure teams, participating in daily activities and team meetings. Usually, contracts are fixed and time-based contracts. Regardless of the contractor status, our contract with any non-employees is with a legal entity and not with a natural person.
- Examples of Employee-like who work for a third party engaged in "labor activities" and whose work is managed by the company: People who do the same work as our employees in case those are temporarily absent (due to illness, vacation, parental leave, etc.) or work in the same workplace as our employees

Consultant

- Consultants are contractors who supplement F-Secure's workforce on a project basis, related to a specific assignment or project in question. Regardless of the contractor status, our contract with any non-employees is with a legal entity and not with a natural person.
- They may have the necessary access to a F-Secure facility or to F-Secure systems based on e.g. a project or frame agreement to perform their duties.

Other

- Covers non-employees who have access to a F-Secure facility but not to F-Secure systems such as Board members or people providing facility services.

Material positive and negative impacts

F-Secure is committed to fostering a workplace that supports employee well-being, inclusivity, and work-life balance. The company ensures fairness across its global operations by addressing regional disparities and implementing initiatives

that promote a thriving workforce. F-Secure's permanent employees, fixed-term employees, and contractors categorized as Employee-like are the individuals who can benefit positively from these initiatives.

Below are actual **positive impacts** and initiatives aligned with the company's **Impacts, Risks, and Opportunities (IROs)** framework:

1. Promoting gender equality

By advancing women and underrepresented groups in the workforce, while actively working to mitigate the **gender pay gap**, F-Secure ensures inclusivity and fairness are deeply embedded in its culture. In 2024 we've already addressed pay-gap issues as part of our annual salary review process, as well as through participating in initiatives such as Women in Tech actively driving diversity at F-Secure.

2. Inclusive culture with a speak-up-culture

The company fosters a **safe and supportive environment** through its "dare to care" value, which empowers employees to voice concerns and share ideas without fear of discrimination or reprisal. This **speak-up culture** reinforces equity, strengthens diversity, and ensures a thriving, inclusive workforce.

3. Number of annual holidays and well-being

F-Secure addresses regional disparities by offering additional vacation days in regions with fewer annual holidays, such as the US. This policy promotes **equitable work-life balance**, reducing burnout risks and enhancing employee satisfaction.

Additionally, flexibility is a cornerstone of F-Secure's approach to employee well-being. Remote work options in regions such as India and Malaysia provide employees with greater control over their schedules. This reduces commuting time, enhances job satisfaction, and supports a **better work-life balance**, transforming potential challenges into opportunities for building a happier, more effective workforce.

F-Secure supports its workforce's physical and mental health through comprehensive health and well-being programs in regions including Finland, India, the US, and Malaysia. These programs address stress and burnout risks while fostering long-term health and satisfaction. By ensuring access to essential support services, F-Secure demonstrates its **dedication to employee well-being**, enabling employees to thrive.

We have not identified any material negative impacts related to our own workforce, whether widespread or systemic such as child labor or forced labor in specific regions or linked to individual incidents such as workplace accidents.

Risks and opportunities arising from impacts and dependencies

F-Secure has not identified any material impacts on its workforce from transition plans for reducing negative impacts on the environment.

Furthermore, F-Secure does not operate in industries/sector where the risk of forced, compulsory or child labor is significant. F-Secure has an office in Malaysia and employees in India which are considered countries with higher risks. However, F-Secure hires educated specialists and leaders and conducts background checks on its employees, which reduces the risk.

This low risk is due to the nature of F-Secure's software-based business and the roles and types of people working for F-Secure limits the risk of any greater harm occurring to any employee. F-Secure has a company culture and several policies and procedures in place limiting discrimination or harassment. We believe that equal opportunities should be available for all employees. In the materiality assessment, F-Secure has not identified people who are or may be negatively affected or at greater risk than other employees.

Risks and opportunities and relation to groups of people

At F-Secure, our policies are designed to apply equally across the entire workforce. While F-Secure's overall approach is inclusive and applies broadly to our workforce, we recognize that some initiatives have a greater impact on a specific region or employee group due to local circumstances, business needs, or employment type.

Examples of instances where specific groups of employees or non-employees may experience unique impacts or opportunities include:

- **Health and Well-being Programs by Region:** Tailored health insurance and programs improve employee well-being, with regional variations like cashless medical services in India and Malaysia.
- **Targeted Opportunity:** These programs directly support employees' well-being by reducing health risks, thus improving employee satisfaction and retention. This approach is aligned with Health and Safety and working conditions as it provides region-specific benefits that address local healthcare challenges while promoting a healthier workforce.
- **Learning and Development Opportunities:** Targeted training for specific roles like R&D or leadership helps upskill employees, mitigate skill shortages, and support career growth while ensuring opportunities for all.
- **Positive Impact on Gender Equality:** Focus on recruiting and advancing women and other underrepresented groups, closing the gender pay gap, and enhancing diversity and inclusion to mitigate workplace inequality risks.

These initiatives directly support creating opportunities for underrepresented groups while addressing risks related to workplace inequality and turnover.

Impact, risk and opportunity management

S1-1 Policies

This section specifies the material sustainability topics addressed by each policy and clearly outlines the target audience for each policy, ensuring transparency and alignment with F-Secure's sustainability objectives.

F-Secure DEI policy

The DEI policy sets guidelines to promote diversity, equity, and inclusion, aligning with our values and Code of Conduct. It creates an inclusive environment where everyone can thrive and defines DEI at F-Secure including a mission statement aligned with business objectives and outlines anti-harassment and non-discrimination guidelines. The policy also sets diverse targets and tactics for talent acquisition and decision-making, ensures legislative compliance, and establishes accountability and reporting mechanisms. Our DEI policies include training, targeted recruitment, and programs that support vulnerable groups and promote leadership development, pay equity, and gender gap closure. The DEI Committee drives initiatives, ensuring a safe and inclusive environment, and regular reporting tracks our progress. DEI is central to our culture, sustainability strategy, and corporate responsibility. To ensure effective implementation, we conduct DEI training sessions, including mandatory training for new hires and periodic refreshers for all employees. Additional details on mitigation actions can be found in the section (S1-3). For reporting incidents, refer to section "S1-17 Incidents, complaints and severe human rights impacts." This policy addresses IROs related to measuring against violence & harassment in the workplace, diversity, and gender equality by ensuring alignment with company values, culture, and the Code of Conduct. This policy applies to all Employees, Employee-like contractors, Leadership Team members, and administrative bodies of F-Secure. It is approved by the Chief People Officer (CPO).

F-Secure Recruitment Policy

F-Secure's global recruitment policy ensures fair and transparent hiring processes, adhering to local requirements and compliance factors like non-discrimination laws and background checks. It aligns with our values, culture, and Code of Conduct, covering the importance of recruitment, diversity and inclusion, the overall recruitment process, employer branding, recruitment metrics, legal considerations, and policy review. This policy addresses IROs related to training and skills development, aligned with DEI goals. This policy is aligned with local compliance integrated with international principles such as the ILO Declaration

on Fundamental Principles and Rights at Work combining it with ILO principles on Non-discrimination and equal opportunity. This policy applies to Employees and Employee-like contractors taking part in hiring processes. The policy is approved by the Chief People Officer.

F-Secure Health and Well-being Policy

Our Health and Well-being Policy outlines principles and practices to ensure employee health and well-being, including cultivating a healthy work culture, the role of leadership, compliance with local health requirements, health activities, continuous learning, promoting well-being through speed and innovation, flexible work environments, and monitoring the success of these activities. In addition to our internal guidelines, we are fully committed to adhering to local legislation and requirements in all countries where we operate, ensuring that our practices meet the regulatory standards. This policy addresses IROs related to Work-life balance, health and Safety and adheres to ILO standards on occupational safety and health. This policy applies to all F-Secure employees. This policy is approved by F-Secure CFO.

F-Secure Learning and Development Policy

The F-Secure Learning and Development Policy emphasizes continuous learning to enhance workforce expertise, foster collaboration, and maintain a structured learning framework. It covers defining training, roles and responsibilities, the learning framework, learning-related data management & reporting, and measuring the effectiveness of learning efforts. This policy addresses IROs related to training and skills development. This policy applies to F-Secure employees, and in certain cases as described in the policy, Employee-like contractors. This policy is approved by F-Secure CPO.

F-Secure Rewards and Recognition Policy

Our Rewards and Recognition Policy outlines principles and practices for fair and transparent rewards, covering, for example, policy principles, our job architecture, base salary, benefits, incentive plans, recognition, and pensions. This policy addresses fair and equal treatment and transparent working conditions. Defines a rewards framework consistent with global standards, ensuring equity and transparency in line with OECD and ILO principles. This policy applies to all F-Secure employees. It does not apply to consultants or others not employed by F-Secure. This policy is approved by F-Secure CPO.

Human Rights Policy Commitments

We are committed to protecting human and labor rights in all our business, operations, and culture. Human rights are incorporated in our Code of Conduct with which all F-Secure employees must comply. The main international principles that F-Secure considers include those mentioned below.

- **OECD Guidelines for Multinational Enterprises:** F-Secure's workforce-related policies are designed to adhere the OECD Guidelines for Multinational Enterprises by emphasizing fair labor practices, employee well-being, and respect for human rights.
- **United Nations Global Compact:** F-Secure's workforce-related policies are designed to adhere to the United Nations Global Compact principles, supporting the respect and promotion of human rights, labor standards, and ethical practices.
- **United Nations Guiding Principles on Business and Human Rights:** F-Secure has designed to adhere its workforce policies with the United Nations Guiding Principles on Business and Human Rights by committing to respect and protect the human rights of all employees across its global operations.
- **United Nations Convention against Corruption:** Through regular training and a clear Code of Conduct, F-Secure empowers employees to recognize and report unethical behavior, while safeguarding against any influence that could compromise the organization's ethical standards.
- **International Bill of Human Rights:** F-Secure upholds the principles outlined in the International Bill of Human Rights by ensuring that all its workforce practices are rooted in equal treatment and opportunities for all.
- **The Declaration of the International Labour Organisation (ILO) on Fundamental Principles and Rights at Work:** F-Secure is committed to adhering with the principles outlined in the Declaration of the International Labour Organisation (ILO) on Fundamental Principles and Rights at Work, ensuring that all employees are provided with a fair and respectful working environment.

Special focus is placed on 1) Respect for Human Rights, 2) Labor Rights and Safe Working Conditions, and 3) Application of Standards.

1. Respect for Human Rights

F-Secure honors internationally recognized human rights standards and strives to prevent any adverse human rights impacts. In cases where such impacts occur, we take swift and effective action to remediate them. Our commitments include

respecting freedom of opinion and expression, as well as freedom of conscience and religion. F-Secure combats digital scams with advanced detection, tailored tools, and user education, protecting digital lives and supporting human rights now and in the future.

2. Labor Rights and Safe Working Conditions

We respect labor rights and comply with local laws as a minimum standard for respecting the rights of all humans at work. We respect the freedom of association and employees' right to organize. We actively ensure safe and healthy working conditions. We do not tolerate any use of child labor, any form of forced labor, human trafficking, or any other human rights violations.

3. Application of Standards

In cases where local laws differ from our **Code of Conduct**, the following principles apply:

- If local laws are less restrictive than the **Code of Conduct**, the **Code of Conduct** prevails.
- If local laws are more restrictive, those laws are followed to ensure compliance.

F-Secure suppliers and partners are also expected to act responsibly and comply with the principles set in the Code of Conduct and local laws.

By incorporating these principles into our operations, F-Secure ensures respect for human rights and labor standards while fostering a culture of accountability and inclusivity.

Engagement with our workforce

F-Secure has established systematic methods to engage with its workforce:

1. **Employee Engagement:** Monthly town halls with Q&A, function-specific all-hands meetings, a Leadership Forum for managers, and a digital suggestion channel promote inclusive participation.
2. **Employee Feedback:** Biannual anonymous surveys gather feedback, leading to action plans visible to the work community and assessments of engagement activities.

3. **Regular Discussions:** Monthly meetings between the People & Culture Operations Director, HR Board, and local representatives address current topics and issues.
4. **Project-Based Engagement:** Employees are involved in specific processes or projects, such as people processes or cultural initiatives.
5. **Collective Bargaining Compliance:** F-Secure adheres to collective bargaining agreements in Finland, France, and Spain, ensuring alignment of policies and practices through the People & Culture Operations Director.

Measures to provide and/or enable remedy for human rights impacts

We aim to avoid adverse human rights impacts and in case those occur, we take actions to remediate them. Every employee at F-Secure has the right and the obligation to raise a concern about a violation of the Code of Conduct, including human rights.

F-Secure provides multiple ways to raise a concern. The employee may talk to their direct Manager, Legal, or HR. Concerns may also be reported via the Whistleblowing channel. Employees may also write to our CEO or our Board.

All concerns are handled confidentially. Each reported concern will be reviewed. Appropriate measures will be taken against violations of the Code of Conduct, including human rights. We are committed to maintaining a culture in which everyone feels comfortable raising good faith concerns about violations of the Code of Conduct. We do not tolerate adverse action against anyone who raises a good faith compliance concern.

Policies addressing trafficking in human beings, forced labor and child labor

F-Secure's **Human Rights Policy** prohibits child labor, forced labor, human trafficking, and other violations, with background checks as part of our **Recruitment Policy** and compliance with local labor laws, regularly updated to align with legal requirements.

Workplace accident prevention

F-Secure tracks and manages workplace accidents using our HR systems, where all incidents are reported and monitored to ensure compliance with local laws and regulations. While physical injuries are rare in the software and cyber security industry, any workplace accident or harm is recorded and managed according to country-specific practices. Our intranet provides employees with detailed information on workplace safety, which is accessible to all. We define

an occupational accident as an unexpected event resulting in injury, including incidents that occur within the workplace, during business trips, or while carrying out employer-ordered errands. Additionally, we address injuries such as muscle or tendon pain, which may be compensable under certain conditions.

Any occupational accident is addressed and handled according to the local legislation and requirements, and occupational healthcare provided by F-Secure.

S1-2 Processes for engagement about impacts

F-Secure engages directly with its workforce and workers' representatives. Engagement occurs at various stages of decision-making and operations. Key engagement activities include:

- **Direct engagement:** Monthly town halls with Q&A sessions, function-specific all-hands meetings, and a monthly Leadership Forum with Team Leaders.
- **Surveys:** F-Secure conducts personnel surveys twice a year. Through the survey, all employees can provide feedback and input. The results are analyzed and presented at company, function, and team levels wherever there are five or more responses
- **Workers' representatives:** The People and Culture Operations Director organizes monthly meetings with the Shop Steward to address and discuss current topics and issues. Also, we have an HR Board that meets monthly to address and discuss current topics together with the Shop Steward and country-specific elected representatives (People & Culture Advisor).

The most senior roles responsible for ensuring engagement are the CEO, Chief People Officer and the rest of the Leadership Team. The CEO or LT representative leads the town halls and the monthly Leadership Forum. The People & Culture Operations Director is responsible for ensuring compliance with collective bargaining agreements and for overseeing engagement with the Shop Steward and elected representatives.

F-Secure conducts biannual personnel surveys to gather employee feedback. Respective action plans using an available template are made at the same organizational levels. We aim to make all actions taken based on the feedback visible for the whole work community in town halls and other internal communications. The survey also serves as a channel to assess how we have succeeded in engagement activities and all our engagement activities have feedback opportunities.

F-Secure complies with collective bargaining agreements in countries like Finland, France, and Spain. These agreements ensure respect for the human rights of the workforce and help the company engage with workers' representatives. The agreements enable F-Secure to gain insight into the perspectives of its workforce by setting up clear processes for engagement and shared decision-making with employee representatives.

F-Secure ensures inclusivity by providing accessible Learning Management Systems, survey tools with screen reader compatibility, and features like text-to-speech and closed captioning. Our virtual townhalls include real-time captioning, and recordings are available in audio and text. We also ensure wheelchair-accessible meeting rooms and clear, simple language in all communications to support employees with mobility or cognitive disabilities.

These steps are part of our broader commitment to creating an inclusive environment where all employees, regardless of their abilities, feel supported and empowered to participate.

S1-3 Processes to remediate negative impacts and channels to raise concerns

F-Secure strongly encourages its employees to speak up if they have concerns related to their own employment or daily work. The Whistleblowing Channel is only a secondary alternative for reporting issues, please refer to G1-1 for more details. Such matters should primarily be reported to one's own team leader, local People & Culture advisor or via personnel surveys. An employee can do that verbally or through electronic means. If the issues relate to one's own team leader, the employee should contact the team leader's leader or the P&C. Employees can also contact the Shop Steward or employee representatives. They may also write to our CEO or our Board of Directors.

All employees have the right and the obligation to raise concerns. All team leaders and the People and Culture team must handle the concerns. All concerns are handled confidentially, and each reported concern will be reviewed. According to the review, appropriate actions are taken with the relevant stakeholders with ongoing follow-ups if needed.

We are committed to maintaining a culture in which everyone feels comfortable raising good-faith concerns about their employment or daily work. We do not tolerate adverse action against anyone who raises a good-faith concern. We actively communicate and train our team leaders and employees on the ways and channels of raising any concerns. Channels are updated regularly on our intranet.

At F-Secure, we assess awareness and trust in our structures and processes through regular employee surveys (such as the personnel survey conducted biannually) and feedback mechanisms (including 1-on-1 meetings with team leaders and town halls). These surveys and feedback channels are designed to gauge employees' understanding of our internal processes and their confidence in the company's commitment to transparency, ethics, and fairness. Additionally, we track specific trust metrics such as eNPS (employee Net Promoter Score). We ensure that these channels are easily accessible to all employees, including those employed at different levels. We also use the results of these assessments to take corrective actions and ensure continuous improvement.

S1-4 Actions and resources

F-Secure actively takes actions to ensure positive effects on its workforce while addressing risks and actual and potential material impacts. The company's initiatives are aligned with fostering a stable, equitable, and inclusive working environment as described next. We have not identified any actual or potential negative impacts related to our own workforce exceeding the threshold set in the impact, risk and opportunity assessment as part of the DMA.

Secure Employment and Flexible Workplace

F-Secure offers stability by prioritizing permanent contracts over fixed-term agreements, minimizing uncertainty for employees. The company's remote work policy allows employees to work from home several days a week, promoting work-life balance and improving employee well-being.

In regions like India and Malaysia, where commuting can be time-consuming and stressful, remote work enhances employee satisfaction and productivity while enabling a more diverse and inclusive workforce.

Healthcare and Well-being Programs

F-Secure ensures that its workforce feels supported and secure through comprehensive healthcare and well-being programs. These initiatives prioritize employee health and create a stable and reliable employment experience.

Fair Working Environment

At F-Secure, we are continuously evaluating and updating our policies and procedures across all locations to ensure full compliance with local, regional,

and national regulations. This proactive approach helps us maintain a fair and transparent work environment for all employees, fostering trust and inclusivity within the organization.

We are also committed to providing a positive work-life balance through a comprehensive suite of benefits designed to support employees beyond the workplace. These benefits include health insurance and vacation/leaves, which offer resources for mental health, and personal well-being. For example, in the US, our leave policies, as outlined earlier, not only meet statutory requirements but also promote equality for all our employees worldwide.

Through these initiatives, F-Secure ensures that all locations provide a fair, equitable, and supportive environment, prioritizing employee well-being and ethical governance.

Promoting Gender Equality

We focus on promoting job openings to underrepresented groups to ensure diverse talent pools. This ensures a robust workforce capable of addressing diverse market needs and reduces the risk of talent shortages by tapping into a broader range of skills and perspectives. We do this by targeting our outreach using multiple online channels, we strive to attract candidates from various backgrounds, contributing to a more inclusive workplace. Other tactics used to promote gender equality are, i.e. strategic employer branding and sourcing, DEI Committee and partnerships with organizations like “Women in Tech” and promoting diversity through a “diversity bonus” when referring new employees.

F-Secure promotes equal pay. Equal pay means that any differences in pay and benefits between employees performing the same or similar work, or work of equal value, must derive from objective reasons and cannot be due to gender (or any protected characteristics). It does not mean that employees must be paid the same.

F-Secure is committed to promoting gender equality and ensuring that women are well-represented in leadership roles. The goal is to reduce the gender disparity in leadership positions. There is a risk that the organization may not have a balanced representation of genders in leadership roles, potentially affecting diversity and inclusivity in decision-making, innovation, and organizational performance. To mitigate this risk, F-Secure has initiated a leadership development program aimed at identifying and grooming high-potential female employees for future leadership roles. The program includes mentorship, training, and leadership experience, along with specific recruitment initiatives to attract women to senior leadership positions.

Inclusive Culture and Speak-Up Culture

F-Secure fosters an inclusive environment where employees feel safe to raise concerns. This enabled through:

- **Training Leaders:** Leadership programs focus on psychological safety, active listening, and feedback.
- **Feedback Channels:** Regular open forums like town halls encourage employees to voice concerns. Employees are celebrated for embodying cultural values, such as giving and receiving constructive feedback.
- **Action on Feedback:** Transparent development plans are co-created with employees and reviewed twice annually to ensure follow-through on concerns and feedback.
- **Anonymous Reporting Channels:** An anonymous whistleblowing channel is available for raising concerns, ensuring confidentiality and prompting action.

The company measures the effectiveness of these initiatives through biannual personnel surveys, KPIs like eNPS, retention rates, and culture and leadership assessments.

Key Actions Taken in the Reporting Year:

- **Secure Employment:** Transitioned employees to permanent contracts where feasible, minimizing fixed-term arrangements to ensure stability and job security. Transitions were completed during the reporting year and are continuously evaluated.
- **Flexible Workplace Policies:** Expanded global remote work options, enabling better work-life balance and environmental benefits by reducing commute emissions. Implementation completed during the reporting year, with ongoing adjustments based on employee feedback.
- **Health and Well-being Programs:** Launched healthcare initiatives, including mental health resources and wellness benefits tailored to regional needs. Renewal and enhancements are continuously evaluated.
- **Gender Equality and Diversity Initiatives:** Implemented targeted recruitment for underrepresented groups. Actions implemented during the reporting year, with further measures planned for subsequent years.
- **Inclusive Culture Building:** Fostered a speak-up culture via leadership training, feedback forums, and anonymous reporting mechanisms. Programs launched

during the reporting year were completed and scheduled for regular follow-ups in the next cycle.

Planned Future Actions:

- 1. Enhance leadership development programs to increase the representation of women and underrepresented groups in leadership roles. Female employees leadership development program. Recruitment initiatives focus on attracting women to senior positions.
- 2. Expand global healthcare initiatives to cover additional services such as mental health resources and wellness benefits to enhance employee well-being globally.
- 3. Launch targeted training modules for fostering DEI and employee growth. For example, for DEI we have "Mother's in Business" and ambassador program, and for employee growth F-Secure launched the Aspiring Leaders program and the Leadership Foundation program.

These activities will start and progress will be evaluated during 2025. We envision them to continue during the strategy period (2025-2027).

Expected Outcomes:

- Enhanced employee satisfaction.
- Progress toward achieving diversity, equity, and inclusion (DEI) goals.
- Reduction of workforce-related risks, such as disengagement and health issues.

By acting on feedback and fostering an inclusive culture, F-Secure achieves a positive impact on the workforce and enhanced employee satisfaction, retention, and engagement while mitigating risks associated with well-being, inability to hire and acquire talent, overall disengagement, and lack of transparency.

Additional initiatives to deliver positive impacts

We believe that success is achieved collectively and internally call this "Fellowship". Our culture emphasizes that "we" surpasses "me," fostering trust and accountability within our teams. Agility and speed are pursued inclusively, ensuring that no one is left behind. This Fellowship culture becomes tangible when we act in alignment with our values, evident in how we lead, connect with, and support one another.

To deepen our commitment to Fellowship, we implemented "Value Weeks," a four-week program featuring keynote speeches, panel discussions, pre-recorded talks,

and skill-building exercises. Each week focuses on a specific core value, creating a positive spirit, strengthening unity, and aligning our culture with strategic objectives. These events were voluntary and open to all employees, fostering engagement across the organization.

1. Competence Development

F-Secure prioritizes continuous learning to stay industry-leading, encouraging employees to take ownership of their development with support from team leaders and People & Culture. The Leading Performance Process aligns career goals with organizational objectives, while the 70/20/10 learning model fosters everyday learning. A Learning Management System (LMS) provides easy access to training resources, and feedback mechanisms improve program effectiveness.

2. Diversity, Equity, and Inclusion (DEI)

F-Secure promotes DEI through a global policy and official targets to ensure meaningful progress. Key initiatives such as Talent Acquisition embed DEI in recruitment to create diverse talent pools. DEITalks platform launched in 2024 to raise awareness, foster learning, and celebrate diversity within our core values: Just Do It, Dare to Care, I Make an Impact, and Keep Focus. These efforts, led by an active DEI Committee, strengthen inclusivity and cultural awareness, creating a more supportive workplace.

3. Improved Working Hours & Overtime Management

F-Secure ensures fixed working hours for employees, with fair compensation for overtime when needed. We actively monitor and adjust work schedules to maintain transparency, fairness, and a healthy work-life balance, while ensuring compliance with legal requirements and industry standards.

4. Employee Health & Well-being

We have implemented various initiatives to support the diverse health and wellness needs of our employees. In Finland, we offer 24/7 access to an Occupational Health Care Provider through a digital clinic or mobile app, ensuring immediate healthcare support. In other regions like India, the US, France, and Malaysia, we collaborate with Medical Insurance Providers to deliver comprehensive health coverage for employees and their families, including cashless services in India and Malaysia. These initiatives ensure our employees have easy and convenient access to necessary health services.

5. About Well-being

We have introduced a global mental well-being service. The service allows our employees to contact the service if there are any issues with stress, motivation, work-life balance, etc. The service is available in all the countries. The service is a preventive, solution-focused service that can be accessed even before the issues escalate to problems. In countries, like Malaysia, Mental well-being is included in the insurance package.

Tracking effectiveness in delivering outcomes for our own workforce

F-Secure employs systematic approaches to track and evaluate the effectiveness of its actions and initiatives in delivering meaningful outcomes for its workforce. These mechanisms ensure that the initiatives align with employee needs, organizational goals, and compliance standards.

1. Employee Feedback and Engagement Surveys

F-Secure regularly conducts anonymous engagement and satisfaction surveys, such as the Employee Net Promoter Score (eNPS), to monitor workforce morale, satisfaction, and engagement levels. The feedback obtained serves as a primary indicator of the success of our initiatives and guides future actions.

2. Audits and Policy Reviews

To uphold fair and equitable practices, F-Secure conducts regular evaluations to ensure compliance with local labor laws and international standards. Internal reviews such as the assessment of the Remuneration Policy, are discussed annually with the Personnel and Nomination Committee.

3. Monitoring Gender Equality Initiatives

F-Secure measures progress in gender equality by conducting pay gap analyses as part of the global salary review process. These assessments are carried out before and after salary reviews to ensure pay equity and to identify areas requiring further action.

4. Inclusive Culture and Speak-Up Initiatives

F-Secure fosters an inclusive workplace by evaluating its "speak-up" culture through biannual surveys, measuring KPIs like eNPS, retention rates, and leadership

assessments. Employee feedback is reviewed and acted upon for continuous improvement. No significant negative impacts have been identified.

Actions to mitigate material risks

To mitigate the risks related to employee workload and well-being, F-Secure has implemented targeted initiatives:

- **Well-being Engagement:** Regular engagement surveys include questions on workload and well-being, allowing us to identify and address concerns promptly.
- **Support Programs:** Well-being webinars and preventative health services provide employees access to coaching and tools to manage stress and workload.
- **Workload Management:** The "Leading Performance" process helps set clear, realistic goals, enabling better workload distribution.
- **Health Monitoring:** Absence data is tracked in Finland to identify trends and address potential systemic issues impacting employee health.

Effectiveness is measured through feedback from engagement surveys, participation rates in well-being initiatives, and analysis of absence trends. These tools enable us to adapt and improve our approach continuously.

F-Secure mitigates risks related to talent acquisition and retention by employing a structured and measurable approach:

- **Strategic Recruitment:** Talent Acquisition strategies are tailored to business goals, with clear plans for sourcing, recruitment timelines, and methods. Time-to-hire and attrition rates are tracked monthly to evaluate recruitment success.
- **Retention Efforts:** Comprehensive measures focus on onboarding, career development, leadership opportunities, and recognition to ensure employee satisfaction and engagement.

Key metrics to track the effectiveness of these actions include time-to-hire, voluntary and total attrition rates, and employee engagement scores. Feedback from onboarding surveys provides additional insights into areas for improvement.

DEI is integral to mitigating risks in partner retention and acquisition, particularly in markets with stringent expectations. Actions include:

- **Alignment with Standards:** Developing clear DEI policies and aligning with partner expectations to strengthen relationships.

- **Internal DEI Progress:** Promoting a diverse and inclusive workplace to meet market-specific DEI requirements and build trust with partners.

Effectiveness is monitored through regular reviews of DEI practices, alignment with partner DEI goals, and tracking partner retention and acquisition outcomes.

Actions related to material opportunities relative to our workforce

1. Expansion of Worktime Tracking Across EU Operations

F-Secure is expanding worktime tracking across its EU operations to ensure compliance with labor regulations, promote fairness, and improve transparency. This initiative will help monitor working hours, ensure equitable compensation, and support employee well-being while boosting productivity through standardized systems in all EU locations.

2. Critical competencies and Learning and Development Initiatives

F-Secure is enhancing its workforce development through a detailed capability analysis and employee surveys to identify skills gaps and create tailored growth paths. The company is leveraging its Learning Management System (LMS) to centralize training, track participation, and measure the impact of learning on performance. Effectiveness will be assessed through engagement surveys, LMS data, and performance evaluations.

3. Promoting Diversity, Equity, and Inclusion (DEI) for Enhanced Employee Reputation

F-Secure is committed to development projects that promote diversity, equity, and inclusion to strengthen the attraction and retention of talent and to build a work community where everyone has equal opportunities to succeed. F-Secure regularly evaluates its DEI practices, collects feedback from employees, and transparently reports on its progress. The DEI committee continuously guides and develops the plan to ensure that the measures are effective and meet the expectations of both current and future employees. The goal is to create a work environment that supports diversity, equality, and inclusion at all levels.

Preventing negative impacts on the workforce

F-Secure ensures that its practices do not cause material negative impacts on its workforce through a variety of measures:

1. **Policy Development:** All workforce-related policies are carefully designed to focus on the health, well-being, and professional growth of employees while minimizing any negative impact.
2. **Regular Feedback:** We continuously gather feedback from employees through surveys and engagement tools, such as eNPS, to monitor satisfaction and address any concerns in real time.
3. **Training & Development:** We offer comprehensive learning and development programs, ensuring employees are equipped to grow and thrive in their roles.
4. **Well-being Initiatives:** Programs to support employee health, such as preventative health services, work-life balance policies, and wellness initiatives.

Resources allocated to managing impacts

The People and Culture team at F-Secure is resourced to manage our material impacts on our own workforce.

The People and Culture team includes two teams, the Employee Experience team and the People & Culture Operations team. The Employee Experience team is resourced to handle employee experience and talent development, talent acquisition, and diversity and supports our various functions in their talent planning. This also includes strategic projects such as developing and enhancing company culture. The Operations team handles day-to-day activities such as payroll, performance and rewarding, HR systems, and supporting our regional offices and teams.

Metrics and targets

S1-5 Targets

F-Secure has defined the following absolute targets related to its own workforce

S1-5 Own workforce targets

Target	Baseline 2023	2024	2030 target
Gender Diversity (directors including leadership team, %)	F: 23 M: 77	F: 25.1% ; M: 74.9%	F: 33 M: 67
Gender Diversity (all employees)	Third gender not implemented, F: 30% M: 70%	M- 69.19%; F- 30.62%	No gender should represent more than 65% of workers.
Nationality among senior management	24	28	> 20
Age target (all employees, and age group are <30, 30-40, 40-50, 50-60 and 60-70)	Under 30: 22.1%, under 40: 35.7%, under 50: 29.4%, under 60: 11.1%, above: 60 1.7%	Under 30: 20,6%, under 40: 36,7%, under 50: 30,1%, under 60: 11,5%, above: 60 1,1%	No age group should represent more than 35% of the total
eNPS evolution	2	40	> 50
Performance and career review target	Baseline year is 2024	82.04%	98%

Table 22. Own workforce targets.

No negative impacts on our own workforce have been identified during the reporting period. As a result, no specific targets for reducing negative impacts have been established.

Methodologies for collecting and tracking against the target are based on F-Secure's HR systems as described in more detail under each target. However, metrics have been selected based on alignment with our material F-Secure ESG topics and ESG regulation, Double Materiality Assessment, and stakeholder feedback. Our long-term targets have also been approved by the Board of Directors.

S1-5 Progress towards targets

Diversity (DEI) related targets

These targets help us make intentional hiring and promotion decisions based on skills and competencies in alignment with our values, driving both inclusion and equality. These targets relate to our diversity policies.

These targets are set by the F-Secure Chief People Officer and apply to F-Secure globally. Alignment of targets with our policies is described under S1-1; Policies. We review progress regularly and should we identify negative trends or issues, our P&C teams build remediation plans accordingly.

1. Diversity, directors

We've set a 2030 gender target among our senior leaders that on the director level, 33% should represent females. These targets apply globally to all F-Secure employees, excluding contractors and employee-like consultants. The baseline year is 2023, with 23% female and 77% male representation among senior leaders. We report progress annually and our 2024 outcome for senior management diversity is 25.1% female and 74.9% male representation.

Progress is measured regularly using data from our HR management system, aligning also with the EU gender equality strategy 2020–2025 and the directive on gender balance in corporate boards.

2. Diversity, All employees

This target reinforces F-Secure's commitment to gender inclusivity beyond the binary categories of male and female, ensuring a fair representation of all genders and encouraging a culture of inclusion and belonging.

We've set a target that no gender (including third gender) should represent more than 65% of the workforce by 2030. This target applies globally to all F-Secure employees, excluding contractors and employee-like consultants. The baseline year is 2023 with 70% male representation. We report progress annually and our 2024 outcome is 69,2% male representation.

Related data is collected through the HR system, where employees can self-identify as male, female, or third gender. Our gender diversity goals align with international standards on gender equality, including the EU gender equality strategy.

3. Nationality among senior management

Maintaining nationality diversity ensures global representation in decision-making and fosters an inclusive environment where leadership reflects our diverse workforce. This helps challenge norms and improves decision-making processes.

F-Secure is already as of today diverse in terms of nationalities and our objective is to maintain or exceed 20 nationalities within senior leadership positions. These targets apply specifically to senior leadership positions and exclude contractors and employee-like consultants.

Our baseline year is 2023, with 24 nationalities represented among senior leaders. We report progress annually and our 2024 outcome is 28.

Related nationality data is collected through the HR management system and reviewed annually. This target aligns with F-Secure's goal of fostering diversity through cross-cultural leadership and international best practices.

4. Age target

Age diversity is essential for fostering a vibrant workforce with a wide range of experiences. By ensuring no single age group dominates, we create space for intergenerational learning, innovation, and mentorship.

We've set a 2030 target that no single age group (under or equal to 30, 31-40, 41-50, 51-60, Over 60) represents more than 35% of the total workforce. This target applies globally to all F-Secure employees, excluding contractors and employee-like consultants. Our baseline year is 2023, where the largest age group represents 35,7% of the workforce (30-40y). We report our progress annually and our 2024 outcome is that one age represents more than 35% which is the group 30-40y at 36,7%.

Related age data is collected through the HR management system and reviewed annually. This target reflects a commitment to creating a balanced workforce that fosters innovation and collaboration across all age groups.

Employee well-being and satisfaction (eNPS)

The fifth target on Employee well-being and satisfaction (eNPS) is related to our health and well-being policy. Employee NPS (eNPS) score directly reflects the health of the company culture, leadership effectiveness, and the well-being of employees.

A higher eNPS indicates a more engaged and satisfied workforce, aligned with the policy's goal of cultivating a healthy and inclusive work environment.

We've set a target to reach an eNPS (employee Net Promoter Score) above 50 in 2030, excluding contractors. This is an absolute target measured as an eNPS score, typically measured on a scale from -100 to +100. Our baseline year is 2023, with a eNPS score of 2. We report our progress annually and our 2024 outcome is 40.

eNPS will be measured through regular employee surveys, ensuring anonymous feedback to accurately gauge engagement and satisfaction. Data is collected globally, using the same survey tool across all regions. We assume that improvements in leadership, work culture, and well-being will positively influence the eNPS score. The eNPS target is defined by F-Secure's CPO, and when part of our remuneration plans like the non-sales STI plan, also with the CEO.

Performance review

The sixth target related to performance reviews supports the company's Leading Performance policies and process, ensuring that employees actively set and follow up on their development goals. It fosters a culture of continuous professional growth by aligning individual aspirations with the organization's vision and strategy and is set by F-Secure's CPO.

Our target is to achieve a 98% completion rate of performance and career target setting for all employees by the end of 2030. This target applies to all company employees globally, excluding employee-like contractors unless specified otherwise. There is no baseline data available for previous years, as 2024 is the first year to capture the data. Our 2024 outcome is 82.04% and will be reported annually as part of our sustainability statement. 2024 will serve as the baseline year going forward.

Target setting process and engagement with the workforce

Overall company-level targets for the short term (fiscal year) and our vision for the strategy period (typically 3 years) are defined by the Leadership Team. For Own Workforce-related measures, targets are defined by the CPO in collaboration with other Leadership Team members or the CEO if part of the incentive schemes. Employee input into target setting is considered based on, for example, surveys conducted during the year or experts participating in target setting within respective functions such as talent development specialists on diversity targets. Progress is shared with the workforce through monthly town halls and other internal communications, where feedback is gathered to improve actions or policies aimed at achieving the targets.

Employee engagement (eNPS) is measured through regular anonymous employee surveys using a standardized global tool. Corrective actions are identified based on the survey results both on the company level, as well as for functions and individual teams.

Individual performance and development goals are jointly defined by line managers and employees at the start of the year, aligned with company and function plans. Progress is tracked through regular 1:1 meetings and team discussions. A mid-year review assesses organizational progress, and end-of-year reviews reflect on goal achievement, alignment with company values, and future development plans, which are documented in the HR system.

S1-6 Characteristics of the undertaking’s employees

Methodologies and assumptions used to compile and report the data

The data for this disclosure is sourced from our HR system (Workday), which is the central system used by F-Secure to manage employee and consultant information. It serves as the single source of truth for all workforce data, ensuring accuracy and consistency across all reporting metrics.

Related to methodology

• Data Entry and Categorization:

All employees, including permanent and fixed-term employees, are managed through the HR system. This ensures all workforce data, regardless of employment type, is systematically recorded and tracked in a standardized manner.

• Processes and Validation:

Standardized data entry processes within the HR system ensure consistency across employee and consultant records. Regular validation steps, such as cross-checks by HR teams, are implemented to confirm data accuracy.

• Data Reporting:

Metrics for workforce categorization and other disclosures are directly derived from the HR system. These metrics are extracted in a consolidated format through the HR system’s reporting tools, which reduce the risk of errors and maintain reliability.

Total number and rate of own employee turnover in the reporting period in head count is calculated by using this methodology:

"Number of all leavers for each month is summarized and then divided by the ending month headcount to get the percentage. Those percentages are summarized together to get the annual attrition rate".

Definition when reporting the number of personnel

F-Secure reports its personnel as headcount.

A Full-Time Equivalent (FTE), used in the tables S1-6 Employee per contract and S1-6 Employee per region represents the number of full-time hours worked by

our employees. It helps standardize the working hours of part-time and full-time employees to determine the total number of full-time employees at F-Secure.

For example, if we assume 40 hours per week as full-time, an employee working 40 hours per week would have an FTE of 1.0. A part-time employee working 20 hours per week would have an FTE of 0.5, indicating they work half the hours of a full-time employee.

The reporting period is annual, and workforce data is captured through the HR system, which provides real-time data on the headcount and full-time equivalents (FTEs). The data reflects the status at the end of the reporting period.

Cross-reference with financial statements

The measures provided in the sustainability statement own workforce section are aligned with related data provided in other sections of the annual report noting that average annual number of personnel is used in the financial statement ([Cross-reference to financial section 7. Personnel expenses](#)).

S1-6 Employee gender

Gender	Number of employees, 2024
Male	366
Female	162
Non-Binary	0
Not reported	1
Total Employees	529

Table 23. Employee gender.

S1-6 Employee per country

Country	Number of employees, 2024
Denmark	2
Finland	270
France	5
Germany	5
India	70
Italy	1
Japan	5
Malaysia	74
Netherlands	7
Norway	1
Poland	15
Slovakia	19
Spain	2
Sweden	7
United Kingdom	13
United States of America	33
Grand Total	529

Table 24. Employee per country.

S1-6 Employee per contract

2024	Female	Male	Other 1)	Not disclosed	Total
Number of employees (head count/FTE)	162/159	366/364	0	1/1	529/525
Number of permanent employees (head count/FTE)	160/157	364/362	0	1/1	525/521
Number of temporary employees (head count/FTE)	2/2	2/2	0	0	4/4
Number of non-guaranteed hours employees (head count/FTE)	0	0	0	0	0
Number of full-time employees (head count/FTE)	153/153	359/359	0	1/1	513/513
Number of part-time employees (head count/FTE)	9/6	7/5	0	0	16/12

1) Gender as specified by the employee themselves.

Table 25. Employee per contract.

S1-6 Employee per region

2024

	Europe	North America	Asia ¹⁾	Total
Number of employees (head count/FTE)	347/343	33/33	149/149	529/525
Number of permanenet employees (head count/FTE)	343/339	33/33	149/149	525/521
Number of temporary employees (head count/FTE)	4/4	0	0	4/4
Number of non-guaranteed hours employees (head count/FTE)	0	0	0	0
Number of full-time employees (head count/FTE)	331/331	33/33	149/149	513/513
Number of part-time employees (head count/FTE)	16/12	0	0	16/12

1) Gender as specified by the employee themselves.

Table 26. Employee per region.

S1-6 Employee turnover

The basis for calculating employee turnover is the number of employees who have left voluntarily or due to dismissal, retirement, or death in service, divided by the F-Secure headcount as of December 31, 2024.

Employee turnover in the reporting period in headcount	2024
Total number	107
Rate, %	20.23%

Table 27. Employee turnover.

S1-9 Diversity metrics

The data included in this section covers:

- Age group by Job grade: the distribution of employees by age group: under 30 years old; 30-50 years old; and over 50 years old in each job grade.
- Gender by Job grade: Gender distribution in each of F-Secure's job grade.
- Gender by Comp Grade: the gender distribution in number and percentage at the top management level. According to F-Secure's Job Architecture, employees in roles classified as F6 and above are considered part of top management.
- Note that These contain only employee data and exclude data related to contractors.

In the context of our HR system, employees are provided with the option to select their gender as female, male, other, or not declared. This ensures that all individuals within our organization can choose the gender that best represents their identity, or they have the option of not declaring it at all. The term "other" refers to individuals whose gender identity does not fall strictly within the categories of male or female.

S1-9 Gender distribution

The gender distribution at top management level amongst its employees, 2024	Female	Male	Other
Total number	12	39	0
Percentage, %	23.50%	76.50%	0

Table 28. Gender distribution.

S1-9 Age distribution

The distribution of employees by age group, 2024	Under 30 years old	30 - 50	Over 50
Total number	109	353	67
Percentage, %	20.60%	66.73%	12.67%

Table 29. Age distribution

S1-13 Training and skills development metrics

Data is available on e-learning completions and global training session participation since August 2023 in our Learning Management System (LMS). Each employee

undergoes two performance reviews per year: a mid-year review and an end-of-year review, both assessing goal achievement and overall performance.

S1-13 Training

2024	Female	Male	Other	Total
The percentage of employees that participated in regular performance and career development reviews (%)	85.8%	88.2%	No Other Gender as of review date	88% ¹⁾
Number of performance reviews per employee				1.7
The average number of training hours per employee (h)				1.84

1) This excludes a single employee who has not reported gender

Table 30. Training.

We've calculated the percentage of employees that participated in regular performance and career development reviews based on all of our employees as of 31 Dec 2024, and only calculating an employee once regardless, if there have been 1 or 2 performance reviews during the year. Additionally, we've excluded employees terminated during 2024.

When calculating the number of performance reviews per employee, we include all performance reviews completed during the year divided by the number of employees as of 31 December 2024.

S1-14 Health and safety metrics

During the autumn of 2024, we introduced a dedicated form within our HR system to systematically track work-related accidents and any resulting absences. The purpose of this initiative was to enhance our monitoring of workplace incidents, ensuring a proactive approach to employee health and safety. Employees here means permanent and fixed-term employees according to the definition mentioned in section S1-1 definitions of Employees and non-employees. For 2024; we have requested employees to retrospectively record any accidents that may have occurred earlier in the year. Beginning in 2025, we expect all accident reports to be submitted promptly following the occurrence of an incident.

In Finland, where we have a large portion of our employees, all health-related data is managed by our occupational health care provider. This tracking provides valuable insights into the health and safety of a significant portion of our workforce. This data allows us to identify trends and areas needing improvement, guiding our preventive measures and policies. We aim to extend similar tracking mechanisms globally, ensuring comprehensive monitoring and enhancement of workplace health and safety.

S1-14 Health and safety

	2024
The percentage of people in its own workforce who are covered by the undertaking's health and safety management system based on legal requirements and/or recognised standards or guidelines,%	100%
The number of fatalities as a result of work-related injuries and work-related ill health	0
The number and rate of recordable work-related accidents	0

Table 31. Health and safety.

Health and safety data only include employees. In addition, F-Secure has chosen to omit the number of cases of recordable work-related ill health, subject to legal restrictions on the collection of data and the number of days lost to work-related injuries and fatalities from work-related accidents, work-related ill health and fatalities from ill health for the first year.

S1-15 Work-life balance metric

At F-Secure, all employees are entitled to take family-related leave, as outlined by applicable laws of countries, company policies, and collective agreements where relevant. F-Secure supports a work-life balance culture, ensuring that employees can access and utilize family-related leave without barriers. F-Secure actively monitors these metrics to ensure equitable access to family-related leave across all genders. We remain committed to addressing any gaps in usage or access to support our broader objectives of work-life balance and inclusion. These insights guide our policies and initiatives to foster a supportive workplace for all employees.

S1-15 Work-life balance

Data point	2024
The percentage of employees entitled to take family related leaves	100%
	Male: 3.2%
The percentage of entitled employees that took family related leaves disaggregated by gender	Female: 2.6%

Table 32. Work-life balance.

S1-16 Remuneration metrics

The main data source is our HR system from where we extract the annual base salary, and the annual total of allowances and benefits paid on top of the base salary valid at the end of the year. We also extract the total amount of one-time payments (including incentives), and overtime compensation (where available) paid during the year. The annual payout amounts from the LTI programs are also obtained. After extracting the data, we calculate the annual total compensation per employee in euros and sort the amounts from the highest to the lowest.

We use the following formula to calculate the gender pay gap and express the outcome as a percentage: (Average annual total compensation of male employees – average annual total compensation of female employees) divided by the average annual total compensation of male employees.

For the annual total remuneration ratio, we first calculate the median annual total compensation amount excluding the highest amount. Then we calculate the ratio using the following formula:

(The highest annual total compensation amount) divided by (the median annual total compensation amount).

S1-16 Remuneration

F-Secure measures the pay gap as part of our annual global salary increase process.

Remuneration	2024
The gender pay gap, %	12.74%
The annual total remuneration ratio of the highest paid individual to the median annual total remuneration for all employees	5.11

Table 33. Remuneration.

S1-17 Incidents, complaints and severe human rights impacts

F-Secure is committed to fostering an inclusive and respectful workplace where all forms of discrimination are prohibited. In alignment with our zero-tolerance policy, we closely monitor and address any incidents of discrimination or harassment across all operations. During the reporting period, there have been no reported work-related incidents of discrimination based on gender, racial or ethnic origin, nationality, religion or belief, disability, age, sexual orientation, or other forms of discrimination involving internal or external stakeholders.

F-Secure provides a confidential Whistleblowing Channel, available 24/7, to allow employees and stakeholders to report any concerns related to discrimination, harassment, or unfair treatment. All reports are reviewed thoroughly and handled following F-Secure's policies, ensuring compliance with privacy regulations and local legislation.

Through this process, F-Secure remains dedicated to maintaining a fair, safe, and respectful environment for all stakeholders.

S1-17 Incidents

	2024
Harassment & discrimination	
The total number of incidents of discrimination, including harassment, reported in the reporting period	0
The number of complaints filed through channels for people in the undertaking's own workforce to raise concerns (including grievance mechanisms)	0
The total amount of material fines, penalties, and compensation for damages as a result of the incidents and complaints disclosed above	0
Severe human rights incidents	
The number of severe human rights incidents connected to the undertaking's workforce in the reporting period	0
The total amount of fines, penalties and compensation for damages for the incidents described above	0

Table 34. Incidents.

S4 – Consumers and end-users

SBM-3 Material impacts, risks and opportunities

F-Secure confirms that all consumers who are impacted by F-Secure are in the ESRS 2 disclosure scope. For clarity, in this statement “consumers” and “end-users” should be understood as synonyms, unless stated otherwise.

Consumers and end-users list of IROs

	Material impact, risk or opportunity	Description
Personal safety of consumers and/or end-users		
Security of a person - Protecting our customers		
Opportunity (OO)	Use of AI in security applications	AI-powered (network) monitoring tools can observe user behavior, detect anomalies, and react accordingly.
Opportunity (OO)	Evolving threat landscape	Scams have become more commonplace. Opportunities for F-Secure to offer engaging and relevant protection services.
Risk (OO)	Consumer willingness to pay	Intensifying competition and negative macro-economic situation may have negative impact on consumer willingness to pay.
Risk (VC)	Channel strategy	Significant agreement changes or loss of a major Service Provider account, or Direct Business decline
Risk (VC)	Tier 1 partnerships	F-Secure may be unable to create, deliver and maintain Tier 1 solutions with sufficient profitability levels (over time) inc. meeting support commitments
Actual positive impact (OO)	Protecting digital moments	According to our product questionnaire our consumers are worried about their online protection. F-Secure provides solution to these threats through its offering.
Risk (VC)	Security of vendors and partners	The reliance on external vendors, especially vendors who are one step removed in the supply chain, adds layers of vulnerability.
Risk (OO)	Cyber security	Cyber security attacks negatively impact reputation and business
Health and safety		
No IROs identified.		
Protection of children		
No IROs identified.		

	Material impact, risk or opportunity	Description
Social inclusion of consumers and/or end-users		
Non-discrimination		
No IROs identified.		
Access to products and services		
No IROs identified.		
Responsible marketing practices		
No IROs identified.		
Information-related impacts for consumers and/or end-users		
Privacy		
No IROs identified.		
Freedom of expression		
No IROs identified.		
Access to (quality) information (Awareness and education)		
Actual positive impact (VC)	Create awareness about cybercrimes	Increase the consumers awareness about cybersecurity and cybercrime through marketing campaigns and events.

Table 35. Consumers IRO-1 list of IROs.

Interaction with strategy and business model

Related to the personal safety of consumers and end-users, F-Secure has identified an *actual positive impact (OO) in protecting consumer's digital moments*. We're already having this positive impact today based on our own operations directly and through our channel partners, and we expect it to remain our material impact also in the long term. Protecting consumers' digital moments continues to guide and form the company strategy, decision making and execution, notably including

1. Product and technology investments: Allocating product and technology investments to provide relevant, engaging and effective protection capabilities to consumers against modern threats. This also includes investments in innovation, threat research and research in consumer needs.
2. Growth Opportunities: Aligned with the above, the evolving threat landscape, including the rise of scams and cybercriminals using AI, presents growth opportunities. The use of AI is seen as an opportunity to innovate new protection capabilities and improve customer experience.
3. Channel sales model: Ensuring that in our go-to-market model that is primarily channel sales-driven we can meet the needs of each partner segment operationally and through our product and services portfolio. This "fit to channel" and being a partner-first company further ensures we can reach a sizable number of consumers behind our partners whether providing application-, network- or SDK/API-based solutions to protect consumers' digital moments with our partners.
4. Consumer Awareness: F-Secure increases awareness about cyber threats through free tools, blogs, newsletters, and education by channel partners. This aligns with the company's purpose to make every digital moment more secure for everyone.

When protecting consumers' digital moments, the *constantly evolving threat landscape* has been identified as a growth opportunity for F-Secure and our channel partners both in the short and long term. Additionally, we see the *use of data and AI in security applications as an opportunity* for innovating new protection capabilities and improving the customer experience.

To take advantage of these opportunities, our portfolio, customer experience and protection roadmaps now focus on scam protection. This includes providing new protection capabilities such as messaging scam protection, implementing AI capabilities to provide effective protection and ensuring an engaging user experience. We expect our scam protection focus to have a positive effect on

our financial performance already in the short term while supporting our long-term growth strategy as our offering becomes more attractive to consumers and our partners. Furthermore, providing a relevant and engaging scam protection offering helps address the risks related to *consumer willingness to pay* for security decreasing or our *channel strategy* exposing us to a potential loss of an existing partner.

Additionally, protecting consumers' digital moments means supporting all consumers, whether they are using F-Secure products or not. Therefore, we're both directly and through our channel partners having an actual positive impact today by *creating awareness about cyber crimes* and cyber security in general.

We increase awareness of cyber crimes directly and through our channel partners including

- Offering free tools like Online Shopping Checker and Text Message Checker to help consumers stay safe online
- Blogs and newsletters, such as F-Alert, provide tips and guidelines on online safety and trending threats
- Our 200 channel partners educate their end-customers on cyber threats and protection methods

All of the above are tightly connected with our very purpose and core strategy. We exist to make every digital moment more secure, for everyone while consumers shop, exercise, work, socialize, relax, and unwind, all while being connected through a holistic consumer cyber security portfolio.

Relationship between material risks and opportunities arising from impacts and dependencies on consumers and/or end-users and its strategy and business model

The *evolving threat landscape (VC)* and scams becoming more commonplace is a major opportunity for F-Secure and our Service Provider partners. Indeed, F-Secure exists to protect consumers and increase their confidence and trust in digital services and thereby in society, representing our tangible contribution to social and economic progress.

As mentioned, consumers are increasingly relying on Service Providers for online safety, which has influenced F-Secure's go-to-market strategy. We are the only consumer cyber security company with a "partner-first" business model. Partnering with major service providers we make holistic cyber security products and

embedded protection capabilities available to hundreds of millions of consumers across the globe.

We recognize the risks in our *channel strategy* (OO), such as changes in agreement scope or losing significant Service Provider partners. However, such changes are uncommon and typically occur over time. Additionally, working with Tier 1 Service Providers may pose profitability challenges or an inability to meet their requirements. These risks could impact revenue, increase costs, or hinder our operations. While the risk exists, our view is that investing in capabilities for our Tier 1 business enhances resilience across all partner segments.

The threat landscape is constantly evolving meaning consumers are subject to new and extremely credible scams. This creates an opportunity to *use AI in security applications* (OO) to combat these threats while providing a relevant, easy-to-use, and engaging protection experience to consumers. Being a trusted companion leveraging AI capabilities and visibly part of consumers' everyday digital moments, we can protect consumers against online threats and deliver the feeling of safety that consumers are looking for.

Consumers trust F-Secure to protect their digital moments, and we take this responsibility seriously. We securely handle personally identifiable information (PII) and never sell it to third parties. Our workforce is regularly trained on PII handling, which is a cornerstone of our Code of Conduct. By ensuring consumer trust while offering engaging cyber security solutions, we mitigate the *risk where consumer willingness to pay for security would lower* (VC), for example, switching to free security products or relying solely on built-in protection capabilities.

We also acknowledge that F-Secure carries the *risk of a cyber security attack* (OO) that may negatively impact our reputation and business. The same cyber security risk applies to F-Secure, and as is customary in the cyber security industry, due to *security of our suppliers and partners* (VC). Our mitigation activities against cyber security breaches are described further down in this section.

Types of consumers negatively impacted by F-Secure

F-Secure provides software-based products and services that are designed for all consumer types and across age groups. As our portfolio consists of cyber security software-based products we don't develop or carry any products that are inherently harmful to people and/or increase risks for chronic disease. Hence, we have not identified any material negative impact related to consumers and end-users, or any consumer subsegments.

Similarly, no products or services exist that may potentially negatively impact consumer rights to privacy, to have their personal data protected, to freedom of expression, and to non-discrimination. On the contrary, F-Secure's cyber security offering is built to protect consumers and their rights online. This includes, for example, privacy or identity protection capabilities, included in our portfolio.

Related to providing accurate and accessible product or service-related information, we've built our products to guide onboarding and usage to minimize the need for manuals. Regardless, we do offer support to consumers on how to use our products and services with the help of manuals, community articles, and a support channel for help.

F-Secure sees no negative impacts related to health or privacy from our portfolio, or arising from our or our partners' marketing and sales strategies toward potentially vulnerable individuals. Our software-based products, including protecting consumer privacy online, are promoted and sold either directly by F-Secure or through reputable Service Providers and are not targeted at children or financially vulnerable individuals.

Types of consumers positively impacted by F-Secure

Our products and services protect consumers against online threats with a positive effect and help people stay safe online.

Protecting digital moments

F-Secure's very purpose is to protect consumers' digital moments. When building digital products at F-Secure, we have created a design system to make our products perceivable, operable, understandable, and robust for the widest possible audience. Our product design focuses on creating solutions that empower users and enhance their safety and confidence online. We prioritize accessibility by designing simple, intuitive products that minimize cognitive load and follow guidelines for visual accessibility, including sufficient contrasts, appropriate text sizes, and awareness of seizure triggers.

Our intent is that in addition to delivering the best security experience, compliance with best accessibility practices in our product creation allows the creation of an inclusive product experience that welcomes both individuals with disabilities and the elderly, and simultaneously serves the general population.

Create awareness about cyber crimes

We also focus on increasing global cyber security awareness to combat cybercrime, educating consumers and end-users on staying safe online. Our global campaigns in various communication channels target diverse regions and involve collaboration with educational institutions, government bodies, NGOs, and customers, emphasizing a shared responsibility for cyber security. This aligns with our ESG goals of mitigating cyber threats and promoting a secure digital environment. We carry out these activities providing educational content and free tools for online safety.

For further details on risks and opportunities, see the section on ESRS 2 SBM-3 – Material impacts, risks and opportunities and their interaction with strategy and business model, and section in General Information.

Impact, risk and opportunity management

S4-1 Policies

For clarity, the following IROs are related to F-Secure's strategy and business operations, while IROs connected to our policies are described under each policy further down in this section: protecting digital moments (impact), creating awareness on security cybercrimes (impact), evolving threat landscape (opportunity), consumer willingness to pay (risk), channel strategy (risk), and Tier 1 partnerships (risk). The alignment of these IROs with our targets and actions are described under S4-5 Targets related to managing IROs

Note also that while our Code of Conduct is applicable also for Consumers and End-Users, serving our customers and partners in a business ethical manner is described in the Business Conduct – section of this statement and under the "Code of Conduct training target".

Personal Data Policy

The F-Secure Personal Data Policy outlines the controls and principles for protecting customer privacy, covering privacy organization and roles, key privacy principles and processes, privacy training, and monitoring of privacy principles. The policy applies to all consumers.

The policy applies to all F-Secure operations and employees, including subcontractors and suppliers. The policy is approved by F-Secure's CEO and leadership team. The Personal Data Policy is based on the EU General Data

Protection Regulation and other relevant privacy regulations and reflects F-Secure's privacy principles published also online.

This policy is related to the following IROs, which may also be connected to other F-Secure policies due to their nature:

- Cyber security attacks negatively impacting our reputation and business (risk)
- Security of suppliers and partners, especially in terms of vulnerabilities (risk)

The processes for monitoring and measuring our progress are described under the Metrics and Targets section where the completion rate of cyber security training and cyber security incidents are primary metrics.

Cyber Security Policy

The F-Secure Cyber Security Policy outlines objectives for strategic cyber security activities, governance practices, and focus areas, including cyber security objectives, governance, information security management, privacy management, software security management, and relevant policies, procedures, and guidelines. The policy applies to all consumers.

The objective of the policy is to define boundaries and guide the implementation of cyber security in F-Secure. This includes the development of cyber security, identifying cyber security-related opportunities, and mitigating cyber security risks. These activities revolve around information security, software security, and privacy. The policy is based on the ISO 27001 standard.

Protection of customer and employee data and maintaining the availability of company services are the primary purpose of the cyber security activities in F-Secure. These activities have a direct impact on consumers' security. In addition, through the activities defined in the policy, F-Secure can collaborate with different stakeholders and promote security awareness across society.

The policy applies to all F-Secure operations and employees, including subcontractors and suppliers. The policy is approved by F-Secure's Chief Executive Officer. F-Secure's CEO is accountable for the enforcement and monitoring of the fulfillment of objectives defined in the Cyber Security Policy, while the Chief Information Security Officer is responsible for driving the implementation of the policy.

This policy is related to the following IROs, which may also be connected to other F-Secure policies due to their nature:

- Cyber security attacks negatively impacting our reputation and business (risk)
- Security of suppliers and partners, especially in terms of vulnerabilities (risk)

The processes for monitoring and measuring our progress are described under the Metrics and Targets section where cyber security incidents, the ratio of externally reported product vulnerabilities to internally identified vulnerabilities and the completion rate of cyber security training are primary metrics.

AI Policy

Artificial Intelligence (AI) applications have massive potential to transform how we work: From making day-to-day work more productive to creating completely new ways of serving and protecting consumers and supporting our partners. The policy applies to all consumers.

The AI Policy at F-Secure encourages innovation with AI applications while ensuring adherence to high standards in privacy, cyber security, intellectual property rights, and business integrity. It outlines the dos and don'ts of working with AI to maintain these standards. The F-Secure AI Policy is based on the following values and principles defined in the F-Secure Code of Conduct:

- Building Trust in Society
- Intellectual Property Rights and Confidentiality
- Protecting Human Rights

The AI policy is new and was approved in the beginning of 2024 by the CEO, before that there was no formal policy in place for the topic. This Policy applies to all employees and employee-like contractors and while related to the use of AI in security applications (opportunity) it should be seen as tightly coupled with the Cyber Security Policy objectives and targets.

Human rights commitments relevant to consumers

F-Secure has firmly embedded its commitment to international human rights in its Code of Conduct, considering also globally recognized principles. Namely, the F-Secure Code of Conduct lists the following as the main international principles F-Secure considers:

- OECD Guidelines for Multinational Enterprises
- United Nations Global Compact
- United Nations Guiding Principles on Business and Human rights
- United Nations Convention Against Corruption
- International Bill of Human Rights
- The Declaration of the International Labour Organisation on Fundamental Principles and Rights at Work

F-Secure's internal policies, procedures and guidelines are aligned with both the Code of Conduct and these international principles, which further embed these principles into the internal practices of F-Secure on a more concrete level.

F-Secure's commitment to international principles is not limited to internal operations but extends to its end-users. The company ensures that its products and services are designed and delivered in a manner that respects human rights and ethical standards. This includes data privacy protections, secure processing of personal data, and transparent communication about user rights and responsibilities.

We encourage engagement with end-users, and end-users can both provide feedback and report concerns about F-Secure products through Customer Care or the whistleblowing channel. The whistleblowing channel allows anonymous reporting of Code of Conduct violations including human rights violations by employees, partners, and stakeholders without fear of retaliation. All reports are taken seriously, investigated, and prompt corrective actions are implemented. The latter may also include remedies for human rights impacts, where deemed appropriate by the result of the investigation. Furthermore, through F-Secure Supplier Code of Conduct, our screening procedures and Know Your Counterpart procedures we expect our suppliers to address the same principles.

Alignment with internationally recognized instruments (SFRD and Pillar)

Protecting consumer data in our daily operations is critical. F-Secure adheres to ISO 27001:2022 Standard for Information Security Management across all its operations. The standard defines controls for managing information security and covers topics such as people security, secure software development, security incident response, and business continuity. The standard is used as a baseline for ensuring that F-Secure's customer data and products are protected against modern security threats. The sub-standards and reference controls used as part of ISO 27001:2022 standard in F-Secure include for example:

- ISO 27001 Annex A controls
- NIST CSF & 800-63B
- OWASP Top10, MASV & MASG
- ISO 3001:2018
- ISO 22301:2019

To our knowledge, there have been no reported cases of non-respect of the UN Guiding Principles on Business and Human Rights, ILO Declaration on Fundamental Principles and Rights at Work or OECD Guidelines for Multinational Enterprises that involve consumers and/or end-users.

S4-2 Processes for engaging about impacts

F-Secure deploys several methods of collecting and analyzing the perspectives of consumers. The majority of the engagements are direct and many of them involve some form of dialog between F-Secure and the consumer. Examples of engagements are customer care contacts, app store feedback, and social media feedback. In addition, F-Secure requests formal feedback through a product survey that is sent out continuously. All data is analyzed, responded to (when the channel allows) and reported to applicable F-Secure stakeholders for further processing.

We also receive feedback from our channel partners regarding their end-users that is processed similarly. The scope and frequency of these engagements vary between partners: some may be joint customer need surveys, we may obtain generic feedback from partners based on their own market and consumer surveys or feedback from their customer care teams.

Stage and frequency of engagement

F-Secure closely follows the performance of the customer lifecycle in its Direct Business. The majority of the engagement with the consumer happens after onboarding - once the consumer customer has installed and activated our protection services (app). Daily engagement happens through the protection app, which works in the background protecting the use of the device and the consumer's digital moments.

Obtaining consumer feedback happens continuously making it possible for F-Secure to respond to possible challenges promptly covering the communication channels mentioned above. All consumer feedback is consolidated, analyzed, and processed on a monthly basis.

F-Secure's Chief Product Business Officer who is part of the Leadership Team and reports directly to the CEO has the operational responsibility for ensuring this engagement happens and that the results are taken into account as part of F-Secure's strategy, business model and daily activities.

Assessing the effectiveness of our engagement

F-Secure follows multiple consumer-generated metrics such as number of support cases, NPS (Net Promoter Score), CES (Customer Effort Score), and app store ratings to follow the effectiveness of engagement. As the metrics are based on the direct business consumer scoring, ratings, and feedback, they enable F-Secure to stay in close connection with the sentiments of the consumer customers even if the majority of our business originates via Service Provider partners. However, we measure and track app store ratings with our partners such as in the Apple App Store or Google Play. Any significant change in the metrics or received feedback is further investigated and corrective actions are taken regardless of channel.

Gaining insights on consumers, particularly vulnerable consumers

F-Secure puts a significant emphasis on the ease of use of the protection app. We strive for demographic representation in our testing processes to ensure a multitude of cultural perspectives in the feedback that we apply to our product creation, and to not exclude any consumer groups.

Additionally, we include compliance with the EU accessibility act to ensure our products are widely usable. No consumer group is excluded in the design and the target is to make protection easy to activate and use even without advanced technical skills. Furthermore, by complying with the European Accessibility Act and accessibility recommendations from W3C, F-Secure strives to ensure ease of use for users with various disabilities.

F-Secure uses also its beta community to verify design decisions before the product is made available to a larger audience.

S4-3 Processes to remediate negative impacts and channels to raise concerns

Channels to raise concerns

End-users can reach F-Secure both through self-help (community forum) and assisted (chat and phone) channels. In addition, F-Secure's Customer care is active on F-Secure's Social Media and app store channels to assist customers. All customer contacts are evaluated with satisfaction measures with a post-ticket survey including the option for open feedback. F-Secure is providing support services in-house with dedicated resources.

F-Secure has also defined support models with its channel partners where end-user support services are provided either by F-Secure or by the Partner. In cases where channel partners are the first point of contact, we provide help desk training, and we always have open support channels for the partner in case any assistance is needed. In all cases, F-Secure provides technical support for the partners related to its offering as per agreed Service Level Agreements.

Effectiveness and trustworthiness of our support channels

F-Secure logs all customer contacts (customer inquiries and support requests) within a ticketing system to ensure we can identify trends, track performance metrics, and make data-driven decisions about how to improve customer experience and customer service. This also helps us to track ticket volume,

resolution time and customer satisfaction (post-ticket survey) per available contact channel.

For common issues raised and addressed, we have a monthly internal review and verification process, customer experience council, with action points to remediate issues and follow up on progress. When topical, we also benchmark our offered service and customer care metrics, especially post-incident customer satisfaction, with other companies in the cyber security industry, and by companies and associations that provide insight and research data within the technology and services sector.

Related to the trustworthiness of our support channels, we engage with the end-users during the customer lifecycle through the protection app and lifecycle messages and inform the end-user about available contact channels. Additionally, all contact channels are available publicly on the web for anyone to find and use. We continuously follow the utilization of each channel to ensure the channels are effective and in use. As mentioned earlier, consumers may also provide feedback under our whistleblowing policy, and through our publicly available whistleblowing channel without fear of retaliation.

To ensure our customers trust these channels, all customer care contacts and remediation of customer issues are evaluated with a satisfaction survey after solving the support case, including the option for open feedback. F-Secure has a complaint process in place triggered by a low post-ticket survey score and the customer's request to be contacted. Within this process, F-Secure engages the customer to better understand customer perceptions and handles the complaint with actions to solve customer issues to satisfaction, and internal actions to improve service and further build trust into the processes. A post-complaint survey is sent to ensure the effectiveness of the complaint handling.

S4-4 Actions and resources

Related to our *actual positive impact (OO) of protecting digital moments* and as described further under S4-3, our cyber security products and services like F-Secure Total help consumers stay safe online and build trust in society. We constantly improve our protection capabilities in our cloud to increase security efficacy and deliver real-time protection for consumers while regularly launching new product versions with expanded protection capabilities to ensure consumers are protected against scams. This is not a one-off activity, rather it is a continuous plan of activity for the strategy period (2025–2027) and executed in our focus regions and channels as described under ESRS 2 "General information" and "Strategy, business model

and value chain." The most material expected outcome of these actions and plans include increasing the number of consumers we protect globally, consumer and partner satisfaction, while creating value for our partners and shareholders.

Related to *actual positive impact (OO) on creating awareness about cyber crimes*, we are also active in driving overall consumer awareness around cyber threats as described earlier and, for example, through the Cyber Citizen initiative together with Aalto University and other partners that also gamifies training to make it more appealing to consumers. F-Secure has supported the Cyber Citizen initiative to, e.g., define the consumer target audience by providing consumer insights expertise. We track the effectiveness of these activities through the number of consumers we reach annually. Similar to the above, this is a continuous plan of activity for the strategy period (2025–2027) and will be executed in our focus regions and channels as described under SBM-3 Strategy, business model and value chain.

See further the section 4-5 on Targets and Metrics and how we track the effectiveness of these actions. No negative impacts were identified in F-Secure's materiality assessment.

Mitigating material risks

Our most material impact is to protect consumers' digital moments by providing holistic, engaging and easy-to-use cyber security products and services directly and through our partners. This carries inherent risks such as

- 1. *Consumer willingness to pay* for security in the future may decline
- 2. Our *channel strategy* may lead to agreement changes or a loss of a major Service Provider partner
- 3. Inability to meet *Tier 1 partner requirements*
- 4. *Security of suppliers and partners* as we rely also on external suppliers adding layers of vulnerability
- 5. *Cyber security* attacks may negatively impact our business

We mitigate risks related to consumer willingness to pay by continuously adding new relevant scam protection capabilities that increase value to consumers and tracking impact through sales and product NPS. Together with our Service Provider partners that offer security either based on F-Secure apps or embedded in their own app, we can provide more value compared to other alternatives and can track the effectiveness of these actions based on subscriber base growth and ARPU increase. Significant attention is paid in all channels to track service activation and usage

rates, thereby increasing the perceived value seen by consumers. These actions remain valid for the strategy period (2025–2027) in our operations and are available to all partners and consumers in our focus regions described under ESRS 2.

F-Secure's Service Provider business can be impacted if a partner reduces or stops purchases with us. To mitigate this channel risk, we help partners drive growth as measured by subscriber base growth, ARPU development, and service activation rates. We also deliver based on a compelling vision and roadmap to meet partners' business needs in the short and long term. We can measure the effectiveness of these activities, for example, tracking product upgrades across our partners, revenue and ARPU increase, partner commitment to sales and marketing activities, and their overall satisfaction with us (partner NPS). Naturally, we continue to develop a healthy sales pipeline of new opportunities, with effectiveness measured in funnel size. These actions remain valid for the strategy period (2025–2027) and are available to all partners and consumers in our focus regions described under ESRS 2.

We also provide consumer cyber security solutions to some of the largest Service Providers in the world ("Tier 1s") and aim to win new Tier 1 contracts. To minimize any risks, F-Secure has defined a partner segment-based operating model to meet Tier 1 specific requirements in a scalable and profitable manner. Additionally, we constantly measure and improve, for example, our project delivery accuracy and quality, and meeting partner's service level needs. Similar to all Service Providers, partner satisfaction (NPS) is also a critical metric and target for Tier 1 partners. These actions remain valid for the strategy period (2025-2027) and are available to all partners and consumers in our focus regions described under ESRS 2.

Regarding the security of our suppliers and tied with our Personal Data and Cyber Security Policies, F-Secure ensures supplier and partner security by implementing security review gateways in the procurement process, enforcing security requirements contractually, and conducting regular security audits of critical vendors. This applies to all our suppliers and partners globally and these actions remain valid for the strategy period.

Cyber security attacks could harm F-Secure's brand and business. To mitigate this, we implement industry standards, including the ISO 27001 standard, proactive security monitoring, vulnerability management, and regular crisis rehearsals. We measure effectiveness through metrics like the number and criticality of security incidents and vulnerabilities in our software and third-party solutions. These actions remain valid for the strategy period (2025–2027) and apply to both F-Secure's own operations and also working with suppliers and partners globally.

Finally, F-Secure continuously monitors and improves its internal security and privacy related policies to ensure that customer data remains protected. F-Secure conducts regular internal audits to confirm compliance with our internal policies and procedures and takes action if possibilities for improvement are identified.

Actions to pursue material opportunities

Evolving threat landscape (VC) is a major opportunity for F-Secure, especially as scams are getting more credible every day, and consumers remain worried about their safety. F-Secure is taking action on several fronts to leverage this opportunity, where the outcomes are directly connected with consumer satisfaction and F-Secure growth:

- Re-direct resourcing and investments into scam-driven research, innovation and product creation capabilities, especially around scam protection. Naturally, some capabilities may be provided by our suppliers and partners as is customary in the industry.
- Ensure our channel partners can take advantage of the opportunity by upgrading them to the latest versions of F-Secure's portfolio with scam protection capabilities and supporting them in launching, promoting and selling to consumers.

Equally, we see the *use of AI in security applications (OO) as an opportunity* that contributes to F-Secure growth with a differentiated and compelling offering to consumers and our partners. F-Secure has for more than two decades used machine learning in our protection offering. The evolution of AI technologies like generative AI is seen to have a major role in F-Secure's product and protection strategy now and in the future. This also allows for combatting scammers who are also using AI technologies to deceive consumers. AI and overall use of data is planned to improve:

- More engaging, relevant and contextual protection experience (user experience)
- Improved security efficacy where AI technologies can further advance F-Secure's threat research capabilities while providing more effective protection capabilities

The above activities remain valid for the strategy period (2025-2027) in our own operations and results will be available to all partners and consumers in our focus regions described under ESRS 2 "General information".

Human rights issues connected to consumers

F-Secure has zero (0) human rights issues or incidents connected to consumers during 2024.

Resources allocated to the management of the material impacts

A sizable share of our material impacts is related to protecting consumers' digital moments by providing relevant, effective, engaging and easy-to-use cyber security solutions against modern cyber threats directly and through partners.

F-Secure's product management function is responsible for the creation of our product vision, offering and related product roadmaps. This ensures we meet our partners and our consumer customers' needs both in the short and long term. Product management also steers our Product Board, which prioritizes product initiatives and roadmaps through which technology organization resource allocation for the implementation projects (product releases) is decided. The technology organization is additionally responsible for threat intelligence and research activities, and ensuring we provide effective protection against modern threats.

We further see we can make an impact by increasing consumer awareness about cyber security and cybercrime through marketing campaigns, events, free tools, and content. In this area, our marketing teams drive our content creation strategy aligned with our own direct business and partner channel needs and opportunities, supported by our technology organization threat intelligence teams such as providing expert views on the latest scams. Implementation of any free tools is governed as part of the Product Board process described above.

Metrics and targets

S4-5 Targets

F-Secure describes its sustainability-related baseline measures and long-term targets in the table below. 2023 is established as a baseline year in all targets except in ratio of reported vulnerabilities and completion rate of security awareness where the baseline year is 2024. The progress will be reported annually moving forward.

S4-5 Targets Consumers

Target	Baseline 2023	2024	2030 target
F-Secure consumer product NPS (Total)	49	49	55
Partner Business NPS	56	63	Above 55
Completion rate of internal cyber security training	Baseline is 2024	97%	98% (all employees)
Number of major cyber security incidents	2 (no customer data was compromised)	1 (no customer data was compromised)	0 incidents involving leaked customer personal data
Ratio of externally reported vulnerabilities compared to internally reported vulnerabilities.	Baseline is 2024	10.1 %	< 10%

Table 36. Targets Consumers.

Methodologies for collecting and tracking against the target vary: All NPS results are measured through a dedicated marketing survey solution, while metrics related to cyber security training are tracked through F-Secure's Learning Management System. Major cyber security incidents and bug bounty-related issues are tracked with a dedicated ticketing system. All these systems are used globally at F-Secure and there is no need for data collection across regions.

The 2023 baseline year figures and 2024 results have not been assessed by any 3rd party- , nor have external stakeholders directly participated in defining the above metrics and targets. However, the metrics have been selected based on alignment with material F-Secure ESG topics, Double Materiality Assessment, industry benchmarking and our own insights, and stakeholder feedback.

The targets have been developed in collaboration with relevant functions and reviewed and approved by the Board of Directors as described above, while no external stakeholders are directly involved in target setting. We track the effectiveness of our actions and policies toward the impacts, risks and opportunities by monitoring the targets we set below.

S4-5 Progress towards targets

F-Secure consumer product NPS evolution (Total)

The target on Consumer Product NPS evolution is related to IROs around measuring our effectiveness in delivering easy-to-use, engaging and effective protection (protecting digital moments), leveraging the opportunities in the evolving threat landscape (scams), and mitigating risks around consumer willingness to pay.

Net Promoter Score (NPS) is the key metric used to measure customer loyalty and satisfaction by asking customers how likely they are to recommend a company's product or service to others on a scale from 0 to 10. The score is calculated by subtracting the percentage of detractors (those who score 0–6) from the percentage of promoters (those who score 9–10), resulting in a score that ranges from -100 to +100. An NPS score of 20 is considered favorable and above 50 is excellent.

At F-Secure, NPS is used for tracking F-Secure's progress in fulfilling our vision to become the number 1 security experience company and mission to continuously deliver brilliantly simple, frictionless security experiences. As NPS reflects product quality, customer journey, sense of security, and trust-related sentiments of consumer customers it is also a valuable measure for tracking the effectiveness of our product improvement activities, as well as how we can deliver on the Code of Conduct principle of Building Trust in Society.

An NPS target has been set for our main consumer product F-Secure Total, which is also sold by our channel partners but here measured in our own Direct Business channel. The invitation to provide feedback is systematical as part of F-Secure Total product lifecycle messaging.

The F-Secure Total NPS target for 2027 is 50 and 55 for 2030. The 2024 outcome for product NPS is 49. We review the progress monthly within F-Secure and should we identify negative trends or negative feedback, our product management teams build remediation plans accordingly, for example, improvements in usability or customer journey. We report the NPS outcome as part of the sustainability report on an annual basis.

It is worth noting that NPS is highly volatile to negative changes. Any larger changes to the product, overall offering, platform coverage, and technologies are visible in the consumer feedback and the NPS ratings, and F-Secure carefully measures such impacts.

The stakeholders who participate in target setting are the F-Secure executives relevant for product NPS, namely the Chief Product Business Officer and respective product manager(s), the CEO and the Chief People Officer if NPS is part of management or employee remuneration targets. The target is set annually and the final measurement for the year is conducted at the end of the year.

Partner Business NPS evolution 2024

The Partner Business NPS evolution target is related to IROs around measuring our effectiveness in supporting our channel partners growing their cyber security business and mitigating against risks around losing a material Service Provider partner or not being able to support our Tier 1 partners

Similar to the product NPS calculation logic, we apply NPS to measure our partner business satisfaction, which is critical for F-Secure as a vast majority of our revenue originates from partners. We invite Service Providers across industries and geographies to respond to the satisfaction survey and report the outcome annually.

F-Secure's global NPS survey results in March 2024 was 63. Our NPS score is on a very good level and we expect it to remain above 55 in the medium and long term.

F-Secure's Chief Revenue Officer is accountable for the target setting in alignment with the sales strategy. The target is set annually and measured once a year. Our regional sales leads and account managers review the survey results to identify

issues and corrective actions in how we engage with partners, where relevant. These actions may also impact other F-Secure functions, for example, survey findings may trigger initiatives for improvements and optimization around our product portfolio or operations like delivery, partner care or partner marketing.

Completion rate of internal cyber security training

The completion rate target of F-Secure's cyber security training measures F-Secure employees' awareness of internal security policies. This target is based on the objectives defined in F-Secure's Cyber Security Policy, as well as Personal Data Policy, and measures the knowledge of employees against the company's general cyber security objectives, and the related supportive security policies and guidelines.

The target is calculated based on the current employee count excluding long-term absences. The target is absolute as it is based on the exact number of current active employees and the number of people who have completed the training. The target is presented as completion percentage (%). There are no geographical boundaries to measurement as all F-Secure employees are part of the target.

We've set a 2030 target of reaching a training completion rate of over 98%. For 2024, which is also the base year for this target, our training outcome is 97%. We review progress regularly and report the outcome on an annual basis.

The stakeholders who participate in target setting are the F-Secure executives relevant to cyber security, including the company CEO, CFO, CTO, CDO, General Counsel, and CISO. The target is set annually and the final measurement for the year is conducted at the end of the year.

The data of the training is extracted from F-Secure's learning management system, and information related to long-term absences comes from our HR systems. The main limitation of the target measurement is the dependency on the Team Leaders maintaining up-to-date information about long-term absences in the system at the time of measurement.

Number of major cyber security incidents

The number of major cyber security incidents target is based on the objectives related to information security and privacy defined in F-Secure's Cyber Security Policy. It measures company security processes and their capability to prevent major incidents from occurring, and the impact of cyber security incidents on F-Secure's customers.

The occurrence of major cyber security incidents is tracked as part of F-Secure's security incident management and crisis management processes. A major incident is defined as an incident impacting critical systems, security of significant amount of our employees or data classified as restricted or confidential as well as all incidents where customer data is externally exposed. All incidents are tracked in F-Secure's incident management system from where the data is extracted and regularly monitored. The amount of incidents is calculated by extracting the number of major security incidents and reviewing if the incident impacted any customer data or employee safety. The data is uploaded to the ticketing system either by F-Secure employees or by F-Secure's security team depending on the reporting channel. In 2023, F-Secure had two major incidents but neither of them impacted customer data. For 2024, our outcome was 1, while the target is to have no major incidents impacting customer data in 2030.

The target measurement is not completely absolute since it is dependent on the human assessment of the incident. F-Secure follows an incident classification that defines boundaries when a cyber security incident should be classified as major. However, there is always room for interpretation and classification of the incident is always slightly dependent on the initial assessor. This shortcoming is mitigated by having multiple security team members review all incidents.

The stakeholders who participate in target setting are the F-Secure executives relevant for cyber security, including the company CEO, CFO, CTO, CDO, General Counsel, and CISO. The target is continuously measured annually and the final measurement is conducted at the end of the year.

Ratio of externally reported product vulnerabilities to internally identified vulnerabilities

The bug bounty-related target is based on the objectives related to software security defined in F-Secure's Cyber Security Policy. It measures F-Secure's engagement with the cyber security researchers' community, and the efficiency of the company's secure software development processes. F-Secure has several security controls and procedures in place to develop secure products, identify bugs and vulnerabilities,

and remediate them in a timely manner. By developing secure products, F-Secure can better protect the data of our customers and partners.

The number of bug bounty reports, their criticality, and the bounty amount paid to researchers are tracked as part of F-Secure's bug bounty program. All reported cases are tracked in F-Secure's ticketing system from where the reports are assessed by the relevant development team and for potential paid bounty. We have similarly a ticketing system for vulnerabilities or bugs identified internally.

We defined a target for the ratio of externally reported product vulnerabilities where we have paid bug bounties to internally identified vulnerabilities. This includes comparing externally reported medium, high and critical vulnerabilities compared to what has been found in F-Secure internally. In 2024, which is also the baseline year, the ratio is 10,1% where we have made payments while we've set a target of having this ratio under 10% by 2030.

The target measurement is not completely absolute as it depends on the human assessment of the reported finding. The criticality of the finding and hence applicability to payment also leaves room for interpretation. This shortcoming is mitigated by having multiple developers review the reports and criticality and the suggested bounty compared to earlier paid bounties. Also, the number of externally reported findings depends on the scope of the bug bounty program and by extending the scope to new products the number of reports is expected to increase. The comparison of externally reported and internally identified vulnerabilities is also dependent on ensuring that product belongs to the scope of bug bounty and not only to internal vulnerability management or vice versa.

The stakeholders who participate in target setting are the F-Secure executives relevant for software development, including the company CEO, CTO, CDO, and CISO. The short-term target can be set annually but the long-term target remains the same. The target is measured quarterly and the final measurement is conducted at the end of the year.

Sustainability Statement - Governance



G1 – Business conduct

IRO-1 Impact, risk and opportunity management

Business conduct related list of IROs

	Material impact, risk or opportunity	Description
Business Conduct		
Corruption or bribery		
Risk (VC)	Partnership business, use of agents and other intermediaries	Partner business model may increase risks of bribery and corruption in cases where middle-men are used
Risk (VC/OO)	M&A transactions	Anti-Bribery and Corruption risks rise as a result of M&A transactions due to limited understanding of the target
Political engagement		
F-Secure does not engage politically. No IROs identified.		
Management of relationships with suppliers including payment practices		
No IROs identified.		
Corporate culture		
Opportunity (OO)	New Culture program	In 2024 F-Secure is launching its new Culture program which is an opportunity to accelerate various ESG topics
Animal welfare		
No IROs identified. F-Secure business does not involve animals.		
Protection of whistleblowers		
Actual Positive impact (OO/VC)	Whistleblower channel available	Protection of whistleblowers encourages and enables all stakeholders to speak up. F-Secure has a whistleblower channel available for all Fellows and business partners. Internal awareness is raised about it in mandatory training internally.

Table 37. Business conduct list of IROs.

G1-1 Company culture

F-Secure is committed to fostering its corporate culture systematically and sustainably. To us, culture means the ways we think and act to pursue our vision and goals as an F-Secure team including the ways we act on our Code of Conduct. It is about *how* we do things right. We see that culture affects what we can achieve together, translates into our daily behavior, and that all employees and employee-like contractors play a significant role in building and living up to our culture. Through values and related behaviors, we want to enable the success and well-being of the company and the work community, teams, and individuals, and our stakeholders such as customers and partners. We also make sure that our culture supports the ethical behaviors and actions of all our employees and employee-like contractors.

In 2024, we've established our new culture including the values and aspired behaviors together with the personnel. During the process, we identified the kinds of values and behaviors that make F-Secure a great place to work and enable us to become the No.1 security experience company.

The work culminated in launching our new values including 1) Keep focus, 2) I make a difference, 3) Just do it, and 4) Dare to care. These values together create our culture which we call "Fellowship". The values shape our behavior, guide our decisions, and help us live up to our mission and reach our vision. Under each value, we have defined the wanted and unwanted behaviors associated with the value to concretize what the values mean in practice.

To foster our corporate culture, we've also put the effort in 1) leadership development and training, 2) forums and tools for leaders, 3) all company internal communications, 4) team, people and culture structures, and processes alignment, and 5) evaluation and follow-up of our culture through our personnel survey.

The F-Secure Leadership Academy offers programs for leaders at various stages. The Leadership Foundation program helps current leaders build core skills and align with F-Secure's culture, focusing on strategy, team empowerment, and feedback culture. The Aspiring Leaders program develops future leaders by enhancing leadership principles, decision-making, problem-solving, and emotional intelligence, promoting personal growth and strategic thinking.

We also develop forums and tools for leaders, including a monthly Leadership Forum for peer learning and to discuss progress in leadership and other related topics such as strategy execution. Internal communications ensure transparent information sharing and engagement with employees, establish communication strategies and

advise our leaders. We align structures and processes with our values, reviewing and renewing them to support building our culture. To track cultural development, we conduct biannual personnel surveys and pulse surveys, analyze results, and create action plans at various levels including the Leadership Team.

G1-1 Policies

Mechanisms for identifying concerns about unlawful behavior or code of conduct violation

F-Secure employees have the right and the obligation to raise a concern of a violation of the Code of Conduct. F-Secure provides multiple ways to raise a concern. Employees may talk to their line manager, Legal, or HR representatives. Concerns may also be reported via the anonymous whistleblowing channel. Employees may also write to our CEO or our Board. External stakeholders can raise concerns through the whistleblowing channel, which is publicly available on the F-Secure website.

Policies on anti-corruption or anti-bribery

F-Secure has an Anti-Bribery and Corruption Policy based on international principles, including the United Nations Convention Against Corruption. The Anti-Bribery and Corruption Policy applies to all employees, officers, and directors across all teams and subsidiaries. F-Secure's management is committed to preventing bribery, and it is the responsibility of each line manager to ensure that their teams understand and comply with this policy.

The Policy is created by the General Counsel and approved by the Board of Directors. The General Counsel is also authorized to issue detailed procedures and guidelines to further implement and enforce this policy, as well as to review and update this policy from time to time. The Policy covers prohibited conduct, gifts and entertainment, conflicts of interest, due diligence on third parties, compliance with laws, reporting and whistleblowing, training and communication, record-keeping and accounting, monitoring and review, as well as enforcement.

Whistleblowing policy and practices

At F-Secure, we are committed to a high level of ethics and integrity in conducting our business operations. We understand that this is crucial to our continued success and reputation. Our values, principles and policies guide our everyday business operations. We have a professional responsibility to speak up, report any possible corrupt, illegal or other undesirable conduct, and take required actions after such conduct is discovered.

F-Secure has a whistleblowing channel that is maintained by a third party, and employees are encouraged to submit concerns via the whistleblowing channel. F-Secure also has a Whistleblowing Policy and offers mandatory training to all employees on its Code of Conduct including a module on taking the Code to action through, amongst other means, whistleblowing.

All concerns are handled confidentially. Each reported concern is reviewed. Appropriate measures are taken against violations of the Code of Conduct. F-Secure is committed to maintaining a culture in which everyone can feel comfortable raising good-faith concerns about violations of the Code of Conduct. We do not tolerate adverse action against anyone who raises a good-faith compliance concern.

F-Secure has a responsibility to protect anyone who makes a whistleblowing report in accordance with the Whistleblowing Policy, including not disclosing their identity and ensuring they are not subject to any retaliation. Reports can be filed on a suspected breach and its potential perpetrator anonymously through our Whistleblowing Channel. All reports coming through the Whistleblowing Channel are confidential, meaning that F-Secure will protect and keep the reporter's identity and the identity of any third party possibly mentioned in the report confidential. The reporting service is entirely independent of the organization to ensure that it is impossible to find out who is behind a report, for example, by tracking IP addresses.

The Whistleblowing Policy outlines the type of protection offered to the whistleblower. This protection includes:

- identity protection; and
- protection from retaliation and possible reversal of the burden of proof in the handling of a claim related to retaliation in the courts and other authorities; and
- possible compensation and remedies e.g. due to retaliation; and
- possible protection against civil, criminal and administrative liability.

In addition to protection provided to the whistleblower, F-Secure provides protection also to person(s) who are suspected of having committed the breach. Such protection includes, for instance, that the person is treated in an equal and non-discriminating manner and the consequences of the breach are based on F-Secure's policies and applicable laws.

Procedures to investigate business conduct incidents

In accordance with the F-Secure Anti-Bribery and Corruption Policy, the effectiveness of our anti-corruption and anti-bribery efforts is regularly monitored through audits and reviews. These help us identify and address any areas of risk or non-compliance.

All employees and other parties acting on behalf of F-Secure must timely, fairly and accurately report and record their transactions involving F-Secure expenses or transfers of F-Secure assets using F-Secure's current expense management systems, including submitting and storing accurate supporting documentation. Any breach of the F-Secure Anti-Bribery and Corruption Policy will result in disciplinary action, which may include termination of employment. F-Secure is committed to investigating all allegations of corruption or bribery and enforcing this policy consistently across the organization promptly, independently and objectively.

Policy for business conduct training

F-Secure offers mandatory training on its Code of Conduct to all employees. This training consists of three parts: reading the Code of Conduct, applying its principles to example scenarios that simulate real-life situations, and resources with additional information.

The training includes an example scenario on bribery and corruption and tests the learner's ability to apply what the Code of Conduct says on the topic to a decision-making situation and covers the appropriate reporting mechanisms. The course is mandatory for all new employees during onboarding. After completing the Code of Conduct course, employees must take a refresher course on the topic every other year. For more information about the Code of Conduct training and the relevant target, refer to section Metrics and targets.

G1-3 Procedures to address corruption and bribery

F-Secure encourages a culture of openness and accountability. If any employee suspects or becomes aware of any activity that may violate this policy or any applicable anti-corruption laws, they are expected to report it immediately.

We provide several channels for reporting: Employees may talk to their line manager, Legal, or HR personnel. Concerns may also be reported via the whistleblowing channel. Employees may also write to our CEO or our Board. We guarantee that all reports will be reviewed and treated confidentially and that the reporter/whistleblower will be protected from retaliation.

To ensure that all employees understand their responsibilities under this policy, we provide regular training on anti-corruption and anti-bribery, as described on the previous page.

Every employee and party acting on behalf of F-Secure must timely, fairly and accurately report and record their transactions involving F-Secure expenses or transfers of F-Secure assets using F-Secure's current expense management systems, including submitting and storing accurate supporting documentation.

The effectiveness of our anti-corruption and anti-bribery efforts is regularly monitored through audits and reviews. These help us identify and address any areas of risk or non-compliance. The F-Secure Anti-Bribery and Corruption Policy is subject to regular review to ensure that it remains robust and relevant to our business operations.

Investigating and reporting incidents

The persons investigating any suspected incident are separate from the chain of management involved. The investigating team is determined on a case-by-case basis to ensure impartiality.

Any substantiated investigations concerning suspected incidents of bribery or corruption are also reported to the Audit Committee. A positive outcome of such an investigation would be reported to and discussed by the relevant internal management and supervisory bodies, depending on the type of incident. Additionally, such cases would be reported to the authorities where required by law.

F-Secure communicates its internal policies to its employees and, where applicable, contractors, via email, collaboration tools, company-wide town hall meetings, intranet, as well as our online learning management system.

Nature and scope of the training programs

F-Secure offers mandatory training to all employees on responsible business conduct, including anti-bribery and corruption issues. [MH1] The training includes an example scenario on bribery and corruption and tests the learner's ability to apply what the Code of Conduct says on the topic to a decision-making situation and covers the appropriate reporting mechanisms. The Code of Conduct training is mandatory for all employees, including 100% of functions at risk, namely the functions involved in sales and procurement activities that have been identified as being most at risk in respect of corruption and bribery through their operations. The course is also mandatory for executive management, including the Leadership Team.

Metrics and targets

G1-4 Targets

G1-4 Targets Business conduct

Target	Baseline 2023	2024	2030 target
Zero-tolerance on bribery & corruption	0 incidents	0 incidents	0 incidents
Code of conduct training target	Baseline is 2024	96%	98% (all employees)

Table 38. Targets Business conduct.

G1-4 Progress towards targets

There have been no (0) convictions or fines (0 euros) for violation of anti-corruption and anti-bribery laws at F-Secure.

As there have been no known breaches in procedures and standards of anti-corruption and anti-bribery, F-Secure has not taken any actions to address such breaches. If breaches were to occur, F-Secure would take appropriate action based on a case-by-case assessment of such a breach.

F-Secure has set targets for anti-bribery and anti-corruption-related incidents and to ensure our employees adhere to our conduct. The baseline year for these targets is 2023.

Zero-tolerance on bribery & corruption

F-Secure's target of zero-tolerance on bribery and corruption is based on its Code of Conduct principles of No Bribery or Corruption and Preventing Conflicts of Interest. These principles are also codified in the F-Secure Anti-Bribery and Corruption Policy.

The objective of the F-Secure Anti-Bribery and Corruption Policy is to reflect F-Secure's commitment to ethical conduct and integrity in all business activities. Honesty, professionalism, and transparency are considered essential to our corporate identity. The policy applies to all employees, officers, and directors across all teams and subsidiaries, with particular relevance to those in sales roles. F-Secure's management is committed to preventing bribery, and each line manager is responsible for ensuring their teams understand and comply with the policy.

The policy outlines F-Secure's measures to prevent bribery and corruption, including descriptions of prohibited conduct, guidance for handling conflicts of interest, and guidelines on appropriate gifts. It also addresses due diligence procedures for counterparties in sales and procurement cases, as well as employee reporting and training. The effectiveness of our anti-corruption and anti-bribery efforts is regularly monitored through audits and reviews, which help identify and address areas of risk or non-compliance.

The target is to remain at the same level of zero incidents of bribery or corruption in the whole F-Secure group. The target is absolute, and it is measured in the number of incidents related to bribery or corruption.

The target applies to the work-related activities of all F-Secure employees, contractors and other representatives across all F-Secure locations. The baseline is 0 incidents in 2023, and there are no interim targets, as the target is to prevent any future incidents. Our 2024 outcome is 0 incidents, and we will continue to report progress annually.

With this target and the accompanying policy, F-Secure is committed to complying with all laws and regulations that apply to our business activities around the world, including but not limited to the Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act 2010. This target is not related to F-Secure's targets related to environmental matters.

Both the Code of Conduct and the F-Secure Anti-Bribery and Corruption Policy, which create the basis for this target, have been approved by the F-Secure Board of Directors. There have been no changes to this policy, and no changes in the policy or F-Secure's performance in achieving the target are expected.

The performance against this target is monitored by reviewing the number of corruption and/or bribery-related incidents reported through the whistleblowing channel or to line managers, the CEO, the HR team, the Legal team, or the Board of Directors. All such reports are carefully reviewed and any reports that lead to a positive outcome are counted for this target. The data is not validated by an external party, except the reports via the whistleblowing channel, which is maintained by a neutral third party.

Code of Conduct training target

This target aims to ensure that all F-Secure employees recognize situations where the Code of Conduct is relevant and know how to make decisions in alignment with the Code in their daily work, as well as how to report any concerns or misconduct to foster ethics, transparency and accountability. The Code of Conduct describes the vision, purpose, and mission of F-Secure. The vision is to become a leading security experience company globally. The F-Secure Code of Conduct also outlines the values and principles that guide the actions needed to achieve this vision. The Code of Conduct is approved by the Board of Directors and reviewed regularly. It is supported by policies, procedures, and guidelines that provide specific enforcement methods and are periodically reviewed.

The Code of Conduct applies to all F-Secure employees and leadership, regardless of location. In addition to adhering to the principles in this Code of Conduct, F-Secure employees must comply with internal policies, as well as applicable local laws. In some cases, local laws may be less restrictive than the principles discussed in the Code. In those situations, the Code of Conduct should be followed. If local laws are more restrictive than these standards, local laws apply. F-Secure expects its suppliers and partners to act responsibly and adhere to the principles set out in the Code of Conduct. The Code of Conduct also references key international principles that F-Secure considers.

The target is that 98% of F-Secure employees and selected contractors have completed the Code of Conduct training. The target is absolute, and it is measured in percentage of the number of employees and selected contractors. The target applies to all F-Secure subsidiaries across the world. The Code of Conduct training was introduced via the F-Secure Learning Academy, the company's eLearning environment, in early 2024 and 2024 is established as the base year.

Our 2024 outcome is 96% while the target is to achieve 98% completion rate by 2027 and to maintain this level. The target is not 100% of employees to account for employees who have recently joined the company or are on a longer

leave. The rationale for the target is to raise awareness of the Code of Conduct and ensure compliance therewith, which aligns with F-Secure's commitment to proper business conduct. The target is indirectly related to F-Secure's targets related to environmental matters, as the course raises awareness of the company's commitment to respecting the environment.

The General Counsel together with the Leadership Team has set the target. The Code of Conduct training is based on the F-Secure Code of Conduct, and a group of F-Secure's employees from different teams contributed to the training modules to ensure that the example scenarios in it simulate real-life decision-making situations across the company.

There have been no changes to this policy, and no changes in the policy or F-Secure's performance in achieving the target are expected. The performance against this target is measured by reporting on the percentage of employees that have completed the training on the F-Secure Learning Academy platform. The target scope of the target is F-Secure employees, but selected contractors may also be included. The data is not validated by a third party but is based on the completion rates on the platform.

G1-4 Incidents of corruption or bribery

G1-4 Confirmed incidents

	2024
The number of convictions and the amount of fines for violation of anti-corruption and anti-bribery laws	0

Table 39. Confirmed incidents.



F-Secure Corporation

Tammasaarencatu 7
00180 Helsinki
Tel. +358 9 2520 0100
helsinki@f-secure.com
www.f-secure.com