F-Secure

Annual report 2024



Contents

F-Secure 2024 ..... **04**

This is F-Secure 04

The year 2024 in numbers 05

President and CEO's review 06

Strategy 08

Board of Directors' Report **10**

Key figures 21

Shares and Shareholders 25

Sustainability statement 27

Consolidated financial statements **132**

Statement of comprehensive income 133

Statement of financial position 134

Statement of cash flows 135

Statement of changes in equity 136

Notes to the financial statements 136

F-Secure Corporation financial statements ... **168**

Signatures of the Board of Directors' report and Financial statements **186**

Information for shareholders **189**

Auditor's report **190**

Assurance Report on the Sustainability Report **195**

Auditor's Assurance Report on ESEF Financial Statements **196**

Corporate Governance **199**

F-Secure Corporate Governance Statement 200

Board of Directors 31 December 2024 204

Leadership team 31 December 2024 212

Remuneration Report 223

This is F-Secure

We exist to make every digital moment more secure for everyone, as the world needs securing like never before.

It's become clear that we live in an era of "scam pandemic," where scams aren't just evolving - they're exploding. They're smarter, faster, and almost impossible for consumers to detect. Consumers are rightly concerned about their security and it's F-Secure's mission to deliver brilliantly simple, frictionless security experiences to protect people's digital moments.

We offer a comprehensive range of award-winning consumer cybersecurity products and services that are personalized, contextually relevant, and protect consumers from scams in the moments that matter most. By increasing consumer trust in digital, we also increase trust in society. We achieve our vision and mission together with our partners. We are a global leader in providing cybersecurity to consumers through approximately 200 channel partners and we have become the undisputed leader among the world's largest Communication Service Providers.

Headquartered in Helsinki, Finland, F-Secure operates globally from multiple locations and protects tens of millions of consumers through all its channels. F-Secure had revenue of EUR 146.3 million in 2024 and employed around 530 people. F-Secure shares are listed on the Nasdaq Helsinki Stock Exchange.

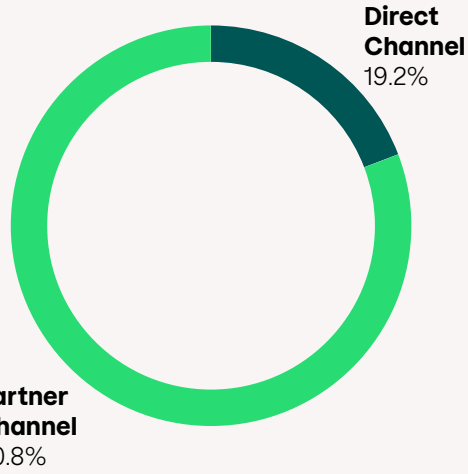


The year 2024 in numbers

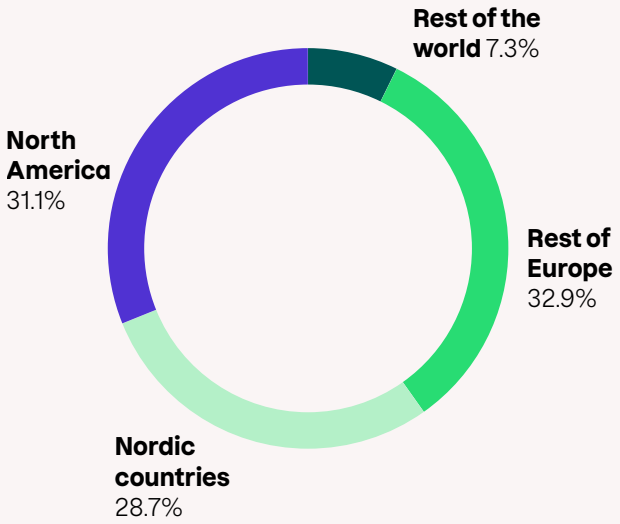
Revenue **146.3** MEUR (+12.2%)	Subscribers **~30** million across channels	Number of Service Provider Partners **~200**
Adjusted EBITA **52.2** MEUR (35.7% margin)	Users in **~200** countries	**~530** fellows
Earnings per share **0.12** EUR	Dividend per share* **0.04** EUR	**45** nationalities

*The Board proposal to the Annual General Meeting

Revenue by channel, %



Revenue by geography, %



F-Secure



President and CEO's review

During 2024, it has become evident that we're living in a scam pandemic, and F-Secure with our partners are at the forefront of defending consumers. According to a study published by the Global Anti-Scam Alliance[1] in October, more than two billion people fell victim to a scam during the year, and more than one trillion US dollars were lost worldwide. Consumers are rightly concerned about their security, and it is F-Secure's mission to deliver brilliantly simple, frictionless security experiences to protect people's digital moments.

The business environment showed a positive trend of profitable growth, driven by Lookout Life acquisition, strategic partnerships, as well as successful product developments. We achieved considerable improvements on our core technology platform performance. We made significant progress on the product front during the year, both in Total and Embedded Security, won new Tier 1 partnerships, exceeded our expectations in Direct Business and finished significant technology platform and partner delivery projects.

Throughout 2024, F-Secure focused on its growth strategy with a primary emphasis on Partner Business, enhancing capabilities to win and serve Tier 1 partners. A major strategic collaboration with a leading Communication Service Provider was announced in March, highlighting the expanding suite of embedded security products and services. The partnership underscores F-Secure's unwavering commitment to delivering innovative security solutions, both to consumers and service providers looking to protect their customers. With this strategic partnership, F-Secure reaffirms the importance of its acquisition of Lookout Life, a move that has augmented the company's mobile-first capabilities, technologies, and competence to form new Tier 1 partnerships.

The integration of Lookout Life's cutting-edge technologies has reinforced F-Secure's position as a leading player in the consumer market, generating a sense of security in the digital moments that matter most to us. The first quarter also marked the launch of a renewed corporate culture, merging F-Secure and Lookout Life values. Our renewed culture is built on the best of both companies uniting all our fellows, guiding us in everything we do. After a couple of years of big changes as a company, a common cultural ground is more relevant than ever before.

Technological independence from Lookout Life was fully achieved by the end of May, marking a milestone in F-Secure's strategic development. In June, significant progress was made with a new Total release, emphasizing scam protection and improved user experience. We also entered into a new partnership with SaskTel,

a regional telecom service provider in Canada, to enhance end-users' access to world-class protection.

The third quarter saw further product and service enhancements, including a substantial extension to the Embedded Security portfolio. With this, we entered into a high-profile partnership with SoftBank, one of the largest telecom providers in Japan. With this strategic partnership, SoftBank is providing unparalleled protection to its mobile users by making F-Secure's identity protection available to its customers as an embedded security capability within its proprietary security app. In mid-October, we implemented a transformation to drive growth and better serve our partners in each customer segment. As a result of the conducted change negotiations, we achieved the targeted organization, operational model and growth strategy alignment as well as cost savings, which will be invested back into the company's growth initiatives during 2025.

Our high-quality performance and product offering was recognized on many occasions throughout the year. In October, Omdia – an Informa Group company - ranked F-Secure as a leader among vendors providing Telcos with consumer cyber security solutions[2]. We received the highest possible rating in all six categories: Internet Security, Identity Protection & Privacy, Device & Network Protection, Professional Services, Mobile Apps, and Market Impact. F-Secure also won the best use case of AI for customer experience for its AI-based SMS Protection at the AI Gala in Finland in October. The feature forms part of F-Secure's recently launched scam protection capabilities. The award celebrates an innovation that has significantly improved customer experience with the help of AI. The award serves as further endorsement to F-Secure's vision to become the #1 in consumer security experience company in the world.

In November, F-Secure received ISO 27001 certification[3], a worldwide standard in information security management. This certification covers all company operations and represents the values and practices to which we are and have been committed to; implementing robust security policies, risk management measures, and data protection protocols to ensure that our customers' and partners' information is handled with utmost care.

Throughout the second half of the year, changes in company leadership brought new capabilities and competencies into our executive team, in line with F-Secure's vision. Our new Leadership team has been fully operational since the last quarter of the year. The team's combined expertise, experience and vision are invaluable assets as we drive transformation, growth and operational excellence at F-Secure. We remain committed to driving innovation and excellence in consumer cyber security, and the well-being, dedication and expertise of our personnel remains an absolute focus for our leadership as we enter 2025. My sincere thanks to all our Fellows for making significant strides in the execution of our growth strategy.

Timo Laaksonen, CEO & President of F-Secure

"Consumers are rightly concerned about their security and it is F-Secure's mission to deliver brilliantly simple, frictionless security experiences to protect people's digital moments."

[1] https://www.gasa.org/research
[2] https://www.f-secure.com/en/partners/insights/f-secure-ranked-as-leader-among-cyber-security-solutions-for-telcos
[3] ISO/IEC 27001:2022 certification is recognized worldwide standard in information security management and is based on the standard set by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Strategy

Our vision Become the number one security experience company in the world.

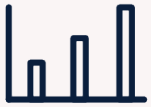
Our mission Deliver brilliantly simple, frictionless security experiences to protect peoples' digital moments

Strategic priorities

#1	#2	#3
Growth across all businesses	**Establish position as scam protection leader**	**Speed of innovation**
All channels and products contribute to revenue growth. Tier 1 deliveries and new deals as key growth engine.	Continuous flow of new scam protection capabilities. Leading Service Providers perceive F-Secure as an industry thought leader.	Unique value and differentiation through research and innovation programs powered by data and AI.

Financial targets

F-Secure medium-term financial targets reflect the company's growth ambitions and strategic direction. 2025 is still a business ramp-up year, after which the journey towards achieving the financial targets is expected to accelerate.



Growth

High single digit growth (CAGR) with additional significant upside from major Tier 1 deals.



Profitability

Adjusted EBITA margin approaching 40% as revenue reaches EUR 200 million.



Dividend yield

Around or above 50% of net profit; which can be adjusted as long as the leverage is higher than the targeted level.



Leverage

Net debt / adjusted EBITDA ratio below 2.5x, excluding temporary impact from acquisitions.

Rule of 40

F-Secure Corporation follows the Rule of 40 metric as internal performance measurement and guiding principle, according to which the combined revenue growth rate and profitability margin should be equal to or greater than 40%.

Board of Directors' Report and Financial Statements



Board of Directors' report

F-Secure Corporation in 2024

F-Secure Corporation is a globally operating consumer cyber security company. F-Secure designs and offers a comprehensive range of award-winning consumer cyber security products and services that are individually personalized, contextually relevant, and protect consumers' digital moments against scams.

F-Secure is the global leader in providing consumer cyber security through Communication Services Providers (CSPs) and has become undisputed leader among world's largest CSPs. Additionally, F-Secure partners with Service Providers such as banks and insurance companies, and sells products directly to consumers through its e-commerce platform and app stores. The company was reborn through the demerger of the consumer business from WithSecure Corporation in June 2022. In 2023, F-Secure strengthened its footprint in the US and among CSPs by the acquisition of Lookout Life, a US-based consumer mobile security business of Lookout Inc.

F-Secure's main product and service portfolios are:

Security Suite: F-Secure Total, which is an all-in-one consumer cyber security application that provides complete protection against scams as well as security, privacy and identity protection on all consumers' personal devices.

Embedded Security: Comprehensive portfolio of consumer cyber security capabilities available as Software Development Kits (SDKs) and cloud Application Programming Interfaces (APIs) that can be embedded in Service Provider's app or service, including also F-Secure Sense providing router security.

Services: F-Secure Security Business Platform based scalable expert and cloud-based services supporting both Security Suite and Embedded Security business such as delivery and integration, customer care, and partner success services that support F-Secure's Partner Business.

F-Secure operates globally in over 100 countries and has tens of millions of subscribers in all channels. F-Secure products are sold to consumers through approximately 200 CSPs, retailers, banks, insurance companies and directly through online and app stores. F-Secure shares are listed on the official list of Nasdaq Helsinki.

Presentation of financial information

Figures in brackets refer to the corresponding period in the previous year, unless otherwise stated. Percentages and figures presented herein may include rounding differences and therefore may not add up precisely to the totals presented.

As announced on 20 March 2024, F-Secure changed the calculation method for gross margin in its income statement. Some of the costs previously recorded in F-Secure income statement as cost of revenue have been included in research and development and Sales and marketing costs. F-Secure applies the new calculation method for gross margin as of 1 January 2024. Comparative figures are also revised.

Financial performance

Revenue

F-Secure revenue increased in January–December 2024 by 12.2% to EUR 146.3 million (EUR 130.4 million). Revenue growth was attributable to the acquisition of Lookout Life consumer business in the second quarter of 2023. Organic revenue growth in January–December was 1.8% and currency neutral organic growth was 2.2%, with impact especially from the JPY but also from the US dollar. Revenue was also impacted by fair valuation adjustments of deferred revenue EUR -1.5 million (EUR -3.1 million) made in purchase price allocation. Deferred revenue increased by 11.1% from last year mainly due to the billings of a large partner contract.

Partner Channel

Revenue from the partner channel increased by 12.5% to EUR 118.2 million (EUR 105.1 million). Organic revenue growth in the partner channel was 2.4%. The strategic collaboration with one of the world's leading CSP, announced in the first quarter, supported revenue growth in the partner channel. The actual business ramp-up started in December 2024 and will bring results towards 2025. Nevertheless, revenue of some long-time F-Secure partners continued to decline as they were addressing challenges in their core business.

Partner channel revenue increased in the USA as well as in the Asia-Pacific (APAC) area, especially in Japan. Revenue increased also in Finland and Sweden. Challenges in Poland eased towards the end of the year. Revenue decreased in Germany and in the UK, due to continued weak partner business performance.

Direct Channel

Revenue from the direct channel increased by 11.0% to EUR 28.0 million (EUR 25.2 million). Organically revenue declined in the direct channel by -0.5%. Renewals remained on a good level throughout the year. The decrease in paid customer acquisition investments was reflected in Direct Business new sales throughout the period as planned.

Revenue by sales channel

EUR million	1-12/2024	1-12/2023	Change %
Revenue from external customers			
Partner channel	118.2	105.1	12.5%
Direct channel (E-commerce)	28.0	25.2	11.0%
Total	**146.3**	**130.4**	**12.2%**

Revenue by geography

EUR million	1-12/2024	1-12/2023[1)]	Change %	Comparable change %[2)]
Revenue from external customers				
Nordic countries	42.0	40.0	5.1%	5.1%
Rest of Europe	48.1	49.2	-2.3%	-2.3%
North America	45.5	32.8	38.8%	39.9%
Rest of the world	10.6	8.4	26.9%	30.3%
Total	**146.3**	**130.4**	**12.2%**	**12.6%**

1) F-Secure has adjusted the geographical split of revenues between Rest of Europe and North America. This adjustment impacts also the change percentages. The adjustment did not have a material impact to the reported figures.

2) Comparable change excludes the impact of exchange rates.

Gross margin

Gross margin was 126.0 million (EUR 118.6 million) and 86.2% of revenue (90.9%). Lookout Life business has a lower gross margin level than what F-Secure traditionally had. The gross margin was also impacted by fair valuation adjustments of deferred revenue made in purchase price allocation. In addition, the gross margin was burdened by some additional costs related to lost synergies post-TSA period. This impact materialized already in the first quarter as full technical autonomy was achieved at the end of 2023 when the TSAs ended with WithSecure. This cost profile gradually improved throughout the year as we have made progress in consolidating our production operations and adapted our hosting infrastructure fully to the usage patterns of an independent consumer company.

The transitional services agreements ("TSA") entered between F-Secure and Lookout consumer security business amounted to EUR 4.3 million (EUR 2.7 million) in cost of revenue in January–December 2024. The only remaining TSA is planned to last several years and is already of commercial nature.

Operating expenses

Operating expenses excluding depreciation and amortization and items affecting comparability (IAC) were EUR -73.3 million (EUR -73.7 million) in January–December 2024. Sales and marketing costs were lower than in the comparison year and totaled EUR -33.4 million (EUR -35.9 million). Decline was mainly due to lower marketing costs in Direct business as planned. Research and development (R&D) costs were EUR -25.4 million (EUR -25.2 million). However, overall R&D cost increased, but more R&D investments were booked as capital expenditure. Administration costs were EUR -14.5 million (EUR -12.7 million), where the increase is related to building maturity specific to Tier 1 partner business.

The transitional services agreements ("TSA") entered between F-Secure and Lookout consumer security business amounted to EUR 1.8 million (EUR 1.7 million) in R&D and EUR 0.2 million (EUR 0.4 million) in administration in January–December 2024. The one remaining TSA in R&D is planned to last several years and is already of commercial nature. The last TSAs in administration terminated during the second quarter of 2024.

Items affecting comparability (IAC) totaled EUR -1.4 million (EUR -8.0 million), consisted of costs mainly related to restructuring and change

negotiation activities announced in October 2024. The comparison period included EUR -6.1 million of items affecting comparability attributable to the acquisition of Lookout consumer security business and EUR -1.8 million restructuring costs related to change negotiations.

Depreciation and amortization excluding purchase price allocation amortization (PPA) totaled EUR -5.8 million (EUR -3.5 million). PPA amortizations related to the Lookout consumer security business acquisition totaled EUR -7.8 million (EUR -4.7 million) in January–December 2024.

Profitability

Adjusted EBITA in January–December 2024 was EUR 52.2 million and 35.7% of revenue (EUR 44.6 million, 34.2%). Items affecting comparability (IAC) were EUR -1.4 million (EUR -8.0 million). EBIT was EUR 38.4 million and 26.3% of revenue (EUR 29.5 million, 22.6%). Profitability was positively impacted by the recording of more long-term technology investments as capital expenditure in the second and third quarter and burdened by higher amortizations and purchase price amortizations.

Cash flow, financial position and financing

In January–December 2024, cash flow from operating activities before financial items and taxes amounted to EUR 53.9 million (EUR 37.6 million), where the increase was due to the acquisition of Lookout Life consumer business. Cash flow from operations was EUR 38.8 million (EUR 30.1 million). Cash conversion rate in January–December 2024 was 80.5% (81.2%). Cash at the end of December 2024 amounted to EUR 8.1 million (EUR 15.9 million). F-Secure has a revolving credit facility (RCF) of EUR 20 million that matures in 2027. F-Secure has drawn down EUR 8 million revolving credit facility for general cash management purposes.

At the end of December 2024, F-Secure net debt amounted to EUR 163.6 million (EUR 177.4 million) and net debt to adjusted EBITDA ratio was 3.1x, being above the medium-term target of below 2.5x, due to Lookout Life acquisition. Subsequently, equity ratio was 17.4% (12.0%). The acquisition of Lookout Life consumer business in the second quarter of 2023 was financed with debt. The Group's loan agreement includes a quarterly measured financial covenant based on the ratio between net debt and adjusted EBITDA. The group has met these covenant terms and conditions on the reporting date. The term loan was repaid by EUR 30 million during financial year 2024.

Total assets were EUR 270.6 million (EUR 275.3 million) at the end of December 2024.

As of 31 December 2024, current lease liabilities were EUR 0.7 million (EUR 1.0 million) and non-current lease liabilities were EUR 0.5 million (EUR 0.3 million). The lease liabilities relate to leases for office premises and cars. In the second quarter of 2024, F-Secure signed a new lease agreement for headquarter office premises. This will be recorded in the balance sheet as right-of-use asset and lease liability during summer of 2025 when the lease term starts, but the lease commitment already exists following the agreement.

F-Secure payables to WithSecure totaled EUR 5.3 million and the receivables from WithSecure totaled EUR 3.8 million. These balances are now short-term and due for payment in the second quarter of 2025 as per the original repayment schedule.

In January–December 2024, capital expenditure including acquisition was EUR 11.2 million (EUR 215.7 million) and was mainly related to technology.

Acquisitions and financial arrangements

F-Secure hasn't made any acquisitions during the reporting period.

During the comparison period, F-Secure announced the acquisition of Lookout consumer security business, US-based consumer focused mobile security business arm of Lookout Inc. The acquired mobile consumer security business unit consists of shares of Lookout LLC in the US and Saferpass s.r.o. in Slovakia as well as certain IP and related know-how transferred to Finland. The acquisition was completed on 1 June 2023. The enterprise value of the acquisition was USD 223 million (approx. EUR 202 million) on a cash and debt-free basis. The acquired business was consolidated as part of F-Secure from 1 June 2023 onwards. In the transaction 65 employees were transferred to F-Secure.

The acquisition was financed with debt for which a new facilities agreement was entered into with Danske Bank A/S and OP Corporate Bank plc. The new financing package consists of two facilities, (i) a EUR 202 million amortizing term loan to finance the acquisition, and (ii) a EUR 20 million revolving loan facility to be used for general corporate purposes of the combined group. The Group's loan agreement includes a quarterly measured financial covenant based on the ratio between net debt and adjusted EBITDA. The group has met covenant terms and conditions on the reporting date. During the reporting period, F-Secure has repaid EUR 30.0 million of the term loan. In addition, F-Secure has drawn down EUR 8 million revolving credit facility for general cash management purposes.

Group structure and changes

No changes have occurred to group structure during the reporting period.

During the comparison period the following changes occurred: Lookout LLC was acquired in connection with the acquisition of Lookout Life on 1 June 2023. Lookout LLC was merged with F-Secure Inc on 15 June 2023. F-Secure s.r.o. (previously SaferPass s.r.o.) was acquired in connection with the acquisition of Lookout Life on 1 June 2023.

Loans, liabilities and guarantees from related parties

F-Secure Corporation's receivables from companies within the same group are presented in note 12 of the parent company's financial statements. These have been provided on market terms. The company has not provided any other loans, liabilities, or guarantees to related parties.

Significant events during the financial year

Updated medium-term financial targets

On 19 November 2024, F-Secure updated the medium-term financial targets and dividend policy for the company. The updated targets reflect the company's growth ambitions and strategic direction. 2025 is still a business ramp-up year, after which the journey towards achieving the financial targets is expected to accelerate. The updated financial targets and dividend policy can be found under Financial targets.

Change negotiations

On 2 December 2024, F-Secure completed the change negotiations that were started in October 2024. The change negotiations concerned most operations within Sales, Marketing, Services and Technology, and approximately 360 F-Secure employees were within the scope of the negotiations. As a result of the concluded change negotiations 33 positions would be terminated, of which 19 in Finland. The estimated annual cost savings of EUR 4 million will be reinvested back into the company to support growth and improve sales and service maturity. One-off costs related to the changes amounted to EUR 1.5 million, and these were recorded as items affecting comparability (IAC) in the fourth quarter of 2024.

Research and development

F-Secure Corporation research and development expenditure amounted to EUR 29.3 (27.5) million in 2024, representing 20.0% (21.1%) of revenue and 33.1% (30.6%) of all expenditures. Capitalized investments in technology were EUR 11.0 (7.6) million.

In 2024, F-Secure Technology function invested heavily in our Total and Embedded product portfolio; in research supporting our product strategy; and in modernizing our technology landscape.

A major theme throughout 2024 was the continued development of our flagship all-in-one Total app, incorporating valuable new intellectual property (IP) brought in from the Lookout Life acquisition, for example the Saferpass password manager. This has resulted in a product which will bring increased value to all our partners as we roll it out throughout 2025.

We are also bringing our own unique IP to the market; our industry-leading SMS Scam Protection capability became available through the Total app, and showed its excellence by winning an award for "best use case of AI for customer experience" at Finland's AI Gala. Throughout 2024 we continued to invest heavily in research efforts, particularly around the scam protection topic. We presented our Scam Techniques and Tactics Framework at the Microsoft Bluehat conference, and in October we launched our first F-Secure Scam Intelligence and Impacts Report, showcasing our insights.

A significant part of our Technology effort in 2024 went directly towards serving our strategic partners. We significantly broadened our Embedded portfolio, through which we believe we now offer the broadest range of SDK/API capabilities in the industry. As a result, we deliver a major product upgrade to AT&T, as well as the first product release to the Tier 1 CSP that we signed in March of 2024, which was successfully launched to end-users before the end of the year.

We continued to invest in our existing technology assets, developing a next-generation VPN client which is complete and will be launched early in 2025. Further, we completed a major modernization to our core anti-malware capabilities, improving performance and reducing cost. Part of this is already launched, and the remaining portion will go live in the first half of 2025.

Finally, we reached two major milestones in modernizing our technology landscape. First, we completed the program of work needed to decouple ourselves from the systems managed by Lookout under the TSA agreement; this work was completed on time in the first half of the year. Second, having successfully upgraded the last remaining partners to newer version, we completely switched off a number of legacy systems supporting old versions of our server software; this happened as planned shortly before the end of the year. These two actions help us reduce our operational overhead and improve the reliability of our systems.

Personnel, management and auditors of the company

At the end of December 2024, F-Secure had 529 (524) employees. The average number of personnel in 2024 was 519 (484). Wages and salaries were EUR 36.1 (33.3) million in 2024.

F-Secure's most important intangible resource is our personnel, which is critical for implementing our strategy. This includes i) our product and technology organizations, who ensure the competitiveness of our product portfolio and our ability to protect consumers' digital moments through research and innovation, ii) our sales, marketing, and services organizations, through which we can serve our partner segments and consumers. In addition, our business support organizations (corporate development, finance and people & culture) support the operational activities of our organization.

During the fourth quarter of 2024, F-Secure conducted change negotiations to reorganize the company to better reflect company's increased focus on addressing specific partner segment needs and opportunities and to secure the successful execution of the company's growth strategy. The change negotiations concerned most operations within Sales, Marketing, Services and Technology. As a result of the concluded change negotiations, 33 positions would be terminated, of which 19 in Finland. All those made redundant were still on the payroll at the end of December 2024.

Leadership team

During 2024 the following changes to F-Secure executive leadership team were announced: Bruno Rodriguez was appointed Chief Revenue Officer and a member of the Leadership Team starting on 1 October 2024. Nina Lehto was appointed as Senior Vice President, Services and a member of the Leadership Team starting on 26 August 2024. Previous SVP Services, Mikko Kestilä was appointed to a new role within the company. Kaisa Tikka-Mustonen was appointed as Chief People Officer and a member of the Leadership Team as of 2 September 2024. Kitta Virtavuo, a former Chief People Officer decided to leave the company in April 2024. Mikko Kestilä was appointed Senior Vice President, Services and member of the Leadership Team as of January 2024. Firas Azmeh, previously Chief Commercial Officer assumed a role of Chief Revenue Officer as of 1 January 2024, while continuing as a member of the Leadership Team. Mr Azmeh decided to leave the company at the end of June 2024.

At the end of December 2024, the composition of the Leadership Team was the following:

Timo Laaksonen	President & Chief Executive Officer
Richard Larcombe	Chief Marketing Officer
Nina Lehto	Senior Vice President, Services
Antero Norkio	Senior Vice President, Corporate Development
Bruno Rodriguez	Chief Revenue Officer
Sari Somerkallio	Chief Financial Officer
Kaisa Tikka-Mustonen	Chief People Officer
TL Viswanathan	Chief Product Officer
Toby White	Chief Technology Officer

The Board of Directors

Members of the Board of Directors of F-Secure are Pertti Ervi, Risto Siilasmaa, Thomas Jul, Petra Teräsaho, Tommi Uitto and Katja Kuusikumpu. Katja Kuusikumpu belongs to the personnel of the F-Secure Corporation. 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, except the people belonging to the company's Leadership Team, is eligible to stand as a candidate. The representatives of the Board of Directors interview three 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.

Auditor

The auditor of F-Secure Corporation is the Authorized Public Accountant PricewaterhouseCoopers Oy with Samuli Perälä, APA, as the auditor with the principal responsibility. The same audit firm acts as sustainability reporting assurance provider for the financial year 2024.

Share-based incentive plans

F-Secure has share-based incentive programs for the key personnel of the company. The share-based long-term incentive plans include a Performance Share Plan as the main plan and Restricted Share Plan as a complementary share-based incentive plan for individually selected key employees in specific situations. The purpose of the share-based long-term incentive plans is to align shareholders' and management's interests, motivate and incentivize key individuals to focus on F-Secure's long-term success and targets and to commit key resources in the company.

In addition, F-Secure has an Employee Share Savings Plan (ESSP). The ESSP consists of annually commencing plan periods, each one comprising a 12-month savings period and a holding period following the savings period. The ESSP is offered to all F-Secure employees. The employees have an opportunity to save a proportion of their salaries and invest those savings in F-Secure shares. The savings are used for acquiring F-Secure shares quarterly after the publication of the respective interim reports. As a reward for the commitment, F-Secure grants

the participating employees a gross award of one matching share for every two shares acquired with their savings. Continuity of employment and holding of acquired shares for the duration of the holding period are the prerequisites for receiving the award.

More information on the programs is provided in Note 19 Share-based payment transactions of the Financial Statements, as well as in the Remuneration Report, which is published separately from the Board of Directors report.

Shares and shareholders

Shares and share capital

At the end of December 2024, the registered share capital of F-Secure was 80,000 and the company had 174,673,165 fully paid shares. F-Secure has one share class and the company's shares are included in a book-entry system.

Information on the authorizations held by the Board of Directors in 2024 to issue shares and special rights entitling to shares, to transfer shares and repurchase own shares, is available in the section on the Annual General Meeting 2024.

Trading of shares

The closing price of the share at the end of December 2024 was EUR 1.78. In January–December 2024, the highest price paid was EUR 2.33 and the lowest EUR 1.67. In January–December 2024, the share's volume weighted average price was EUR 1.95. The share trading volume in January–December 2024 was EUR 45 million or 23 million shares. On 31 December 2024, the company's market capitalization was EUR 312 million.

Shareholders

The number of registered shareholders at the end of December 2024 was 33,921, including nominee registers. The proportion of nominee-registered and direct foreign shareholders was 9.98% of the company's shares at the end of the year. The list of the shareholders of F-Secure Corporation is based on the information given by Euroclear Finland Ltd.

Treasury shares

During or at the end of the financial year 2024, F-Secure did not hold any treasury shares.

Flagging notifications

During the review period, F-Secure received one flagging notification of change in holdings in accordance with Chapter 9, Section 10 of the Securities Market Act:

According to a notification received on 20 February 2024, the number of voting rights in F-Secure controlled by Nordea Funds decreased below ten (10) per cent of the total shares and voting rights of F-Secure Corporation on 19 February 2024.

Short-term risks and uncertainties

Risks related to the integration of Lookout consumer business

Following the completion of the transitional services agreements (TSA) and carve-out with Lookout, F-Secure faces an elevated risk level due to the new operational landscape. Despite gaining full control, the integration of acquired systems, processes, and personnel has introduced complexities and potential operational challenges that may expose F-Secure to claims related to Service Level Agreements ("support penalties"), and/or impact negatively partner relationships and future revenue outlook. This heightened risk is expected to persist in the short-term as we adapt to and optimise our expanded operations. F-Secure is actively monitoring and implementing mitigation strategies to reduce the risk exposure over time.

Risks related to F-Secure's operating environment

Intensifying competition in the consumer security market could lead to a general decline of the price level and affect F-Secure's ability to maintain or increase its market share, and the intensifying competition could thus have an adverse effect on F-Secure revenue, profitability and market share.

F-Secure may not be able to keep up with rapid changes in customer demand, distribution channels, technologies and the evolution of malware and cyber security threats, which could have an adverse effect on F-Secure reputation, competitiveness, operational results and financial position.

Uncertainty on F-Secure's key markets, financial markets and general economic situation could have an adverse effect on F-Secure's business and growth opportunities and reduce the demand or increase cost of the products and services offered by F-Secure. Geopolitical instability has increased uncertainty in the world and the risk of unexpected disruptions of the world economy. The war for example in Ukraine has caused some exceptional consequences to the cyber security landscape, such as highly visible governmental activities, as well as organized civilian response to the war efforts.

Risks related to F-Secure's business operations and strategy

If F-Secure's agreement with a significant business partner or Channel Partner ends or is terminated, or if F-Secure is unable to continue cooperating

with a business partner or Channel Partner under acceptable terms, or if there is a failure by a Channel Partner to fulfil its duties, this could significantly decrease F-Secure revenue, increase its costs, hinder its operative business and weaken its ability to offer services or solutions to its customers. Furthermore, some Channel Partners may be slow in adopting new solutions that may delay F-Secure revenue growth or increase maintenance related costs.

The loss of key persons and skilled employees, the possible delay of new hires or increase in personnel expenses could weaken F-Secure's profitability and the standard of its services or solutions, hinder operations and prevent F-Secure from successfully developing and growing its business.

Actual, possible or perceived defects, disruptions or vulnerabilities in F-Secure products or services, including risks from cyber security attacks and errors or abuses by F-Secure employees and business partners, could harm F-Secure or its customer reputation, decrease sales, hinder operations, tie up personnel resources and give rise to claims for damages and increase other costs.

Integration of F-Secure and Lookout consumer security product portfolios over time may prove to be more costly than estimated or take longer than planned. These may increase F-Secure's costs or negatively impact planned future product releases, their scope, availability and/or competitiveness and thereby revenue growth.

F-Secure provides consumer cyber security solutions to some of the largest Service Providers in the world ("Tier 1 Channel Partners") and aims to win new Tier 1 Channel Partner contracts. Tier 1 Channel Partners may require solutions that F-Secure is unable to create, deliver and maintain with sufficient profitability over time. These contracts may also expose F-Secure to claims related to Service Level Agreements (support penalties) or include other similar and material contractual liabilities , such as consumer data breach. F-Secure may have to invest upfront to create and deliver said solutions, which in turn may have a negative impact on F-Secure product roadmaps, company revenue and profitability.

F-Secure is in the process of transforming the company and its operating model with its growth strategy. Changes in the company strategic priorities, structure and processes may take time to become effective. Additionally, these changes may at least initially have a negative impact on company's product roadmap and its operations. New strategy and implemented changes may also lead to higher attrition rate. These combined can have a negative impact on financial outlook of the company.

Risks related to the technology used by F-Secure, intellectual property rights and other regulations

Any malfunctions in technologies, IT systems or network connections used by F-Secure or any security breaches could endanger disruptions to F-Secure's service offering. F-Secure may not succeed in registering, protecting, managing, maintaining and enforcing its intellectual property rights, and F-Secure may be targeted by intellectual property right infringement claims which can cause significant costs. Leakage of personal data collected by F-Secure may have a material adverse effect on F-Secure's business and reputation and result in claims for damages as well as fines and orders imposed by the authorities. As is customary in the cyber security industry, F-Secure protection is combination of own IPR and third-party solutions. F -Secure continues to have a relationship with Lookout and WithSecure, related to certain protection capabilities after the carve-out and demerger and having completed the TSAs with both companies. third-parties, such as Lookout's or WithSecure's, inability to provide these protection capabilities could have a material adverse effect on F-Secure's business operations and its customers.

Risks related to F-Secure's financial position and financing

The number of operations and sites outside the Eurozone in different currencies exposes F-Secure to a risk related to currency fluctuations. Changes in the exchange rates between currencies could have an adverse effect on F-Secure's revenue, results and financial position. F-Secure is exposed to transaction risks caused by purchasing and selling products and goods in currencies that are not F-Secure's home currencies, especially USD after Lookout consumer security business acquisition. In addition, F-Secure is exposed to investment risks in units abroad and translation risks that arise when investments in subsidiaries in different currencies are converted into F-Secure's operational currency, i.e., the euro. Furthermore, F-Secure financed the acquisition of Lookout's consumer security business with bank debt subject to leverage covenants. Failure to comply with the covenants would lead to early expiry of the debt. Changes in interest rates have an impact on interest costs.

Annual General Meeting 2024

The Annual General Meeting of F-Secure Corporation held on 13 March 2024 adopted the annual accounts and the consolidated annual accounts for the financial year ended 31 December 2023, discharged the members of the company's Board of Directors and the CEO from liability, and approved all proposals made to the Annual General Meeting by the Board of Directors. The Annual General Meeting also approved the 2023 remuneration report for governing bodies.

The resolution was of an advisory nature according to the Finnish Companies Act.

Resolution on the use of the profit shown on the balance sheet and the payment of dividend

The Annual General Meeting resolved that for the financial year that ended on 31 December 2023, a dividend of EUR 0.07 per share be paid. The dividend was paid in two installments as follows; The first dividend instalment of EUR 0.035 per share was paid on 22 March 2024. The second dividend instalment of EUR 0.035 per share was paid on 4 October 2024.

Composition and remuneration of the Board of Directors

The Annual General Meeting resolved that the number of members of the Board of Directors shall be six (6). The current board members Pertti Ervi, Risto Siilasmaa, Thomas Jul and Petra Teräsaho were re-elected to the Board of Directors. Tommi Uitto was elected as a new member. Katja Kuusikumpu, who belongs to the personnel of the corporation, was also elected as a new member of the Board of Directors.

It was resolved that the remuneration of the members of the Board shall remain unchanged. The remuneration is as follows: EUR 80,000 annually for the Chair of the Board of Directors, EUR 48,000 annually for the Committee Chairs, EUR 38,000 annually for the members of the Board of Directors, and EUR 12,667 for members employed by F-Secure. It was resolved that approximately 40% of the remuneration be paid as shares in the company repurchased from the market or as treasury shares held by the company. The company will pay any transfer tax levied on the repurchase of shares. The company will repurchase the shares or transfer shares held by the company as treasury shares in the name and on behalf of the members of the Board of Directors.

Furthermore, the travel expenses and other costs of the members of the Board of Directors directly related to board work are paid in accordance with the company's policy in force from time to time and that each member of the Board of Directors of F-Secure is paid a predetermined travel fee in addition to travel expenses for meetings held outside their country of residence as follows: A separate meeting fee of EUR 1,000 is paid to the Board members travelling from another European country to an on-site meeting in Europe. If inter-continental travel is required, the fee is EUR 2,000. No separate travel fee will be paid to members of the Board of Directors employed by the company.

Election and remuneration of the Auditor

The Annual General Meeting re-elected the audit firm PricewaterhouseCoopers Oy as auditor of the company. Mr Samuli Perälä, APA, will continue as the company's Responsible Auditor. The same audit firm was elected to audit the sustainability report from the financial year 2024.

The Auditor will be remunerated in accordance with an invoice approved by the company and the same applies to the auditor's fees relating to the audit of the company's sustainability report from the financial year 2024.

Authorizing the Board of Directors to decide on the repurchase of the company's own shares

The Annual General Meeting authorized the Board of Directors to resolve on the repurchase of a maximum of 10,000,000 of the company's own shares in one or more installments with funds belonging to the company's unrestricted equity. This number of shares corresponds to approximately 5.72% of the company's total number of shares on the date of the notice to the Annual General Meeting

The authorization entitles the Board of Directors to decide on the repurchase also in deviation from the proportional holdings of the shareholders (directed repurchase). The authorization comprises the repurchase of shares either in public trading or otherwise based on the market price on the date of purchase, or with a bid to the shareholders in which case the repurchase price must be the same for all shareholders. The company's own shares shall be repurchased to be used for carrying out acquisitions or implementing other arrangements related to the company's business, for optimizing the company's capital structure, as part of the implementation of the company's incentive scheme or otherwise to be transferred further or cancelled. The authorization includes the right of the Board of Directors to decide on all other terms related to the repurchase of the company's own shares. The authorization is valid until the conclusion of the next Annual General Meeting, but no later than 30 June 2025. The authorisation cancels the company's prior authorizations concerning the repurchase of the company's own shares.

Authorizing the Board of Directors to decide on the issuance of shares and special rights entitling to shares

The Annual General Meeting authorized the Board of Directors to decide on issuance, in one or more installments, of new shares or shares possibly held by the company through share issue and/or issuance of option rights or other special rights entitling to shares, referred to in Chapter 10, Section 1 of the Finnish Limited Liability companies Act, so that by virtue of the authorization altogether 17,000,000 shares may be issued and/or transferred at the maximum. This number of shares corresponds to approximately 9.73%

of the company's total number of shares on the date of the notice to the Annual General Meeting.

The authorization can be used for financing or execution of potential acquisitions or other arrangements or investments relating to the company's business, for implementation of the company's incentive scheme or for other purposes subject to the Board of Directors' decision.

The authorization entitles the Board of Directors to decide on all terms and conditions of the share issue and the issuance of special rights referred to in Chapter 10, Section 1 of the Finnish Limited Liability Companies Act. The authorization thus includes the right to issue shares also in a proportion other than that of the shareholders' current shareholdings in the company under the conditions provided in law, the right to issue shares against payment or without charge, as well as the right to decide on a share issue without payment to the company itself, subject to the provisions of the Finnish Limited Liability Companies Act on the maximum amount of treasury shares.

The authorization will remain valid until the conclusion of the following Annual General Meeting, but no later than 30 June 2025. The authorization cancels the company's prior authorizations concerning the issuance of shares and special rights entitling to shares.

Organizational meeting of the Board of Directors

In its organizational meeting the Board of Directors of F-Secure re-elected Pertti Ervi as Chairman of the Board of Directors. From among its members, the Board elected Petra Teräsaho (Chair of the committee), Pertti Ervi and Risto Siilasmaa as members of the Audit Committee.

Establishment of the Personnel and Nomination Committee

In its organizational meeting, the Board of Directors resolved to establish a Personnel and Nomination Committee. The Personnel and Nomination Committee prepares material and instructs with issues related to composition and compensation of the Board of Directors and remuneration of other members of top management of the company. From among its members, the Board elected Pertti Ervi (chair of the committee) and Risto Siilasmaa as members of the Personnel and Nomination Committee. Following the announcement on 3 April 2024, F-Secure Corporation's Board of Directors appointed Thomas Jul, F-Secure Board member as the third member of the Personnel and Nomination Committee.

Outlook for 2025

Growth: F-Secure expects mid-single digit revenue growth for 2025.

Profitability: The group's adjusted EBITA is expected to be approximately on the same level as in 2024 (EUR 52.2 million).

Background for the outlook:

- F-Secure expects the core consumer cyber security market to grow mid-single digit CAGR mid- to long-term[1]. F-Secure sees the potential to grow faster than the market focusing on partner channel and its offering around Embedded security and Scam Protection. The growth may be moderated due to the uncertainties around consumer sentiment in certain markets.
- Partner business and especially Embedded services expected to drive F-Secure growth during 2025. Growth is expected to accelerate throughout the year as new partners and services gradually start to generate revenue.
- Direct business revenue development is expected to be negative due to continued strategy of refraining from paid customer acquisition.
- Gross margin is expected to be slightly lower than in 2024 (86.2%) due to growth of strategic partners with embedded solutions, as these typically have a lower gross margin level than F-Secure Total business.
- F-Secure continues to develop its service, operations and production capabilities further to meet Tier 1 partner requirements. These efforts are still reflected in the higher cost base. As business scales we expect to leverage continued service level investments across a wider partner base, leading to positive Adjusted EBITA % development over time.
- Capex level is expected to remain on similar level as in 2024. However, new product development projects related to partner demand can have an impact on the outcome.

Financial targets

F-Secure's medium-term financial targets and dividend policy for the company was published on 19 November 2024. The targets reflect the company's growth ambitions and strategic direction. 2025 is still a business ramp-up year, after which the journey towards achieving the financial targets is expected to accelerate.

- **Growth:** High single digit growth (CAGR) with additional significant upside from major Tier 1 deal
- **Profitability:** Adjusted EBITA margin approaching 40% as revenue reaches EUR 200 million

[1] Industry analyst views such as Gartner and IDC, and F-Secure management estimates

- **Dividend Yield:** Around or above 50% of net profit; which can be adjusted as long as leverage is higher than the targeted level
- **Leverage:** Net debt / adjusted EBITDA ratio below 2.5x, excluding temporary impact from acquisitions

F-Secure Corporation follows the Rule of 40 metric as internal performance measurement and guiding principle, according to which the combined revenue growth rate and profitability margin should be equal to or greater than 40%.

Corporate Sustainability Statement

F-Secure has prepared its Sustainability Statement in accordance with the EU Corporate Sustainability Reporting Directive (CSRD) and the related Finnish legislation. The statement is published with this Board of Director's Report; (Sustainability statement 2024).

Annual General Meeting 2025

The Annual General Meeting 2025 is scheduled for Tuesday, 1 April 2025. The Board of Directors will convene the meeting.

Board of Directors' proposal for the distribution of profit

According to the company's dividend policy, F-Secure aims to pay around or above 50% of net profit as dividend on an annual basis, which can be adjusted as long as leverage is higher than the targeted level. On 31 December 2024, distributable funds of F-Secure Corporation were EUR 13.7 million. As the leverage (3.1x) is above the target level, the Board of Directors proposes to the Annual General Meeting 2024 that a dividend of EUR 0.04 per share to be paid. Earnings per share (EPS) for the period January–December 2024 was EUR 0.12, and the proposed dividend is 33.2% of the group's January– December 2024 earnings. The dividend is proposed to be paid in two installments.

No material changes have occurred in the company's financial position since the end of the financial year.

Significant events after the review period

On 10 January, F-Secure Board's Personnel and Nomination Committee gave proposals to the Annual General Meeting scheduled for 1 April 2025 for the composition and remuneration of the Board of Directors. Committee proposes that the Board of Directors consists of a total of six members and that the following persons be elected as members of the Board of Directors for a term expiring at the end of the Annual General Meeting 2026: Pertti Ervi, Petra Teräsaho and Tommi Uitto are proposed to be re-elected, and as new members, are proposed to be elected Roxana Diaconescu and Cornelia Schaurecker. Of the current members, Thomas Jul and Risto Siilasmaa have informed that they are not available for re-election to the Board.

The Personnel and Nomination Committee proposes to the Annual General Meeting that the following annual remuneration be paid to the members of Board of Directors to be elected at the Annual General Meeting: EUR 80,000 annually for the Chair of the Board of Directors; EUR 38,000 annually for the external members of the Board of Directors; EUR 12,667 for members employed by F-Secure; EUR 10,000 additional remuneration for the Audit Committee Chair; EUR 4,000 additional remuneration for the Personnel and Nomination Committee Chair; EUR 2,000 additional remuneration for the members of Audit Committee as well as Personnel and Nomination Committee. The proposed annual fee and the fees for Committee work correspond to the current remuneration, with the exception of the additional remuneration for Personnel and Nomination Committee Chair and members of the Audit Committee and Personnel and Nomination Committee. In addition, The Personnel and Nomination Committee proposes that approximately 40 percent of the remuneration be paid as shares in the company repurchased from the market or as treasury shares held by the company.

On 7 February 2025, F-Secure Board's Personnel and Nomination Committee supplements the original proposal to the Annual General Meeting 2025 for the composition of the Board of Directors. In deviation from the proposal made on 10 January 2025, F-Secure Board's Personnel and Nomination Committee proposes that i) the board would consist of seven members and that ii) Alessandro Adriani and Rachit Mittal be elected as new members in addition to the previously proposed members. Except for the revised proposal concerning the Board's composition, the proposal by the Board's Personnel and Nomination Committee remains valid and unchanged.

Key figures

EUR million	2024	2023	2022	Carve-out 2021	Carve-out 2020
Revenue	146.3	130.4	111.0	106.3	100.1
Revenue growth %	12.2%	17.4%	4.5%	6.1%	5.5%
Adjusted EBITDA	53.5	45.7	44.5	47.4	46.7
% of revenue	36.6 %	35.0 %	40.1 %	44.6 %	46.7 %
EBITA	50.8	36.6	40.2	44.8	46.5
% of revenue	34.7%	28.1%	36.2%	42.2%	46.5%
Adjusted EBITA	52.2	44.6	43.9	47.2	46.5
% of revenue	35.7 %	34.2 %	39.6 %	44.4 %	46.5%
EBIT	38.4	29.5	38.8	43.5	44.7
% of revenue	26.3 %	22.6 %	34.9 %	40.9 %	44.6 %
Profit before taxes	27.0	27.7	38.6	43.6	43.7
% of revenue	18.5 %	21.2 %	34.7 %	41.0 %	43.6 %
Result for the period	21.1	22.4	30.2	34.4	34.2
% of revenue	14.4 %	17.2 %	27.2 %	32.4 %	34.2 %
R&D costs	29.3	27.5	16.4	16.9	15.3
% of revenue	20.0 %	21.1 %	14.8 %	15.9 %	15.2%
Capital expenditure	11.1	7.9[1)]	4.6	1.7	1.7
% of revenue	7.6 %	6.1 %	4.2 %	1.6 %	1.7 %
Operating cash flow	38.8	30.1	36.4	36.1	34.5
Net debt (+)/Net cash (-)	163.6	177.4	-19.3	0.2	0.2
Equity ratio %	17.4 %	12.0 %	39.6 %	24.5%	24.5%
Cash conversion	80.5 %	81.2 %	96.2 %	95.6%	89.8%
Wages and salaries	36.1	33.3	20.8	16.1	14.3
Personnel on average	519	484	368[2)]	245[3)]	233[3)]
Personnel on Dec 31	529	524	376	248	243

1) Excluding acquisition

2) Average number of personnel for 2022 represents the average employees after demerger (July-December 2022).

3) For carve-out periods the average number of personnel consists of direct personnel working in the Consumer Security Business.

The key figures are presented combining actuals and carve-out basis for 1-12/2022 and on an actuals basis for financial position at 31 December 2022. For periods 2020-2021 financial information is on carve-out basis.

F-Secure

Key ratios	2024	2023	2022
Earnings / share (EUR)	0.12	0.13	0.17
Earnings / share diluted (EUR)	0.12	0.13	0.17
Shareholders' equity per share (EUR)	0.27	0.19	0.14
Dividend per share (EUR)	0.04[1)]	0.07	0.07[2)]
Dividend per earnings (%)	33.2 %	54.7 %	41.2 %
Effective dividends (%)	2.2 %	3.4 %	2.5 %
P/E ratio	22.9	27.7	16.4
Share price, lowest (EUR)	1.67	1.64	2.29
Share price, highest (EUR)	2.33	3.44	3.26
Share price, average (EUR)	1.95	2.35	2.68
Share price Dec 31	1.78	2.04	2.83
Market capitalization (MEUR)	311.6	355.5	494.0
Trading volume (millions)	44.8	39.0	15.8
Adjusted number of shares			
average during the period	174,673,165	174,647,528	174,526,944
average during the period, diluted	174,924,124	174,526,944	174,526,944
Dec 31	174,673,165	174,673,165	174,526,944
Dec 31, diluted	175,243,726	174,526,944	174,526,944

1) Board proposal for 2024.

2) For 2022 dividend distribution was based on July-December 2022 net profit and 78% from July-December earnings.

Reconciliation between adjusted EBITDA, EBITDA, adjusted EBITA, EBITA and EBIT

EUR 1,000	2024	2023
Adjusted EBITDA	**53,480**	**45,651**
Adjustments to EBITDA		
Costs related to acquisition		-6,150
Costs related to restructuring	-1,438	-1,805
EBITDA	**52,042**	**37,696**
Depreciation and amortization	-13,621	-8,199
EBIT	**38,422**	**29,497**
Adjusted EBITA	**52,248**	**44,575**
Adjustments to EBITA		
Costs related to acquisition		-6,150
Costs related to restructuring	-1,438	-1,805
EBITA	**50,810**	**36,620**
Amortization	-4,573	-2,465
PPA amortization	-7,816	-4,658
EBIT	**38,422**	**29,497**

Calculation of key figures

Key figure	Definition	
EBITDA	EBIT + Depreciation, amortisation and impairment	
EBITA	EBIT + Amortisation and impairment	
EBIT	Result before taxes and net financial items	
Adjusted EBITDA	EBITDA before items affecting comparability	
Adjusted EBITA	EBITA before items affecting comparability	
Items affecting comparability	Items affecting comparability are associated with restructuring, acquisition and cost related to listing	
Operating expenses	Sales and marketing, research and development, and administration expenses	
Capital expenditure	Corresponds to the Statement of Cash Flow line item Investments in intangible and tangible assets	
Operating cash flow	Corresponds to the Statement of Cash Flow line item Cash flow from operations	
Net debt (+) / Net cash (–)	Interest-bearing liabilities – Interest-bearing receivables – Cash and cash equivalents	
Equity ratio, %	Total equity / Total assets	× 100

Key figure	Definition	
Cash conversion, %	(Adjusted EBITDA – Capital expenditure –/+ Change in net working capital) / Adjusted EBITDA	× 100
Earnings per share, EUR	Profit attributable to equity holders of the company / Weighted average number of outstanding shares	
Earnings per share, excluding PPA, EUR	(Profit attributable to equity holders of the company + PPA amortization adjusted by tax impact) / Weighted average number of outstanding shares	
Shareholders' equity per share, EUR	Equity attributable to equity holders of the company / Number of outstanding shares at the end of period	
P/E ratio	Closing price of the share (at period end) / Earnings per share (annualized)	
Gearing, %	(Interest-bearing liabilities – cash and bank) / Total equity	× 100

Shares and Shareholders

Shares and share ownership distribution, 31 Dec 2024

Shares	Number of shareholders	% of shareholders	Total shares	% of shares
1-100	10,818	31.89%	470,096	0.27%
101-1 000	17,546	51.73%	6,706,311	3.84%
1001-50 000	5,464	16.11%	21,028,823	12.04%
50 001-100 000	37	0.11%	2,588,592	1.48%
100 001-	56	0.17%	143,879,343	82.37%
Total	**33,921**	**100.00%**	**174,673,165**	**100.00%**

Shareholders by category, 31 Dec 2024	Total shares	% of shares
Private individuals	87,713,004	50.22%
Pension & Insurance companies	26,876,763	15.39%
Fund companies	19,004,379	10.88%
Companies	8,583,169	4.91%
Foundations	1,734,992	0.99%
Nominee registered	16,843,908	9.64%
Others	13,916,950	7.97%
Total	**174,673,165**	**100.00%**

Largest shareholders and administrative register

Owner	Shares	% of shares	% of votes
Risto Siilasmaa	60,035,288	34.37%	34.37%
Nordea Nordic Small Cap Fund	11,582,976	6.63%	6.63%
Ilmarinen Mutual Pension Insurance Company	6,273,663	3.59%	3.59%
Elo Mutual Pension Insurance Company	4,353,000	2.49%	2.49%
Mandatum Life Insurance Company Ltd	4,341,986	2.49%	2.49%
Danske Invest Finnish Equity Fund	4,236,558	2.43%	2.43%
Varma Mutual Pension Insurance Company	3,970,660	2.27%	2.27%
The State Pension Fund of Finland	3,900,000	2.23%	2.23%
Säästöpankki Kotimaa investment fund	2,612,499	1.50%	1.50%
Investment fund Aktia Capital	2,565,164	1.47%	1.47%

Administrative register	Shares	% of shares	% of votes
Skandinaviska Enskilda Banken	11,520,490	6.60%	6.60%
Citibank Europe Plc	4,282,072	2.45%	2.45%
Other registers	1,041,346	0.60%	0.60%
Other shareholders	157,829,257	90.36%	90.36%
Total	**174,673,165**	**100.00%**	**100.00%**
Own shares F-Secure Corporation			
Total	**174,673,165**	**100.00%**	

Ownership of management

Board of Directors	Shares	% of shares
Risto Siilasmaa	60,035,288	34.37%
Pertti Ervi	120,103	0.07%
Petra Teräsaho	22,640	0.01%
Thomas Jul	17,923	0.01%
Tommi Uitto	8,431	0.00%
Katja Kuusikumpu	7,626	0.00%
Total	**60,212,011**	**34.47%**

Leadership team	Shares	% of shares
Antero Norkio	69,392	0.04%
Timo Laaksonen	38,282	0.02%
Toby White	32,085	0.02%
Sari Somerkallio	15,481	0.01%
Richard Larcombe	12,079	0.01%
Viswanathan Tirunillai	3,394	0.00%
Nina Lehto		
Bruno Rodriguez		
Kaisa Tikka-Mustonen		
Total	**170,713**	**0.10%**

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 Personal 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.

Board of Directors

- Reviews and approves the company's strategy, business model and related targets, which include ESG.
- ESG progress and achievements reported to the Board annually.
- The Board reviews remuneration policies aligned to ESG requirements.

Audit committee

- Review related strategy and activities
- Review sustainability related policies including ESG reporting, Corporate Governance, Cyber Security, and Risk Management
- Other duties assigned to AC under applicable law relating to sustainability reporting

Leadership Team

- Responsible for establishing and reviewing company ESG strategy and business model
- Ensures that ESG is part of company culture and approves policies and principles
- Risk Management review conducted minimum twice a year
- Reviews annual sustainability statement, targets and metrics

F-Secure ESG Council

- Identify and assess ESG impacts, risks and opportunity
- Develop and implement ESG strategies and preparation of annual sustainability statement
- Propose targets and metrics, and develop policies & principles
- Drives ESG compliance, and provides views on certifications and standards
- Ensures required stakeholder engagement in matters related to ESG

ESG Function
Leading ESG Council and facilitating ESG strategy execution and reporting. Together with Legal function ensures ESG activities meet regulative requirements.

General Counsel
Align ESG governance with the overall corporate governance and Code of Conduct and other relevant policies.

ESG Committee

DEI
Reviews and sets ambition on DEI related plans. Evaluates and provides feedback on progress.

Culture, Health & Wellbeing[1]
Reviews and sets ambition on H&W related plans. Evaluates and provides feedback on progress.

Environment
Driving environmental initiatives and climate change related targets.

Topics covered by ESG council

Donations & Sponsorship
Reviews and set principles for allocations of corporate donations and sponsorship.

Customers and end-users
Reviews and sets ambition on stakeholder ESG. Specific task force appointed.

Business conduct
Ensure that ESG governance is aligned with the overall corporate governance and Code of Conduct.

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 renumeration 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' renumeration 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 regual occurance 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.

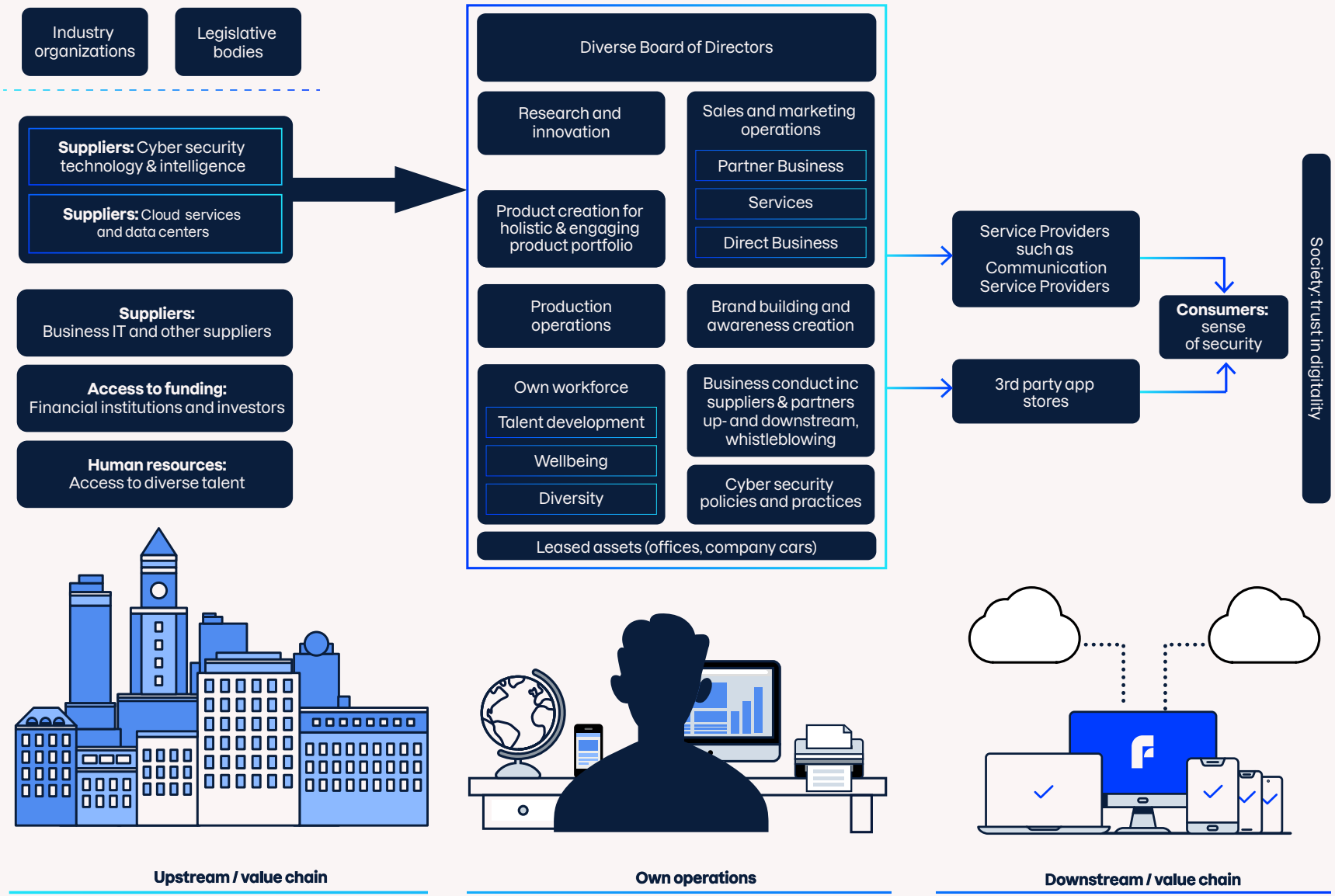
Furthermore, to realize our purpose of making every digital moment more secure for everyone, our go-to-market model is primarily channel-based and through Service Providers allows us to reach hundreds of millions of consumers behind these partners in our focus regions in Europe, North America and APAC/Japan. 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-Scure'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 oppositive 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
Climate change	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 toF-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

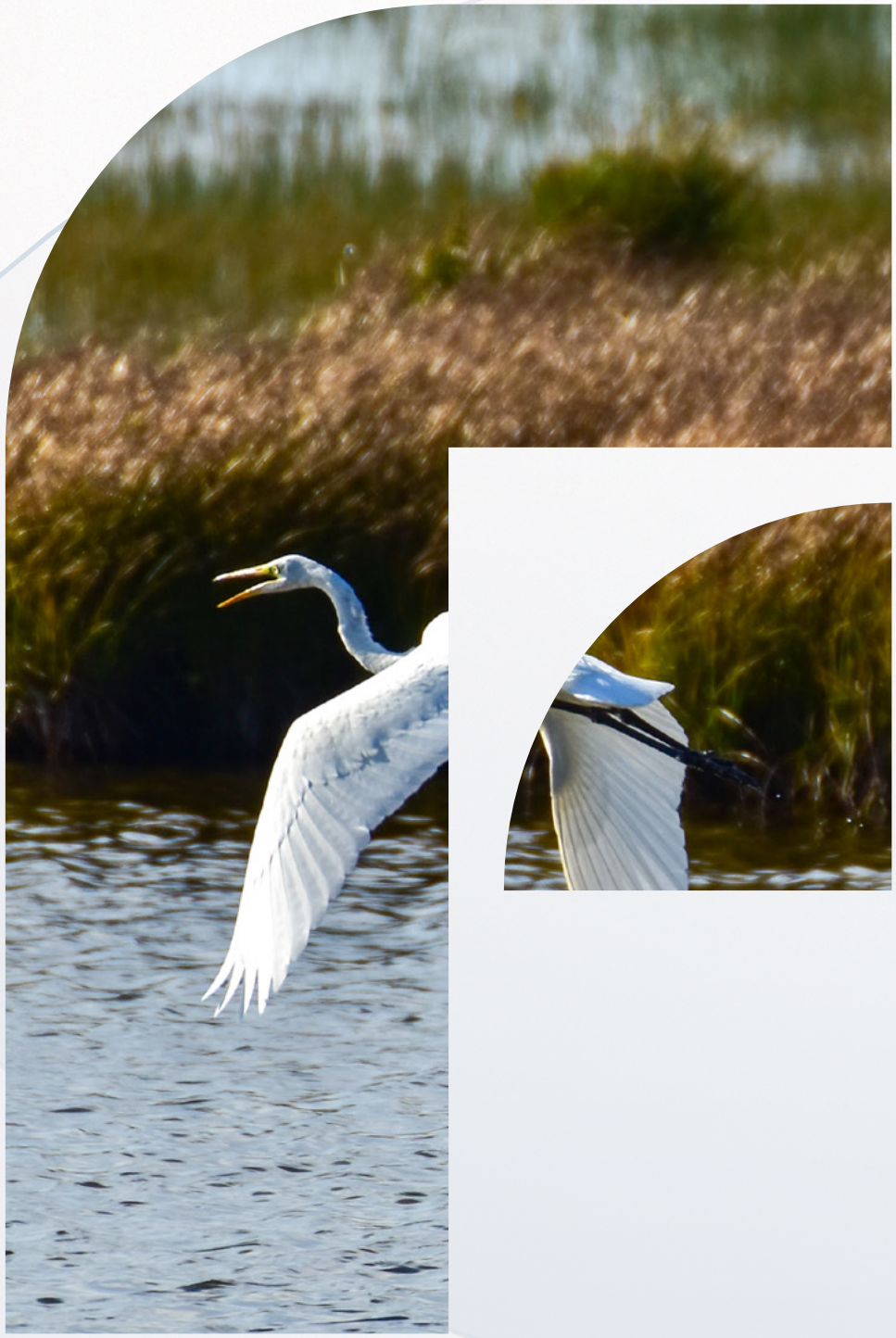
Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS S1-14 Number of days lost to injuries, accidents, fatalities or illness paragraph 88 (e)	Indicator number 3 Table #3 of Annex I				Omitted 2024
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 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																			
A.1 Environmentally sustainable activities (Taxonomy-aligned)																			
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 %	0.0 %								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																			
A.1 Environmentally sustainable activities (Taxonomy-aligned)																			
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**																			
A.1	**Environmentally sustainable activities (Taxonomy-aligned)**																			
CapEx 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%		
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 %	0.0 %								0%		
A.	CapEx of Taxonomy-eligible activities (A.1 + A.2)		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								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.

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 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

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

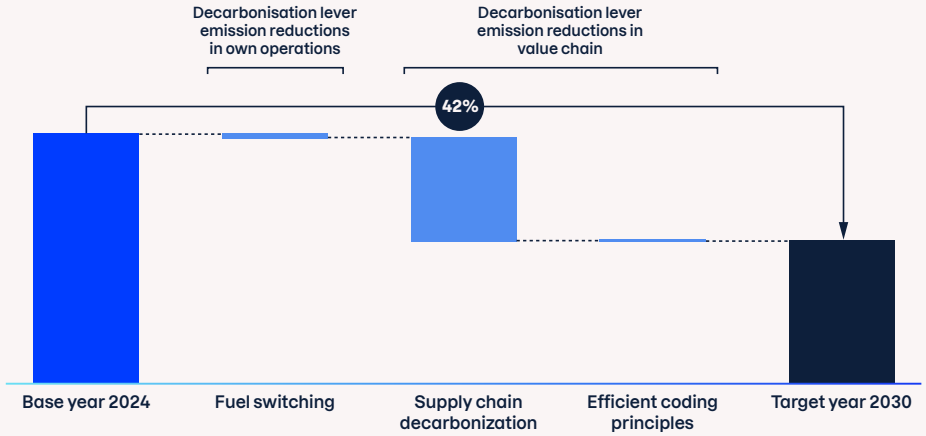
F-Secure has established GHG emission reduction targets that are compatible with limiting global warming to 1.5°C. Therefore, F-Secure aims to decrease emissions in Scope 1&2 and in Scope 3 by 42% by 2030. This means that in 2030 Scope 1&2 emissions aim to be 127 tons of CO2e and Scope 3 emissions aim 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 coverd 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 (tCO2eq)	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 (tCO2eq)	233	-	233	-	-	-	-	-
Gross market-based Scope 2 GHG emissions (tCO2eq)	189	-	189	-	-	110[1]	-	8.70%[2]
Scope 3 GHG emissions								
Total Gross indirect (Scope 3) GHG emissions (tCO2eq)	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) (tCO2eq)	8594	-	8594	-	-	-	-	-
Total GHG emissions (market-based) (tCO2eq)	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 (tCO2eq/MEUR)	58.76
Total GHG emissions (market-based) per net revenue in millions (tCO2eq/MEUR)	58.46
Net revenue used to calculate GHG intensity	
Total net revenue (in financial statements) MEUR	146.3

Table 20. GHG intencity per net revenue.

Sustainability Statement -

Social



S1 – Own workforce

SBM-3 Material impacts, risks and opportunitites

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 educates 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 commited to adhereing 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 safetymanagement 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%
The percentage of entitled employees that took family related leaves disaggregated by gender	Male: 3.2% 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 if 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.

Consolidated financial statements

Statement of comprehensive income

EUR 1,000	Note	2024	2023
Revenue	(3)	146,258	130,371
Cost of revenue		-20,243	-11,814[1]
Gross Margin		**126,015**	**118,557**
Other operating income	(4)	751	830
Sales and marketing	(5,6,7)	-34,591	-36,996[1]
Research and development	(5,6,7)	-29,275	-27,496[1]
Administration[2]	(5,6,7)	-24,478	-25,398
EBIT		**38,422**	**29,497**
Financial income	(9)	1,714	6,995
Financial expenses	(9)	-13,124	-8,815
Profit before taxes		**27,011**	**27,677**
Income tax	(10)	-5,944	-5,316
Result for the financial year		**21,067**	**22,360**
Other comprehensive income			
Exchange difference on translation of foreign operations		4,047	-1,990
Comprehensive income for the year		**25,114**	**20,370**
Result of the financial year is attributable to:			
Equity holders of the parent		21,067	22,360
Comprehensive income for the year is attributable to:			
Equity holders of the parent		25,114	20,370
Earnings per share, eur (basic and diluted)[3]	(11)	0.12	0.13

1) F-Secure changed the calculation method for gross margin in its income statement. Some of the costs previously recorded in F-Secure income statement as Cost of revenue have been included in Research and development and Sales and marketing costs.

2) Costs related to restructuring increase administration expense by EUR 1.4 million in 2024 (EUR 1.8 million). In addition, costs related to acquisition increase administration expense by EUR 6.2 million in 2023.

3) Earnings per share is based on the average number of shares.

Statement of financial position

EUR 1,000	Note	2024	2023
ASSETS			
Non-Current Assets			
Tangible assets	(14)	326	360
Right-of-use assets	(5,14)	1,200	1,257
Intangible assets	(14)	125,736	125,179
Goodwill	(13,14)	89,783	88,361
Deferred tax assets	(22)	58	883
Interest-bearing receivables, non-current	(16,21)	-	3,658
Other non-current receivables	(17)	223	-
Total non-current assets		**217,327**	**219,698**
Current Assets			
Inventories	(15)	29	35
Accrued income	(17)	3,333	1,953
Trade and other receivables	(16,17,21)	37,049	35,604
Interest-bearing receivables, current	(16,21)	3,757	-
Income tax receivables	(17)	968	2,108
Cash and cash equivalents	(16,21)	8,095	15,867
Total current assets		**53,231**	**55,568**
TOTAL ASSETS		**270,558**	**275,266**

EUR 1,000	Note	2024	2023
EQUITY AND LIABILITIES			
Shareholder's Equity	(18)		
Share capital		80	80
Translation differences		1,977	-2,070
Unrestricted equity reserve		9,590	9,590
Retained earnings		35,371	25,485
Equity attributable to equity holders of the parent		**47,018**	**33,086**
Non-Current Liabilities			
Interest bearing liabilities, non-current	(5,20,21)	131,431	165,963
Deferred tax liabilities	(22)	3,584	2,064
Other non-current liabilities	(23)	6,443	5,888
Total non-current liabilities		**141,459**	**173,915**
Current Liabilties			
Interest bearing liabilities, current	(5,20,21)	44,046	30,965
Trade and other payables	(21,23)	14,142	14,182
Provisions	(23)	1,427	1,739
Income tax liabilities	(23)	387	1,592
Other current liabilities	(23)	22,079	19,788
Total current liabilities		**82,081**	**68,265**
TOTAL EQUITY AND LIABILITIES		**270,558**	**275,266**

Statement of cash flows

EUR 1,000	Note	2024	2023
Cash flow from operations			
Result for the financial year		21,067	22,360
Adjustments			
Depreciation and amortization	(6)	13,621	8,199
Provisions	(23)	-312	-
Share-based payments	(19)	1,045	619
Other adjustments		177	-22
Financial income and expenses	(9)	11,324	1,759
Income taxes	(10)	5,944	5,316
Cash flow from operations before change in working capital		**52,866**	**38,232**
Change in net working capital			
Current receivables, increase (-), decrease (+)	(16)	-2,812	-8,092
Inventories, increase (-), decrease (+)	(15)	6	6
Non-interest bearing debt, increase (+), decrease (-)	(23)	3,812	7,425
Cash flow from operations before financial items and taxes		**53,872**	**37,571**
Interest expenses paid	(9)	-11,283	-7,178
Interest income received	(9)	838	739
Other financial income and expenses	(9)	-945	4,476
Income taxes paid	(10)	-3,664	-5,499
Cash flow from operations		**38,817**	**30,109**

EUR 1,000	Note	2024	2023
Cash flow from investments			
Investments in intangible and tangible assets	(14)	-11,109	-7,920
Proceeds from sale of intangible and tangible assets		1	0
Acquisition of subsidiaries, net of cash acquired	(12)	-132	-207,764
Cash flow from investments		**-11,240**	**-215,684**
Cash flow from financing activities			
Increase in interest bearing liabilities, non-current	(20)	-	202,000
Repayments of lease liabilities	(5)	-1,174	-1,070
Repayments of interest-bearing liabilities, non-current	(20)	-30,000	-10,000
Change of short-term interest-bearing liabilities	(20)	8,000	-
Dividends paid		-12,227	-12,227
Cash flow from financing activities		**-35,401**	**178,703**
Change in cash		-7,824	-6,872
Cash and bank at the beginning of the period	(21)	15,867	22,953
Effects of exchange rate changes		52	-214
Cash and bank at period end		**8,095**	**15,867**

Statement of changes in equity

Attributable to the owners of F-Secure

EUR 1,000	Note	Share capital	Unrestricted equity reserve	Retained earnings	Translation differences	Total
Equity 31 December 2022		**80**	**9,590**	**15,213**	**-79**	**24,804**
Result of the financial year		-	-	22,360	-	22,360
Translation difference		-	-	-	-1,990	-1,990
Total comprehensive income for the year		-	-	**22,360**	**-1,990**	**20,370**
Transactions with owners in their capacity as owners						
Cost of share-based payments	(19)	-	-	139	-	139
Dividend		-	-	-12,227	-	-12,227
Equity 31 December 2023		**80**	**9,590**	**25,485**	**-2,070**	**33,086**
Result of the financial year		-	-	21,067	-	21,067
Translation difference		-	-	-	4,047	4,047
Total comprehensive income for the year		-	-	**21,067**	**4,047**	**25,114**
Transactions with owners in their capacity as owners						
Cost of share-based payments	(19)	-	-	1,045	-	1,045
Dividend		-	-	-12,227	-	-12,227
Equity 31 December 2024		**80**	**9,590**	**35,371**	**1,977**	**47,018**

1. Basis of preparation and accounting principles

1.1 Basis of preparation

Background

F-Secure is a Finnish, globally operating cybersecurity company. The parent company of the Group is F-Secure Corporation incorporated in Finland and domiciled in Helsinki, Finland. The company's registered address is Tammasaarenkatu 7, 00180 Helsinki. F-Secure operates globally with presence in multiple locations, and its headquarters is located in Helsinki.

F-Secure Corporation formed a separate legal group ("F-Secure", the "Group") as of 30 June 2022 when all assets and liabilities of the Consumer Security Business were transferred from WithSecure Corporation ("WithSecure") to a company incorporated in connection with the partial demerger ("Demerger") and named F-Secure Corporation ("F-Secure"). The trading in F-Secure's shares on Nasdaq Helsinki began 1 July 2022.

A copy of consolidated financial statements can be downloaded on www.f-secure.com or can be received from the parent company's registered address. These financial statements were authorized for issue by the Board of Directors on 25 February 2025.

F-Secure business

F-Secure designs and offers security and privacy products and services that help millions of consumers to protect themselves against online threats. F-Secure's offering includes a comprehensive range of security and privacy products and services related to endpoint security, privacy protection, password management and digital identity protection, and router security that protects consumers' entire connected home. The majority of F-Secure's sales come from selling products and services through its extensive and global Channel Partner network, including approximately 200 Channel Partners. Channel Partners include, for example, communication service providers, retailers, banks, and insurance companies. In addition to selling products through Channel Partners, F-Secure makes standalone and all-in-one security offerings available to consumers through various e-commerce channels such as mobile application stores and its own online store.

Basis of preparation for the consolidated financial statements

The consolidated financial statements for the year ended 31 December 2024 have been prepared for the purpose of presenting the financial position, results of operations and cash flows of F-Secure on a consolidated basis. The consolidated financial statements of F-Secure Corporation of 2024 have been prepared in accordance with IFRS Accounting Standards, applying the IAS and IFRS accounting standards as well as SIC and IFRIC interpretations that were in force and had been approved by the EU by 31 December 2024. In addition, accounting and limited liability company legislation and official regulations of Finland have been considered in the preparation of the consolidated financial statements.

F-Secure also publishes its financial statements in XHTML format in accordance with the European Single Electronic Format (ESEF) reporting requirements. In line with the ESEF requirements, the primary financial statements have been labelled with XBRL tags. Notes to financial statements have been labelled with XBRL block tags. The ESEF reporting has been subject to audit.

The consolidated financial statements have been prepared on a going concern basis and management has not recognized any material uncertainties related to continuity of operations.

The financial information is presented in thousands of euros unless otherwise stated. All figures have been rounded which may cause the sum of individual figures to deviate from the sum of the presented line-item totals.

1.2 Accounting principles

Accounting principles applied in F-Secure's financial statements.

Change in calculation method for gross margin in income statement

F-Secure has changed the calculation method for gross margin in its income statement. Some of the costs previously recorded in F-Secure income statement as cost of revenue have been included in research and development and sales and marketing costs. Prior year financials have been revised.

Previously, development related hosting costs, customer support and delivery costs have been reported as part of cost of revenue above the gross margin in the income statement. According to the new calculation method the gross margin for 2023 was 90.9% (reported 87.7%). Following the reclassification, in the comparison period income

statement EUR 2.3 million transferred from cost of revenue to sales and marketing costs, and EUR 1.9 million to research and development costs. The change in the calculation method did not impact F-Secure's revenue or earnings (EBITA, EBIT).

The change in the calculation method aimed at identifying costs directly linked to production costs of F-Secure's software products and services. In previous reporting, F-Secure's cost of revenue also included development related hosting costs, as well as customer support and delivery costs which are fixed costs in nature or not variable related to changes in revenue. In the revised model customer support and delivery are presented under sales and marketing costs whereas development related hosting is presented under research and development. The revised gross margin captures costs related directly to production which are variable based on company's revenue. These are mainly production related hosting and royalty costs as well as some merchandise costs.

Management judgment on significant accounting principles and use of estimates

The preparation of consolidated financial statements requires use of estimates and assumptions as well as use of judgment when applying accounting principles. These affect the contents of the financial statements, and it is possible that actual results may differ from estimates.

Estimates made in connection with preparation of financial statements are based on management's best knowledge at the reporting date. Estimates build upon past experience as well as assumptions of future development of economic environment of the Group. Revisions in estimates and assumptions are recognized in the period they occur and in future periods if the revision affects both current and future periods.

The following areas require significant judgement and estimation:

- Business combinations: Net assets acquired through business combinations are measured at fair value. The measurement of fair value is based on valuation methods which are subject to management judgment (See Note 12 Acquisitions).
- Impairment testing: Recoverable amount of goodwill from acquisitions is based on present value of estimated future cash flows which are subject to management judgment. In addition to goodwill the intangible assets that are not yet ready for use are tested annually for impairment. The recoverable amount of these assets is based on estimated future cash flows from sales and/or use of the asset.
- Expected credit losses: The allowance for expected credit losses in F-Secure's statement of financial position is EUR 687 thousand as at 31 December 2024 (See Note 16 Financial assets).
- Share-based payments: The Group's share-based incentives programs are mainly tied to market-based conditions. Management uses external valuations in determining the fair value of the shares granted under these incentive programs. The method for the valuation is either Monte Carlo Simulation or Cox, Ross & Rubenstein method.
- Provisions: The amount of provision is the best estimate of the cost required to settle the obligation at the reporting date. Provisions are reviewed on a regular basis and adjusted when necessary.

	Reported	Revised
EUR 1,000	**1-12/2023**	**1-12/2023**
Revenue	130,371	130,371
Cost of revenue	-16,025	-11,814
Gross margin	**114,346**	**118,557**
Other operating income	830	830
Sales and marketing	-34,698	-36,996
Research and development	-25,583	-27,496
Administration	-25,398	-25,398
EBIT	**29,497**	**29,497**
Financial income	6,995	6,995
Financial expenses	-8,815	-8,815
Profit before taxes	**27,677**	**27,677**
Income tax	-5,316	-5,316
Result for the period	**22,360**	**22,360**
Other comprehensive income		
Items that may be reclassified to profit or loss:		
Exchange difference on translation of foreign operations	-1,990	-1,990
Comprehensive income for the period	**20,370**	**20,370**

Consolidation principles

The consolidated financial statements incorporate the financial statements of F-Secure Corporation and entities controlled by F-Secure Corporation. Consolidation is done using the acquisition method and begins when control over the subsidiary is obtained. The consolidation stops when the control ceases. The Group does not have any associated companies nor is there any non-controlling interest in the Group.

All intra-group transactions and balances, including unrealized profits arising from intra-group transactions, have been eliminated on consolidation. Where necessary, accounting policies of the subsidiaries have been adjusted to ensure consistency with the policies adopted by the Group.

Transactions in foreign currency

The financial statements are presented in euros, which is the functional and presentation currency of F-Secure's parent company. At each reporting date for the purpose of presenting financial statements, the income statements of foreign Group companies are translated at the average exchange rates for the reporting period and the balance sheets are translated using the European Central Bank's exchange rates prevailing on the reporting date. Foreign currency transactions are translated using the exchange rates prevailing at the dates of the transactions. Exchange rate gains and losses are recognized in financial items in the statement of comprehensive income.

Revenue recognition

F-Secure provides a comprehensive range of cybersecurity products related to endpoint protection, privacy protection, digital identity protection and security for all consumers' connected devices at home. Revenue derives from the sale of security products through partner and direct (ecommerce) channels. Majority of revenue comes from the sale of cyber security products through the partner channel. F-Secure also sells consumer products through various retail partners, as well as F-Secure's own web shop. Partner channel sells F-Secure Total and Embedded Security products whereas direct channel sells F-Secure Total products.

F-Secure's cybersecurity products are sold as Security-as-a-Service. Customers are granted access to use the intellectual property during the license period and they are provided with access to continuously updated software. All software and the accompanied services F-Secure provides are highly interdependent and therefore treated as one performance obligation for which revenue is recognized over time on a straight-line basis for license period despite the sales channel.

Partner channel customers can have different invoicing depending on the customer agreement. Majority of the agreements are licenses fees – either F-Secure Total or Embedded Security – which are provided as a continuous service, when they are invoiced and revenue is recognized each month. Some agreements are for a fixed term, when they are invoiced e.g. annually upfront and revenue is recognized over time. Non-recurring revenue, which e.g. relates to custom built integration, is usually invoiced in the beginning of the agreement period and revenue is recognized over time on a straight-line basis for the contract period.

Direct channel selling F-Secure Total is usually invoiced fully upfront for the license period and the revenue is recognized over time on a straight-line basis for the license period. The typical length of a license period is 12, 24, or 36 months.

Generally, the term between invoicing and when payment is due is not significant.

Pensions

All of F-Secure's pension arrangements are defined contribution plans. Contributions to defined contribution plans are recognized in the statement of comprehensive income in the period to which the contributions relate.

Leases

Leases are recorded in the balance sheet as right-of-use asset with a corresponding lease liability. Right-of-use assets and lease liabilities are initially measured at the present value of the remaining lease payments. An incremental borrowing rate is applied in discounting the remaining payments. F-Secure's incremental borrowing rate varies between 2.45% and 6.9% depending on geographical location of the leased asset and lease period, and the rate of 5.9% applies to the majority of the right-of-use assets.

F-Secure's right-of-use assets are comprised of leased offices and cars. In the second quarter of 2024, F-Secure signed a new lease agreement for headquarter office premises. This will be recorded in the balance sheet as right-of-use asset and lease liability during summer 2025 when the lease term starts, but the lease commitment already exists following the agreement.

Changes in estimates are accounted for at each reporting date. In measuring the present value of the liabilities arising from leases, any service-related fees are excluded from the lease payment. F-Secure's lease contracts do not contain residual value guarantees or purchase options. The estimated duration for on-going contracts varies between 1 to 3 years and the total liability from on-going contracts is EUR 1,210 thousand

(EUR 1,263 thousand) (see Note 5 Leases and Note 20 Financial liabilities).

Income taxes

The income tax expense in statement of comprehensive income represents the sum of current taxes and deferred taxes. Current taxes are calculated on the taxable income for all Group companies in accordance with the local tax rules. Deferred taxes, resulting from temporary differences between the financial statement and the income tax basis of assets and liabilities, use the enacted tax rates in effect in the years in which the differences are expected to reverse. Deferred tax assets are recognized to the extent that it is probable that future taxable profit will be available. Deferred tax liabilities are recognized for all temporary differences.

Deferred tax assets and liabilities are offset when there is a legally enforceable right to set off current tax assets against current tax liabilities and when they relate to the same taxation authority and the Group intends to settle the assets and liabilities on a net basis.

Business combinations

Acquisition method is used for accounting the acquisition of businesses. The consideration transferred in a business combination is measured at fair value, which is calculated as the sum of the acquisition date fair values of assets transferred by the Group and liabilities incurred by the Group to the former owners of the acquiree. Costs related to the acquisition are recognized in profit and loss statement.

The identifiable assets acquired and the liabilities assumed are recognized at fair value at the acquisition date except for deferred tax assets or liabilities which are measured in accordance with IAS 12 Income taxes.

Goodwill is measured as the excess of the transferred consideration over the net amount of the acquired identifiable assets and assumed liabilities.

Goodwill

Goodwill is initially recognized and measured in business combinations as set out above. Goodwill is not amortized but is instead tested for impairment at least annually and whenever there is an indication that it may be impaired. For the purpose of impairment testing goodwill has been allocated to cash generating unit (CGU) expected to benefit from the synergies of the combination. If the recoverable amount of the cash generating unit is less than the carrying amount of the unit, the impairment loss is allocated first to reduce the carrying amount of any goodwill allocated to the unit and then to the other assets of the unit. If an impairment loss for goodwill is recognized it will not be reversed in the subsequent periods. Goodwill is recorded at historical cost less accumulated impairment losses. F-Secure has only one CGU which consists of F-Secure's total business and the carrying amount of goodwill is allocated to this CGU.

Intangible assets

Research and development expenditure

Research expenditure is recognized as an expense at the time it is incurred. Development expenditure on new products or product versions with significant new features are recognized as intangible assets when F-Secure has the technical feasibility to complete the asset, has the ability and intention to use or sell the asset; can demonstrate that the asset will generate future economic benefits; has resources available to complete the asset; and has the ability to measure reliably the expenditure during development.

Development assets relate to developing new products and services or developing essential improvements for products and services. Amortization is recorded once the asset is ready on a straight-line basis over the estimated useful life, which is 3-5 years for these assets. These assets are reported either under Capitalized development or under Advance payments & incomplete development in Note 14 Non-current assets.

Intangible assets acquired in business combinations

Intangible assets acquired in business combinations and recognized separately from goodwill are initially recognized at fair value on the acquisition date. Subsequent to initial recognition these assets are reported at initial value less accumulated amortization and accumulated impairment losses. Intangible assets acquired in business combinations include technology and customer relationships, which all have a finite useful life. These assets are reported under Intellectual property (see Note 14 Non-current assets) The estimated useful lives for intangible assets acquired in business combinations are:

Technology 15 years

Customer relationships 5–15 years

Other intangible assets

Other intangible assets include intangible rights and software licenses, all with a finite useful life. Other intangible assets include also partially or completely internally developed intangible assets which e.g. relate to platforms. Other intangible assets are recorded at historical cost less accumulated amortization and possible impairment. Amortization is recorded on a straight-line basis over the estimated useful life, which is 3–5 years for these assets.

Tangible assets

Tangible assets are recorded at historical cost less accumulated depreciation and possible impairment. Depreciation is recorded on a straight-line basis over the estimated useful life of an asset. The estimated useful lives of tangible assets are as follows:

Machinery and equipment 2–8 years

Other tangible assets 2 years

Impairment of assets

At each reporting date, or more frequently if needed, F-Secure assesses whether there is any indication that an asset may be impaired. Where an indicator of impairment exists, F-Secure makes a formal estimate of the recoverable amount. The recoverable amount of goodwill and intangible assets that are not ready for use are estimated annually regardless of whether any indication of impairment exists. The intangible assets that are not ready for use are software projects which cannot be assessed on its own because they don't have independent cash flow. If it is stated at the end of reporting period that the projects are finalized and will be taken in use, there is no need for impairment testing. Intangible assets that are not ready for use are tested as part of F-Secure's single cash generating unit. Where the carrying amount of an asset exceeds its recoverable amount, the asset is considered impaired and the carrying amount is reduced to its recoverable amount. The recoverable amount is the fair value of an asset less costs of disposal or value in use, whichever is higher. An impairment loss is recorded in the statement of comprehensive income.

A previously recognized impairment loss is reversed only if there has been a change in the estimates used to determine the asset's recoverable amount since the last impairment loss was recognized. The maximum reversal of an impairment loss amounts to no more than the carrying amount of the asset if no impairment loss had been recognized, net of depreciation.

Inventories

Inventories are measured at the lower of cost and net realizable value. Cost is determined by the first-in first-out method. Net realizable value is the estimated selling price that is obtainable, less estimated costs of completion and the estimated costs necessary to make the sale.

Financial instruments

Financial instruments are originally measured at fair value. Subsequentially, financial assets are classified into the following categories: at amortized cost or fair value through profit and loss. The classification is made at the time of acquisition and is based on the cash flow characteristics and the business model of managing the financial asset. Financial liabilities are subsequentially classified and recognized at amortized cost or at fair value through profit and loss.

Financial instruments measured at fair value through profit and loss include derivative instruments to which hedge accounting is not applied. Realized and unrealized gains or losses arising from changes in fair values are recognized in the profit and loss in the period in which they incur.

According to F-Secure's treasury policy, company may enter derivative contracts to hedge against exchange rates and interest rates fluctuations. Company has no outstanding derivative contracts on the reporting date 31.12.2024.

Financial instruments are classified as current financial instruments unless the maturity exceed 12 months from the end of the reporting period.

Financial assets

Cash and cash equivalents, interest-bearing receivables and trade receivables are considered as financial assets. Financial assets are originally measured at fair value. Cash and cash equivalents in the balance sheet comprise cash at bank, deposits held at bank, and other highly liquid short-term investment with original maturity less than 3 months. Interest-bearing receivables are measured at amortized cost.

Trade receivables are originally measured with transaction price and later with amortized cost reduced by an expected credit loss for trade receivables. Trade receivables and other receivables are written off from the balance sheet as the rights to associated cash flows end or become transferred to the counterparty. An expected credit loss is recognized for trade receivables according to IFRS 9, Financial Instruments. The amount of expected credit loss is updated at each reporting date to reflect changes in credit risk since initial recognition of the respective financial instrument. The expected credit loss is estimated using a provision matrix where trade receivables are grouped based on historical credit loss experience and characteristics that depict the credit risk of receivables (e.g. geographical area and days past due).

Financial liabilities

F-Secure classifies bank loans, trade payables, lease liabilities and other interest-bearing liabilities as financial liabilities. Bank loans are initially recognized at the fair value of consideration plus directly attributable transaction costs. After initial recognition, bank loans are measured at amortized cost using the effective interest method. Other financial liabilities are measured at amortized cost.

Provisions

Provisions are recognized when F-Secure has a present obligation (legal or constructive) as a result of a past event, the outflow of resources is probable, and a reliable estimate of the amount of the obligation can be made. The amount recognized is a best estimate of the consideration required to settle the obligation at each reporting date. Risks and uncertainties are taken into account when making the estimate.

Management has recognized a provision of EUR 1,427 thousand (EUR 1,539 thousand) related to restructuring as at 31 December 2024. Comparison period had also a EUR 200 thousand provision related to other provisional costs and expenses. See Note 23 Other liabilities.

Share-based payment transactions

F-Secure provides incentives to employees in the form of equity-settled share-based instruments. F-Secure's share-based incentive programs are targeted to F-Secure's key personnel. The programs are equity-settled. Equity-settled program is valued at fair value at grant date, and the expense is recognized evenly in the statement of comprehensive income over the vesting period with the counter-entry in retained earnings. In programs with market based conditions, the fair value is determined by utilizing commonly used valuation techniques. If a person leaves the company before vesting, the reward is forfeited. F-Secure updates its estimate of the ultimate number of shares at each reporting date. These changes in the estimate are recorded in the statement of comprehensive income.

Presentation of expenses

Classification of expenses by function has been made by presenting direct expenses in their respective functions.

Operating result

IAS 1, Presentation of Financial Statements, does not define the concept of Earnings before interest and taxes (EBIT). F-Secure has defined it as follows: EBIT is the net amount, which consists of revenue and other operating income less cost of revenue, personnel costs, depreciation and amortization, possible impairment losses, and other operating expenses.

New standards and interpretations not yet effective

New or amended standards or interpretations are not expected to have an impact on the financial statements.

Effective 1 January 2027:

IFRS18 Presentation and disclosure in Financial Statements standard will impact presentation and disclosure in financial statements. The structure of the statement of profit or loss will change and at the same time certain related measures, i.e. management-defined performance measures, that are reported outside an entity's financial statements are required. Company is following IFRS18 accounting standard impact on the financial statements. The effects of the new standard are not yet reviewed.

2. Segment information

F-Secure's operations and profitability is reported as a single operating segment which is consistent with the internal reporting and the way that operative decisions and assessment of performance have been made by F-Secure's leadership team. Consumer Security Business consists of designing and providing a comprehensive range of cybersecurity products and services related to data security, privacy protection as well as privacy protection and digital identity protection of consumers' terminal devices, networks and devices connected to a network, sold, in each case, either directly or indirectly, to consumers.

Geographical information

Geographical information about revenue is presented in Note 3 Revenue .

EUR 1,000	2024	2023
Long-term assets		
Nordic countries	163,160	161,129
Rest of Europe	342	1,939
North America	53,064	55,799
Rest of world	761	832
Total	**217,327**	**219,698**

3. Revenue

Principles of revenue recognition are stated in Note 1.2 Accounting principles, section Revenue recognition.

Disaggregation of revenue

EUR 1,000	2024	2023
Sales channels		
Revenue from external customers		
Partner channel	118,237	105,122
Direct channel (E-commerce)	28,021	25,249
Total	**146,258**	**130,371**

EUR 1,000	2024	2023
Geographical information		
Revenue from external customers		
Nordic countries	42,019	39,989
Rest of Europe	48,099	49,221[1)]
North America	45,518	32,792[1)]
Rest of world	10,621	8,370
Total	**146,258**	**130,371**

1) F-Secure has adjusted the geographical split of revenues between Rest of Europe and North America. The adjustment did not have a material impact to the reported figures.

F-Secure had one individual customer which represented more than 10% of Group's 2024 revenue. Total revenue from this customer was EUR 17,147 thousand.

Assets and liabilities from contracts with customers

Satisfied performance obligations from contracts with customers that have not yet been invoiced on the reporting date are presented in the balance sheet as Accrued income. The balances relate to products delivered to customers and recognised as revenue but not invoiced. Liabilities from contracts with customers are presented in the balance sheet as Deferred revenue and included in Total non-current liabilities or Total current liabilities depending on the duration of the liability. Prior year current deferred revenue is recognised as revenue in the current period. Remaining performance obligations from contracts with customers represent contracted revenue that has not yet been recognised. These balances are presented as Deferred revenue and relate to obligations to provide software subscription services in contracts with a duration of multiple years.

EUR 1,000	2024	2023
Accrued income	3,333	1,953
Deferred revenue, non-current	6,398	5,837
Deferred revenue, current	22,079	19,788

Increases in deferred revenue resulting from billing were EUR 22,640 thousand for the year ended (EUR 22,005 thousand). Decreases in deferred revenue resulting from satisfying performance obligations were EUR 19,788 thousand for the year (EUR 17,324 thousand).

4. Other operating income

EUR 1,000	2024	2023
Government grants	228	330
Transition services	515	426
Other	8	74
Total	**751**	**830**

The government grants are received for certain research and development projects and are recognised as income over those periods in which the corresponding expenses arise.

None of the amounts included in Other are individually significant.

5. Leases

The principles of lease accounting are stated in Note 1.2 Accounting principles, section Leases.

EUR 1,000	2024	2023
Depreciation		
Right of use assets		
Buildings	1,049	936
Cars	117	103
Total	**1,165**	**1,039**
Interest expense on lease liabilities	66	29
Short-term leases booked as rent expense	213	163

Right of use assets	2024	2023
Buildings	969	1,060
Cars	231	197
Total	**1,200**	**1,257**

Lease liabilities	2024	2023
Buildings	988	1,076
Cars	222	187
Total	**1,210**	**1,263**
Repayments of lease liabilities	1,174	1,070

In the second quarter of 2024, F-Secure signed a new lease agreement for headquarter office premises. This will be recorded in the balance sheet as right-of-use asset and lease liability during summer 2025 when the lease term starts, but the lease commitment already exists following the agreement. The four-year contract value is EUR 5.1 million.

Right of use assets related changes are stated in Note 14. Non-current assets.

Interest expenses related to lease liabilities are stated in Note 9. Financial income and expenses.

Maturity of lease liabilities is stated in Note 20. Financial liabilities.

6. Depreciation and amortization

EUR 1,000	2024	2023
Depreciation and amortization of non-current assets		
Other intangible assets	9,663	4,829
Capitalized development	2,581	2,201
Intangible assets	**12,244**	**7,030**
Right of use assets	1,165	1,039
Other tangible assets	211	130
Tangible assets	**1,377**	**1,169**
Total depreciation and amortization	**13,621**	**8,199**

Depreciation and amortization by function (EUR 1,000)		
Sales and marketing	1,213	1,115
Research and development	3,882	2,339
Administration	8,525	4,745
Total depreciation and amortization	**13,621**	**8,199**

7. Personnel expenses

EUR 1,000	2024	2023
Personnel expenses		
Wages and salaries	36,065	33,295
Pension expenses - defined contribution plan	4,856	4,742
Share-based payments	1,045	619
Other social expenses	3,062	2,639
Total	**45,029**	**41,296**

For share-based payments, see further in Note 19. Share-based payment transactions.

Employee benefits of the management are stated in Note 24. Related party transactions.

	2024	2023
Average number of personnel	519	484

Personnel by function December 31		
Sales and marketing	169	197
Research and development	308	277
Administration	52	50
Total	**529**	**524**

Previously separately reported function Delivery is merged to Sales and marketing function in connection with the change in calculation method for gross margin. Comparison period is also revised.

8. Audit fees

EUR 1,000	2024	2023
Group auditor		
Audit fees, PricewaterhouseCoopers	159	205
Audit related fees, PricewaterhouseCoopers	21	
Tax consulting, PricewaterhouseCoopers	11	
Other consulting, PricewaterhouseCoopers	126	1,233
Total	**317**	**1,438**

Other consulting during 2024 includes, among others sustainability advisory and assurance.

EUR 1,000	2024	2023
Other auditors		
Audit fees	26	26
Total	**26**	**26**

9. Financial income and expenses

EUR 1,000	2024	2023
Financial income		
Exchange gains	850	6,167
Interest income from receivables	838	739
Other financial income	26	89
Total	**1,714**	**6,995**
Financial expenses		
Exchange losses	-1,090	-1,201
Interest expenses	-11,370	-7,240
Other financial expenses	-597	-345
Interest expense from lease liabilities	-66	-29
Total	**-13,124**	**-8,815**

10. Income tax

This note presents F-Secure's income tax expenses included in the financial statements. The accounting principles of income taxes are stated in Note 1.2, section Income tax.

EUR 1,000	2024	2023
Current income tax for the year	3,610	4,469
Change in deferred tax	2,334	847
Total	**5,944**	**5,316**

A reconciliation of income tax expense in the income statement and income tax calculated at the parent company's country of residence income tax rate (20%):

EUR 1,000	2024	2023
Profit before taxes	27,011	27,677
Income tax at Finnish tax rate of 20%	-5,402	-5,527
Effect of overseas tax rates	-425	-218
Non-deductible expenses/tax-exempt revenue	-130	283
Effect of deferred tax not recognized	8	-12
Adjustments for prior period tax	10	283
Other	-5	-126
Total	**-5,944**	**-5,316**

11. Earnings per share

Basic earnings per share amounts are calculated by dividing net profit for the year attributable to ordinary equity holders of the parent by the weighted average number of ordinary shares outstanding during the year. Diluted earnings per share amounts are calculated by dividing the net profit attributable to ordinary shareholders by the weighted average number of ordinary shares outstanding during the year adjusted for the effects of dilutive options.

EUR 1,000	2024	2023
Net profit attributable to equity holders from	21,067	22,360
Weighted average number of ordinary shares (1 000)	174,673	174,673
Weighted average number of ordinary shares (1 000), diluted	174,924	174,527
Basic and diluted earnings per share (EUR/share)	0.12	0.13

Earnings per share is based on the average number of shares. During the period, F-Secure hasn't had Treasury shares.

12. Acquisitions

Group hasn't made any acquisitions during 2024.

Comparative period

On 1 June 2023 F-Secure completed the acquisition of mobile consumer security business unit from Lookout Inc. The acquired mobile consumer security business unit consists of shares of Lookout LLC in the US and Saferpass s.r.o. in Slovakia as well as certain IP and related know-how transferred to Finland. In the transaction 65 employees were transferred to F-Secure.

The acquisition strengthens F-Secure's position as a leading consumer security company. F-Secure has significantly increased scale, strengthened footprint in the US and in the communication service provider channel as well as a complementary mobile optimized software product portfolio reaching tens of millions of subscribers worldwide.

Purchase consideration

The purchase consideration comprises of cash payment of EUR 207.9 million which was financed with external debt. The initial consideration EUR 206.9 million was paid in USD in June. EUR 0.9 million was settled during Q4/2023 and final purchase price adjustment EUR 0.1 million was settled in Q1/2024. Adjustments relate to net working capital. The company hedged the purchase price between signing and closing which resulted in profit of EUR 5.5 million booked in financial income. The company did not apply hedge accounting for the arrangement.

EUR 1,000	
Cash flow from the acquisition	
Consideration paid in cash	-207,900
Cash and cash equivalents of the acquired business	9
Total cash flow from the acquisition	**-207,891**

Recognized amounts of identifiable assets required and liabilities assumed

Lookout's net assets were identified and recognized at fair value as of the acquisition date on 1 June 2023. The following table summarizes the fair values of assets acquired and liabilities assumed.

Provisional fair values of the assets and liabilities recognized as a result of the acquisition

EUR 1,000	
Tangible assets	1
Technology-related intangibles	83,013
Customer-related intangibles (Partner business)	31,717
Customer-related intangibles (Direct business)	1,829
Deferred tax assets	647
Trade and other receivables	5,583
Cash and cash equivalents	9
Total assets	**122,800**
Other non-current liabilities	473
Trade and other liabilities	2,979
Deferred tax liabilities	546
Total liabilities	**3,998**
Total net assets	**118,802**
Goodwill	**89,099**

The identified intangible assets relate to technology and customer relationships. Fair values for the intangible assets have been determined using appropriate valuation methods including multi-period excess earnings method (MEEM) for customer relationships and Relief from royalty method (RfR) for technology. The amortization period for these varies from 5 years to 15 years. Goodwill reflects the value of buyer specific synergies, geographic presence, assembled workforce, future technology and customers. The total amount of goodwill that is expected to be deductible for tax purposes in Finland and in USA is EUR 83.5 million.

Aquisition related costs of EUR 6.2 million are expensed and included in administration expenses in consolidated income statement and in operating cash flow in the consolidated statement of cash flows.

Impact on F-Secure's comprehensive income statement

The acquired business contributed revenues of EUR 17.4 million and net profit of EUR –0.1 million to F-Secure for the period from 1 June to 31 December 2023 including amortization of the fair valued assets acquired for the period EUR –4.7 million and fair valuation of deferred revenue EUR –3.2 million.

Had the acquisition occurred on 1 January 2023, management estimates that combined illustrative revenue would have been EUR 142.7 million for Jan–Dec 2023 and combined illustrative net profit would have been EUR 18.4 million including amortization of fair valued assets EUR –8.0 million, interest expenses for the loan EUR –10.8 million and fair valuation of deferred revenue EUR –4.1 million.

Financial information of Lookout consumer business unit for the 5-month period ended May 30, 2023 has been carved out and combined from Lookout Inc's management reporting, accounting records and other sources of financial information. Lookout consumer business carve-out financial data for the above period includes cost allocations, management assumptions, judgements and estimates as Lookout consumer business unit has not formed a legal sub-group within Lookout and it has not prepared consolidated group financial information prior to the transaction. Pro forma adjustments are attributable to accounting policy alignments between F-Secure's accounting policies and US GAAP accounting principles applied by Lookout and impact of the fair value adjustments.

13. Goodwill

F-Secure's has a single operating segment as the group is followed as a whole. For impairment testing goodwill is allocated to cash-generating units (CGUs). F-Secure has only one CGU which consists of F-Secure's total business. The carrying amount of goodwill EUR 89,783 thousand is allocated to this CGU.

Goodwill is tested for impairment annually, or more frequently if there are indications that goodwill might be impaired. The recoverable amount for the CGU is determined based on a value in use calculation which uses cash flows for the period determined for the CGU. Cash flows are based on financial budgets and forecasts approved by the Board of Directors. Forecast period of five years is used. Discount rate is 8.39% (9.71%) before taxes.

Cash flows beyond forecast period have been extrapolated using steady 2% (2%) per annum growth rate. Markets where CGU operates are expected to grow faster than the terminal growth rate in impairment testing. Market is expected to grow mid single digit annually by 2027 (based on F-Secure management estimate and industry analyst reports).

Sensitivity analysis

F-Secure has prepared a sensitivity analysis of the impairment tests, adjusting the key assumptions which are revenue, profitability, and discount rate -based on management judgment. Any reasonable possible changes in the key assumptions in impairment tests would not cause the aggregate carrying amounts exceeding the recoverable amounts.

14. Non-current assets

	Intangible assets						Tangible assets			
EUR 1,000	Intellectual property	Other Intangible[1]	Goodwill	Capitalized development[2]	Advance payments & incomplete development	Total	Machinery & Equipment	Right of use assets	Other Tangible	Total
Acquisition cost Dec 31, 2022		**588**		**7,837**	**1,988**	**10,413**	**124**	**2,631**	**91**	**2,845**
Translation difference		-1,062	-738			-1,799	3	-1		2
Acquisitions and divestments	82,910	33,536	89,099	103		205,648				
Additions					7,625	7,625	319	493	18	829
Transfers		1,544		1,917	-3,461	0				
Disposals				-675		-675	-1	-102		-103
Acquisition cost Dec 31, 2023	**82,910**	**34,607**	**88,361**	**9,182**	**6,152**	**221,212**	**444**	**3,020**	**108**	**3,573**
Translation difference		2,002	1,422			3,424	14	-10		5
Additions					10,986	10,986	170	1,193	2	1,365
Transfers		6,955		8,322	-15,662	-385				
Disposals							-14	-831		-845
Acquisition cost Dec 31, 2024	**82,910**	**43,563**	**89,783**	**17,504**	**1,475**	**235,237**	**615**	**3,372**	**110**	**4,097**
Acc. depreciation Dec 31, 2022				**-1,350**		**-1,350**	**-41**	**-797**	**-19**	**-857**
Translation difference		33				33	-3	1		-2
Depreciation for the period	-3,125	-1,703		-2,201		-7,030	-77	-1,036	-52	-1,165
Depreciation of disposals				675		675		69		69
Acc. depreciation Dec 31, 2023	**-3,125**	**-1,670**		**-2,876**		**-7,672**	**-121**	**-1,763**	**-71**	**-1,955**
Translation difference		-154				-154	-3	7		5
Transfers		282		103		385				
Depreciation for the period	-5,546	-4,149		-2,581		-12,276	-182	-1,175	-34	-1,391
Depreciation of disposals							12	759		770
Acc. depreciation Dec 31, 2024	**-8,671**	**-5,691**	**-**	**-5,354**	**-**	**-19,717**	**-294**	**-2,172**	**-105**	**-2,571**
Book value as at Dec 31, 2023	79,785	32,937	88,361	6,305	6,152	213,540	323	1,257	37	1,617
Book value as at Dec 31, 2024	**74,239**	**37,872**	**89,783**	**12,150**	**1,475**	**215,520**	**321**	**1,200**	**4**	**1,526**

1) Other intangible consists mainly of customer relationship from acquisition.

2) Capitalised development expenses relate to new products and development of new product versions with significant new features (refer to the section on Research and development expenditure included within Intangible assets in Note 1.2 Accounting principles).

15. Inventories

The accounting principles of inventories are stated in Note 1.2 Accounting principles, section Inventories.

EUR 1,000	2024	2023
Inventories	29	35

The inventory balances included in the financial statements consist of the packaging used for license key cards.

16. Financial assets

This note presents F-Secure's financial assets included in the financial statements. The accounting principles of financial assets are stated in Note 1.2 Accounting principles, section Financial instruments.

EUR 1,000	2024	2023
Cash at bank and in hand	8,095	15,867
Interest-bearing receivables, non-current	223	3,658
Interest-bearing receivables, current	3,757	-
Trade receivables	27,604	28,558
Total	**39,678**	**48,083**

Interest-bearing receivables relate to WithSecure structuring loans which are due in the second quarter of 2025. Since Group also has liability against WithSecure the credit risk is unlikely.

Aging of trade receivables and expected credit losses

Trade receivables 31 Dec 2024 (EUR 1,000)	Not fallen due	Overdue 1-30 days	Overdue 31-60 days	Overdue 61-90 days	Overdue 91-120 days	Overdue more than 120 days	Total
Average expected credit loss rate	0.4 %	0.4 %	5.0 %	12.0 %	17.0 %	35.0 %	
Gross trade receivables	22,039	4,058	413	685	421	675	28,291
Loss allowance	-88	-16	-21	-82	-71	-249	-528
Additional provision	-	-	-	-	-	-160	-160
Total trade receivables at amortized cost Dec 31, 2024	**21,951**	**4,042**	**392**	**603**	**349**	**266**	**27,604**

Trade receivables 31 Dec 2023 (EUR 1,000)	Not fallen due	Overdue 1-30 days	Overdue 31-60 days	Overdue 61-90 days	Overdue 91-120 days	Overdue more than 120 days	Total
Average expected credit loss rate	0.5 %	0.5 %	5.0 %	12.0 %	19.0 %	50.0 %	
Gross trade receivables	22,947	3,388	1,771	597	87	314	29,104
Loss allowance	-115	-17	-89	-72	-17	-157	-465
Additional provision	4	-1	-	-	-	-84	-81
Total trade receivables at amortized cost Dec 31, 2023	**22,836**	**3,371**	**1,683**	**525**	**71**	**73**	**28,558**

EUR 1,000	2024	2023
Movements in loss allowances on trade receivables		
Book value as at Jan 1	547	394
Change for the year	190	183
Receivables written off during the year	-49	-31
Book value as at Dec 31	**687**	**547**

17. Other receivables

Non-current receivables

EUR 1,000	2024	2023
Other receivables	223	-
Total	**223**	-

Current receivables

EUR 1,000	2024	2023
Other receivables	845	647
Prepaid expenses	8,600	6,400
Accrued income	3,333	1,953
Income tax receivables	968	2,108
Total	**13,747**	**11,108**

Material items included in prepaid expenses

EUR 1,000	2024	2023
Prepaid royalty	918	879
Grant receivables	192	382
Merchandise cost	453	299
Other prepaid expenses	7,037	4,840
Total	**8,600**	**6,400**

Other prepaid expenses include mainly annual software licenses.

18. Shareholders' Equity

Issued and fully paid

EUR 1,000	Number of shares	Share capital	Unrestricted equity reserve
Demerger 30 June 2022	174,526,944	80	9,590
31 December 2022	174,526,944	80	9,590
Share issue 2023	146,221		
31 December 2024	**174,673,165**	**80**	**9,590**

The share capital amounting to 80,000 euro was formed in the demerger on 30 June 2022. The number of shares was 174,673,165 (no own shares) at the end of 2024.

Company has made two directed share issues in March 2023 to the plan participants of the company's Performance Share Plan and Restricted Share plan. The shares issued account for the rewards earned from the performance period 2020–2022 and retention period 2021–2022.

A share has no nominal value. Accountable par value is EUR 0.01.

Translation differences

The translation difference is used to record exchange difference arising from the translation of the financial statements of foreign subsidiaries.

Unrestricted equity reserve

Unrestricted equity reserve was formed in connection with demerger on 30 June 2022. Unrestricted equity reserve includes other equity-related investments and that part of the share subscription price which is not recognized in share capital according to a specific decision.

Dividends proposed and paid

Proposed for approval at AGM for financial year 2024 is that dividend of 0.04 euro per share will be paid.

Dividend for financial year 2023 was 0.07 per share, paid during 2024 (12,227,121.55 euro in total).

Dividend for financial year 2022 was 0.07 per share, paid during 2023 (12,227,121.55 euro in total).

Treasury shares

At the end of 2024 company doesn't hold any treasury shares.

19. Share-based payment transactions

F-Secure has had several share-based incentive programs during the period. The purpose of the plans is to align the interests of the shareholders and the plan participants in order to increase the value of F-Secure share and retain and motivate key management by offering them a competitive incentive plan.

Prior to demerger, F-Secure personnel have participated in the incentive plans in WithSecure and the ongoing incentive programs from WithSecure continue. All long-term incentive plan allocations made originally in the shares of WithSecure were adjusted through a modification to be the allocation of F-Secure Corporation after the demerger. The effect of the plans and related expenses attributable to F-Secure for each financial year are presented below. Accounting principles for share-based payments are stated in Note 1.2 Accounting principles, section Share-based payment transactions.

Share-based incentive programs

The share-based incentive programs offer the participants a possibility to receive shares of F-Secure Corporation as an incentive reward if the company's financial targets set for the earning period have been achieved. No reward can be given to any participating employee, whose employment has terminated before the end of the lock-up period. The plan structure is following: a Performance Share Plan for the company's senior management, a Restricted Share Plan for individually selected key employees and an Employee Share Savings Plan for all employees.

Performance share plan 2020–2022 (originally from WithSecure)

WithSecure established originally in February 2020 a share-based incentive program 2020–2022. The program's duration is five years and it comprises three earning periods, 2020–2022 with the grant date in April 2020, 2021–2023 with the grant date in April 2021, and 2022–2024 with the grant date in March 2022. Each earning period lasts for three years. The program has ended on December 31, 2024. The value of WithSecure share at grant date for the program were EUR 2.18 for the 2020–2022 earning period, EUR 3.42 for the 2021–2023 earning period, and EUR 5.12 for the earning period 2022–2024. After demerger, there were adjustments made to earning periods 2021–2023 and 2022–2024 using the reference prices of the two new companies.

Criteria measurement for 2020–2022 was decided to execute as if the two companies would still form the old entity. After demerger allocations made originally in the shares of WithSecure were adjusted through modifications. There was no fair value increase resulting from the modifications. The rewards will be equity-settled.

The vesting of the rewards for all periods was conditional to the participant remaining in the service of F-Secure. In addition, the 2020–2022 period has a performance condition based on F-Secure's and WithSecure's relative total shareholder return of WithSecure's and F-Secure's share and the periods 2021–2023 and 2022–2024 have a performance condition based on absolute total shareholder return of F-Secure's share. The Board approves the metrics, targets and participants on annual basis for each earning period.

In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the Share-based incentive program 2020–2022 was EUR 259 (287) thousand in 2024.

Performance share plan 2023–2025

F-Secure established a share-based program 2023–2025. The program's duration is three years with the grant date in April 2023. The value of F-Secure share at grant date for the program were EUR 3.39 for the earning period 2023-2025. The current program ends in March 2026 with a possible reward payment, paid during spring 2026. The payment of the reward is conditional on the achievement of the performance targets. The maximum total of shares to be given is 800,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards is conditional to the participant remaining in the service of F-Secure. The incentive plan has a performance condition based on F-Secure's absolute total shareholder return and revenue growth and profitability.

In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the Performance share plan 2023–2025 was EUR 351 (262) thousand in 2024.

Performance share plan 2024–2026

F-Secure established a share-based program 2024–2026. The program's duration is three years with the grant date in April 2024. The value of F-Secure share at grant date for the program were EUR 1.72 for the earning period 2024-2026. The current program ends in March 2027 with a possible reward payment, paid during spring 2027. The payment of the reward is conditional on the achievement of the performance targets. The maximum total of shares to be given is 1,512,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards is conditional to the participant remaining in the service of F-Secure. The incentive plan has a performance condition based on F-Secure's absolute total shareholder return and revenue growth and profitability.

In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the Performance share plan 2024–2026 was EUR 267 thousand in 2024.

Restricted share plan 2023–2025

F-Secure established a restricted share plan in March 2023. The program's duration is three years and potential reward will be paid during spring 2026. Company can grant fixed share rewards during retention period. The restricted share plan complements the incentive programs for separately selected key persons in special situations. The values of the F-Secure share at grant date for this program was EUR 2.98 and EUR 2.05 and the maximum total of shares to be given is 80,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards for all periods is conditional on the participant remaining in the service of F-Secure. The Board approved the metrics, targets and participants on an annual basis for each earning period. In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the restricted share plan was EUR 18 (27) thousand in 2024.

The participating employee of a share-based incentive program shall be entitled to the shareholder rights of the reward shares (e.g., dividend) from the moment the shares have been entered into the participating employee's book-entry account.

The costs of equity-settled transactions are measured by reference to the fair value of shares at the date on which they are granted. Fair value for performance based programs is based on the share price on the grant date. Fair value for market based programs is based on externally accepted valuation methods. The costs of cashsettled transactions are measured by reference to the market price of the share on the balance sheet date. F-Secure updates the estimate of the number of equity instruments that will ultimately vest at each reporting date.

Restricted share plan 2024–2026

F-Secure established a restricted share plan in March 2024. The program's duration is three years and potential reward will be paid during spring 2027. Company can grant fixed share rewards during retention period. The restricted share plan complements the incentive programs for separately selected key persons in special situations. The values of the F-Secure share at grant date for this program was EUR 1.65 and EUR 2.01 and the maximum total of shares to be given is 300,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards for all periods is conditional on the participant remaining in the service of F-Secure. The Board approved the metrics, targets and participants on an annual basis for each earning period. In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the restricted share plan was EUR 65 thousand in 2024.

The participating employee of a share-based incentive program shall be entitled to the shareholder rights of the reward shares (e.g., dividend) from the moment the shares have been entered into the participating employee's book-entry account.

The costs of equity-settled transactions are measured by reference to the fair value of shares at the date on which they are granted. Fair value for performance based programs is based on the share price on the grant date. Fair value for market based programs is based on externally accepted valuation methods. The costs of cashsettled transactions are measured by reference to the market price of the share on the balance sheet date. F-Secure updates the estimate of the number of equity instruments that will ultimately vest at each reporting date.

Employee share savings plan

During 2022, F-Secure launched a employee share savings plan which was available for all employees. The plan consists of annually commencing plan periods, each one comprising of a 12-month savings period and a holding period following the savings period. The first plan period commenced on 1 October 2022 and ends on 30 September 2025. The second plan period commenced on 1 October 2023

and ends on 30 September 2026. Third plan period commenced on 1 October 2024 and ends on 30 September 2027. Every employee was eligible to save a proportion of their salaries and invest those savings in F-Secure shares. The savings will be used for acquiring F-Secure shares quarterly after the publication of the respective interim reports. F-Secure grants the participating employees a gross reward of one matching share for every two shares acquired with their savings. For the first plan period the maximum number of of matching shares is approximately 200 000 shares, for the second plan period 250 000 shares and for the third plan period 392,023 shares.

The vesting of the rewards is conditional on the participant remaining in the service of F-Secure and on an initial investment. The Board approves the metrics, targets, and participants on an annual basis for each earning period. The expense arising from the employee shares savings plan was EUR 85 (44) thousand in 2024.

Impacts of share-based payment transactions on financial statements

EUR 1,000	2024	2023
Booked as expense during the period	1,045	619
Booked in retained earnings during the period	1,045	139
Balance sheet liability at the end of the period	84	87

20. Financial liabilities

F-Secure's financial liabilities consist of interest-bearing liabilities and trade payables. Interest-bearing liabilities include bank loans, structuring loans towards WithSecure as well as lease liabilities from building and cars (see Note 1.2 Accounting principles, section Leases and Note 5. Leases).

Interest-bearing liabilities

EUR 1,000	2024	2023
Bank loans	168,933	190,357
Lease liabilities	1,210	1,263
Other interest-bearing liabilities	5,334	5,307
Total	**175,477**	**196,928**

F-Secure acquired the mobile consumer security unit from Lookout Inc. in 2023. The acquisition was financed by external debt and resulted to a significant increase in interest-bearing liabilities. Loan agreement including two facilities for EUR 202 million amortizing term loan and EUR 20 million revolving credit facility was signed with Danske Bank A/S and OP Corporate Bank Plc. Maturity of both facilities is 3 years with two 1-year extension options and the first extension option was exercised in April 2024. During the accounting period, the term loan was repaid by EUR 30.0 million (EUR 10.0 million). F-Secure has drawn down revolving credit facility by EUR 8.0 million at the reporting date for general cash management purposes.

The Group's loan agreement includes a financial covenant, measured on quarterly basis. The covenant relates to the ratio between net debt and adjusted EBITDA, as defined under the terms of the loan agreement. Group has met covenant terms and conditions during the reporting period and on the reporting date. Carrying amount for bank loans at the end of reporting period is EUR 168.9 million (EUR 190.4 million).

Prior to completion of the demerger, WithSecure's consumer business conducted by its foreign subsidiaries was separated from the rest of the business into separate companies through business acquisitions or similar transactions in each relevant country. The transaction prices vary between approximately EUR 70 thousand and EUR 3.0 million. The payback time for the resulting payables and receivables is primarily three years from the effective date of each local transaction, and prepayment is allowed. Therefore, these balances are now short-term and due for payment in the second quarter of 2025. The interest rate for the unpaid transaction price varies by country. F-Secure's payables totalled EUR 5.3 million, presented in the table above as Other interest-bearing liabilities.

F-Secure has no outstanding derivative contracts on 31 December 2024.

Contractual maturities of interest-bearing liabilities

EUR 1,000	2024	2023
Amount due for settlement within 12 months	44,046	30,965
Amount due for settlement after 12 months	131,431	165,963
Total	**175,477**	**196,928**

Bank loan carry variable interest rates. The weighted average interest rates paid during the year were as follows:

	2024	2023
Bank loans	5.8 %	5.6 %

Contractual maturities of financial liabilities

Contractual maturities of financial liabilities (EUR 1,000)	Less than 1 year	1 to 2 years	2 to 3 years	3 to 4 years	4 to 5 years	over 5 years	Total contractual cash flows	Carrying amount
2024								
Bank loans	38,000	30,000	102,000				170,000	168,933
Interest payment for bank loan	7,059	5,507	1,435					
Lease liabilities	756	328	111	37	14		1,247	1,210
Other interest-bearing liabilities	5,334						5,334	5,334
Trade payables	1,545						1,545	1,545
Total	**52,694**	**35,835**	**103,545**	**37**	**14**		**178,125**	**177,022**

Contractual maturities of financial liabilities (EUR 1,000)	Less than 1 year	1 to 2 years	2 to 3 years	3 to 4 years	4 to 5 years	over 5 years	Total contractual cash flows	Carrying amount
2023								
Bank loans	30,000	30,000	132,000				192,000	190,357
Interest payment for bank loan	10,986	8,933	2,392					
Lease liabilities	991	115	74	39	35	14	1,269	1,263
Other interest-bearing liabilities		5,307					5,307	5,307
Trade payables	3,911						3,911	3,911
Total	**45,888**	**44,356**	**134,466**	**39**	**35**	**14**	**202,488**	**200,839**

21. Financial risk management

Classes and categories of financial assets and liabilities and their fair values

Fair value hierarchy levels 1 to 3 are based on the degree to which the fair value is observable:

Level 1: Fair values of financial instruments are based on quoted prices in active markets for identical assets and liabilities.

Level 2: Financial instruments are not subject to trading in active and liquid markets. The fair values of financial instruments can be determined based on quoted market prices and deduced valuation.

Level 3: Measurement of financial instruments is not based on verifiable market information, and information on other circumstances affecting the value of the instruments is not available or verifiable.

The carrying amount of the Group's interest-bearing financial assets and liabilities does not significantly differ from their fair value. Interest-bearing receivables and other interest-bearing liabilities are agreements with WithSecure, which are short-term and tied to variable market interest rates, and therefore their carrying amount is estimated to be the same as their fair value. The carrying amount of the Group's bank loans as of the December 31, 2024, is EUR 168.9 million, and the fair value is EUR 168.8 million.

			Carrying value		
2024			Financial assets	Financial liabilities	
EUR 1,000	Note	Fair value hierarchy	Amortized cost	Amortized cost	TOTAL
Cash and bank	16		8,095		8,095
Interest-bearing receivables	16	Level 2	3,980		3,980
Trade receivables	16		27,604		27,604
Trade payables	20			1,545	1,545
Lease liabilities	20			1,210	1,210
Bank loans	20	Level 2		168,933	168,933
Other interest-bearing liabilities	20	Level 2		5,334	5,334

2023			Carrying value		
			Financial assets	Financial liabilities	
EUR 1,000	Note	Fair value hierarchy	Amortized cost	Amortized cost	TOTAL
Cash and bank	16		15,867		15,867
Interest-bearing receivables	16	Level 2	3,658		3,658
Trade receivables	16		28,558		28,558
Trade payables	20			3,911	3,911
Lease liabilities	20			1,263	1,263
Bank loans	20	Level 2		190,357	190,357
Other interest-bearing liabilities	20	Level 2		5,307	5,307

General

The responsibility for F-Secure's risk management lies with the CEO, management and ultimately with the Board of Directors. The goal of risk management is to identify risks that may hinder the company from achieving its business objectives. F-Secure is exposed to various financial risks in its business operations. Main financial risks are credit risk, liquidity risk, foreign currency exchange risk and interest rate risk. The Board of Directors of F-Secure approves the general principles of risk management, and the Group's treasury function is responsible for managing market risks.

Credit risk

F-Secure manages credit risk on group level with Credit risk policy. Credit risk derives from trade receivables. The maximum exposure to credit risk at the reporting date is the carrying value of trade receivables. Trade receivables do not include any major concentrations of credit risk by customer. Group trades only with recognized, creditworthy third parties and monitors customers' creditworthiness. Trade receivables are monitored and collected on an ongoing basis. The top three customers account for 16.0%, 6.6% and 5.5% in 2024 (16.1%, 7.1% and 6.6% in 2023) of trade receivables. See Note 16. Financial assets.

Liquidity risk

Liquidity risk arises if the Group's existing liquidity reserves, net cash flows and available additional financing are not sufficient to cover commitments falling due within next 12 months. Group manages its liquidity risk by centralizing the management of cash reserves, maintaining sufficient cash balances, and utilizing committed credit facilities. F-Secure has a revolving credit facility (RCF) of EUR 20 million that matures in 2027. F-Secure has drawn down revolving credit facility by EUR 8.0 million at the reporting date. Group Treasury is responsible for monitoring cash balances and cash forecasts to keep liquidity risk at manageable level. We expect the stable and positive cash flow from operations, existing cash balances, and revolving credit facilities to be sufficient to fund our operations and obligations for the next 12 months. Contractual maturities of financial liabilities are presented in note 20 Financial liabilities.

The Group's loan agreement includes a financial covenant, measured on quarterly basis. The covenant relates to the ratio between net debt and adjusted EBITDA, as defined under the terms of the loan agreement. The group closely monitors the covenant situation and will take action if necessary. Group has met covenant terms and conditions during the reporting period. Carrying amount for bank loan at the end of reporting period is EUR 168.9 million (EUR 190.4 million).

Foreign currency risk

The Group operates globally and is exposed to a currency risk arising from exchange rate fluctuations against its reporting currency euro. Transaction risk is related to foreign currency transactions in sales and expenses. Translation risk arises from the Group's net investments outside euro zone.

Transaction risk

Transaction risk arises from future commercial transactions and recognized assets and liabilities denominated in a currency that is not the functional currency of the relevant group entity. The majority of sales is invoiced in Euro. The other main currencies for invoicing are US dollar (USD), the Swedish krona (SEK), the pound sterling (GBP) and the Japanese yen (JPY). The currency risk arising from sales

invoicing is reduced by operational expenses arising in the same currencies as the sales invoicing. The transaction risk is managed centrally such that the F-Secure operations mainly have transactions in their legal entities' functional currency and intercompany transactions are carried out in the group entities functional currencies. The main foreign currency risk arises from USD denominated sales invoicing, purchases and intercompany transactions at the F-Secure parent entity level, creating volatility in the financial income and expenses.

Exchange gains were EUR 0.9 million (EUR 6.2 million) and exchange losses EUR -1.1 million (EUR -1.2 million).

	2024	2023
Sales in different currencies	**%**	**%**
EUR	59	64
USD	30	25
JPY	5	4
SEK	4	3
GBP	2	2
Other currencies	1	2
Total	**100**	**100**

The carrying Euro (thousand) amounts of the Group's financial assets and liabilities at the reporting date are as follows:

Financial assets (EUR 1,000)	2024	%	2023	%
EUR	19,255	49	26,417	55
USD	12,090	27	13,074	27
GBP	2,958	7	4,108	9
JPY	2,023	5	1,782	4
Other currencies	3,353	11	2,701	6
Total	**39,678**	**100**	**48,082**	**100**

Financial liabilities (EUR 1,000)	2024	%	2023	%
EUR	173,526	98	197,917	99
JPY	1,306	1	1,372	1
MYR	1,356	1	889	0
USD	327	0	205	0
Other currencies	506	0	455	0
Total	**177,022**	**100**	**200,839**	**100**

Financial liabilities in the above table also include lease liabilities.

The table below demonstrates how sensitive F-Secure's profit before taxes is to foreign exchange rate fluctuations when all other variables are held constant. The open exposure against USD arising from F-Secure trade receivables and trade payables have an impact on F-Secure's profit before taxes. The sensitivity calculation is based on a change of 10% in the Euro exchange rate against the functional currencies F-Secure operates in. There were no other material exposures.

EUR million	2024	2023
USD	-1.0/+1.2	-1.0/+1.2

Translation risk

Translation risk arises from the F-Secure's net investments in foreign currencies. Translation differences arise from translating balances into euro using exchange rates prevailing on the reporting date. Most significant translation risks arise from goodwill (EUR 23.8 million) and intangible assets (EUR 29.2 million) generated in acquisition of mobile consumer security business unit from Lookout Inc. Main currency is USD. According to current policy, F-Secure does not hedge investments made in its subsidiaries.

Change in foreign exchange translation differences amounted EUR 4.0 million in 2024 (EUR -2.0 million).

The table below demonstrates how sensitive the Group's equity is to foreign exchange rate fluctuations when all other variables are held constant. The sensitivity calculation is based on a change of 10% in the Euro exchange rate against the functional currencies exposing the Group to translation risk. There were no other material exposures.

EUR million	2024	2023
USD	-7.0/+5.7	-6.8/+5.5

Interest rate risk

F-Secure is exposed to interest rate arising from interest-bearing liabilities which relate to bank loans and structuring loans against WithSecure. The interest rate of bank loan of EUR 162 million (Facility A) is tied to variable reference interest rate. The interest rate related to WithSecure structuring loans (EUR 5.3 million in total) varies by country. F-Secure is regularly evaluating the need for hedging interest rate risk. In the financial year 2024, the company did not hedge against interest rate risk. Apart from bank loan there were no other material exposures. The table below demonstrates the sensitivity of Group's profit before taxes to 1% change in interest rate when all other variables are held constant.

EUR million	2024	2023
Interest-bearing liabilities, bank loans	-1.9/+1.9	-1.2/+1.2

Capital management

F-Secure's shareholders' equity is managed as capital. The objective of F-Secure's capital management is to maintain an efficient capital structure that ensures the functioning of business operations and promotes shareholder value. F-Secure's capital structure is reviewed regularly as a part of financial performance monitoring. The capital structure can be adjusted among other things by distribution of dividends, share repurchase or capital repayment. The dividend policy of F-Secure Corporation is to aim to pay around or above 50 per cent of its net profit as dividend on an annual basis. This can be adjusted as long as leverage is higher than the targeted level (below 2.5x). Subject to circumstances, the F-Secure can deviate from this policy.

22. Deferred tax

EUR 1,000	2024	2023
Deferred tax assets relate to following:		
Intangible assets and property, plant and equipment	1,162	1,311
Provisions and other liabilities	178	656
Other temporary differences	640	574
Total	**1,980**	**2,541**
Offset against deferred tax liabilities	-1,921	-1,658
Net deferred tax assets	**58**	**883**
Change in deferred tax assets:		
Recognized in profit or loss	-561	1,766
Acquisitions and disposals		647
Total, increase (+), decrease (-)	**-561**	**2,413**

EUR 1,000	2024	2023
Deferred tax liabilities relate to the following:		
Intangible assets and property, plant and equipment	4,874	2,808
Provisions and other liabilities	349	600
Other temporary differences	283	314
Total	**5,506**	**3,722**
Offset against deferred tax assets	-1,921	-1,658
Net deferred tax liabilities	**3,584**	**2,064**
Change in deferred tax liabilities:		
Recognized in profit or loss	1,783	2,613
Acquisitions and disposals		546
Total, increase (+), decrease (-)	**1,783**	**3,159**

Intangible assets and property, plant and equipment at 31 December 2024 includes deferred tax liabilities of EUR 0.5 million (0.5 million) related to fair value adjustments of the acquired net assets in the mobile consumer security business of Lookout Inc.

23. Other liabilities

EUR 1,000	2024	2023
Non-current liabilities		
Deferred revenue	6,398	5,837
Other non-current liabilities	45	51
Total	**6,443**	**5,888**
Current liabilities		
Deferred revenue	22,079	19,788
Trade payables	1,545	3,911
Provisions	1,427	1,739
Other liabilities	2,135	1,818
Accrued expenses	10,462	8,453
Income tax liabilities	387	1,592
Total	**38,035**	**37,301**
Material amounts shown under accrued expenses		
Accrued personnel expenses	7,937	6,183
Other accrued expenses	2,525	2,270
Total	**10,462**	**8,453**

Other liabilities under Current liabilities consist mainly of personnel and VAT related accruals.

Provisions

EUR 1,000	2024	2023
Book value as at 1.1.	1,739	
Increases during the year	1,427	1,739
Used during the year	-1,739	
Book value as at 31.12.	**1,427**	**1,739**

Management has recognized a provision of EUR 1,427 thousand (EUR 1,539 thousand) related to restructuring. Comparison period had also a EUR 200 thousand provision related to other provisional costs and expenses.

24. Related party disclosures

The Group's related parties include members of the Board, CEO and other members of the Leadership Team, their family members and organizations in which these individuals have direct or indirect control or significant influence.

Compensation of key management personnel of the Group

EUR 1,000	2024	2023
Wages and other short-term employee benefits	1,897	2,133
Pensions	211	422
Share-based payments		574
Total	**2,108**	**3,129**

Wages and other short-term employee benefits

EUR 1,000	2024	2023
CEO and President	334	422
Leadership Team	1,564	1,711
Members of the Boards of Directors	267	270
Total	**2,164**	**2,403**

Board of Directors and CEO and President

EUR 1,000	Wages	Fees
Timo Laaksonen, CEO and President	334	
Pertti Ervi, Chair of the Board		86
Risto Siilasmaa		38
Thomas Jul		43
Petra Teräsaho		48
Tommi Uitto		38
Katja Kuusikumpu		13
Madeleine Lassoued		1
Total	**334**	**267**

The CEO's retirement age and the determination of his pension conform to the standard rules specified by Finland's Employee Pension Act (TYEL). The pension cost of the CEO during the financial period was EUR 58 thousand (EUR 82 thousand). The period of notice for the CEO is six (6) months both ways and CEO is entitled to severance payment equivalent of six (6) months' salary.

25. Subsidiaries

Name	Country of incorporation	Group (%)
Parent F-Secure Corporation, Helsinki	Finland	
F-Secure Data Oy, Helsinki	Finland	100
F-Secure Data Oy, Norwegian branch	Norway	100
F-Secure Data Oy, Danish branch	Denmark	100
F-Secure Inc., Palo Alto	United States	100
F-Secure (UK) Ltd, Buckinghamshire	United Kingdom	100
F-Secure KK, Tokyo	Japan	100
F-Secure GmbH, Munich	Germany	100
F-Secure SAS, Paris	France	100
F-Secure AB, Stockholm	Sweden	100
F-Secure Srl, Milan	Italy	100
F-Secure Poland SP z.o.o., Poznan	Poland	100
F-Secure Sdn Bhd, Kuala Lumpur	Malaysia	100
F-Secure Pvt Ltd, Mumbai	India	100
F-Secure B.V., Hilversum	The Netherlands	100
F-Secure Iberia SL, Madrid	Spain	100
F-Secure do Brasil Tecnol. da Informãcao Ltda, Saõ Paulo	Brazil	100
F-Secure s.r.o., Bratislava	Slovakia	100

26. Subsequent events

On 10 January, F-Secure Board's Personnel and Nomination Committee gave proposals to the Annual General Meeting scheduled for 1 April 2025 for the composition and remuneration of the Board of Directors. Committee proposes that the Board of Directors consists of a total of six members and that the following persons be elected as members of the Board of Directors for a term expiring at the end of the Annual General Meeting 2026: Pertti Ervi, Petra Teräsaho and Tommi Uitto are proposed to be re-elected, and as new members, are proposed to be elected Roxana Diaconescu and Cornelia Schaurecker.

The Personnel and Nomination Committee proposes to the Annual General Meeting that the following annual remuneration be paid to the members of Board of Directors to be elected at the Annual General Meeting: EUR 80,000 annually for the Chair of the Board of Directors; EUR 38,000 annually for the external members of the Board of Directors; EUR 12,667 for members employed by F-Secure; EUR 10,000 additional remuneration for the Audit Committee Chair; EUR 4,000 additional remuneration for the Personnel and Nomination Committee Chair; EUR 2,000 additional remuneration for the members of Audit Committee as well as Personnel and Nomination Committee. The proposed annual fee and the fees for Committee work correspond to the current remuneration, with the exception of the additional remuneration for Personnel and Nomination Committee Chair and members of the Audit Committee and Personnel and Nomination Committee. In addition, The Personnel and Nomination Committee proposes that approximately 40 percent of the remuneration be paid as shares in the company repurchased from the market or as treasury shares held by the company.

On 7 February 2025, F-Secure Board's Personnel and Nomination Committee supplements the original proposal to the Annual General Meeting 2025 for the composition of the Board of Directors. In deviation from the proposal made on 10 January 2025, F-Secure Board's Personnel and Nomination Committee proposes that i) the board would consist of seven members and that ii) Alessandro Adriani and Rachit Mittal be elected as new members in addition to the previously proposed members. Except for the revised proposal concerning the Board's composition, the proposal by the Board's Personnel and Nomination Committee remains valid and unchanged.

F-Secure Corporation financial statements

Income statement

EUR 1,000	Note	FAS 2024	FAS 2023
Revenue	(1)	125,913	112,878
Cost of revenue		-18,996	-10,438[1)]
Gross Margin		**106,917**	**102,439**
Other operating income	(2)	2,181	2,849
Sales and marketing	(3,4)	-30,604	-33,616[1)]
Research and development	(3,4)	-26,917	-23,292[1)]
Administration	(3,4)	-25,406	-24,225
EBIT		**26,170**	**24,155**
Financial income and expenses	(6)	-4,417	-2,488
PROFIT (LOSS) BEFORE APPROPRIATIONS AND TAXES		**21,754**	**21,667**
Appropriations	(7)	-2,726	-7,566
Income taxes	(8)	-2,488	-2,535
RESULT FOR THE FINANCIAL YEAR		**16,539**	**11,566**

1) F-Secure changed the calculation method for gross margin in its income statement. Some of the costs previously recorded in F-Secure income statement as Cost of revenue have been included in Research and development and Sales and marketing costs.

Balance sheet

EUR 1,000	Note	FAS 2024	FAS 2023
ASSETS			
Non-current assets			
Intangible assets	(9)	151,788	155,877
Tangible assets	(9)	36	69
Investments in group companies	(10)	63,831	66,821
Other financial assets	(12)	36	-
Total non-current assets		**215,692**	**222,767**
Current assets			
Inventories	(11)	29	35
Trade and other receivables	(12)	29,493	32,655
Cash and bank accounts	(13)	5,395	12,935
Total current assets		**34,917**	**45,625**
TOTAL ASSETS		**250,609**	**268,391**

EUR 1,000	Note	FAS 2024	FAS 2023
EQUITY AND LIABILITIES			
Shareholder's equity	(14,15)		
Share capital		80	80
Reserve for invested unrestricted equity		9,590	9,590
Retained earnings		397	1,058
Profit for the financial year		16,539	11,566
Total shareholders' equity		**26,607**	**22,294**
Appropriations			
Depreciation difference		10,293	7,566
Non-current liabilities	(17)		
Interest bearing liabilities, non-current		132,811	163,356
Other non-current liabilities		4,952	5,715
Total non-current liabilities		**137,763**	**169,071**
Current liabilities	(17)		
Interest bearing liabilities, current		38,000	30,000
Provisions		-	200
Trade and other payables		17,837	22,141
Other current liabilities		20,110	17,118
Total current liabilities		**75,947**	**69,459**
TOTAL SHAREHOLDERS' EQUITY AND LIABILITIES		**250,609**	**268,391**

Cash flow statement

EUR 1,000	FAS 2024	FAS 2023
Cash flow from operations		
Result for the financial year	16,539	11,566
Adjustments		
Depreciation and amortization	16,854	9,089
Provisions	-200	
Change in depreciation difference	2,726	7,566
Other adjustments	-105	33
Financial income and expenses	4,417	2,488
Income taxes	2,488	2,535
Cash flow from operations before change in working capital	**42,719**	**33,277**
Change in net working capital		
Current receivables, increase (-), decrease (+)	1,727	-5,207
Inventories, increase (-), decrease (+)	6	6
Non-interest bearing debt, increase (+), decrease (-)	-1,588	15,381
Cash flow from operations before financial items and taxes	**42,864**	**43,456**
Interest expenses paid	-10,657	-8,675
Interest income received	442	378
Other financial income and expenses	-437	4,555
Income taxes paid	-1,991	-3,610
Cash flow from operations	**30,221**	**36,106**

EUR 1,000	FAS 2024	FAS 2023
Cash flow from investments		
Investments in intangible and tangible assets	-12,733	-155,910
Acquisition of subsidiaries	-456	-66,768
Other received distribution of assets from subsidiaries	3,446	
Dividends received	6,169	1,108
Cash flow from investments	**-3,574**	**-221,570**
Cash flow from financing activities		
Increase in share capital		
Increase in interest-bearing liabilities	8,000	202,000
Decrease in interest-bearing liabilities	-30,000	-10,000
Dividends paid	-12,227	-12,227
Cash flow from financing activities	**-34,227**	**179,773**
Change in cash	-7,579	-5,691
Effect of exchange rate changes on cash	40	-47
Cash and bank at the beginning of the period	12,935	18,673
Cash and bank at period end	**5,395**	**12,935**

Notes to the parent company Financial Statements

Basic information

F-Secure is a cybersecurity company who designs and offers security and privacy products and services to consumers to protect themselves against online threats.

F-Secure Corporation is the parent company of F-Secure Group, incorporated in Finland and domiciled in Helsinki. F-Secure Corporation was established through partial demerger on 30 June 2022. In the demerger F-Secure Corporation received assets and liabilities from WithSecure Corporation on 30 June 2022. Assets and liabilities were transferred with book values, and the transferred net equity was 9,670 thousand euro. Demerger plan, dated 17 February 2022, defines further which assets and liabilities were transferred. Company's registered address is Tammasaarenkatu 7, 00180 Helsinki. Copy of consolidated financial statements can be downloaded from www.f-secure.com.

Accounting principles

The financial statement of F-Secure Corporation has been prepared in accordance with Finnish Accounting Standards (FAS).

Foreign currency translation

Foreign currency transactions are translated using the exchange rates prevailing at the dates of the transactions. On the reporting date, assets and liabilities denominated in foreign currencies are translated using the European Central Bank's exchange rates prevailing at that date. Exchange rate gains and losses are recognized in financial items in the income statement.

Revenue recognition

F-Secure provides a comprehensive range of endpoint protection, privacy and password management solutions, and security for all consumers' connected devices at home. Revenue derives from the sale of security products through service provider and direct consumer channels. Majority of revenue comes from the sale of endpoint protection products through the service provider partner channel. F-Secure also sells consumer products through various retail partners, as well as F-Secure's own web shop. Partner channel sells F-Secure Total and Embedded Security products whereas direct channel sells F-Secure Total products.

F-Secure's cybersecurity products are sold as Security-as-a-Service. Customers are granted access to use the intellectual property during the license period and they are provided with access to continuously updated software. All software and the accompanied services F-Secure provides are highly interdependent and therefore treated as one performance obligation for which revenue is recognized over time on a straight-line basis for license period despite the sales channel.

Partner channel customers can have different invoicing depending on the customer agreement. Majority of the agreements are licenses fees – either F-Secure Total or Embedded Security – which are provided as a continuous service, when they are invoiced and revenue is recognized each month. Some agreements are for a fixed term, when they are invoiced e.g. annually upfront and revenue is recognized over time. Non-recurring revenue, which e.g. relates to custom built integration, is usually invoiced in the beginning of the agreement period and revenue is recognized over time on a straight-line basis for the contract period.

Direct channel selling F-Secure Total is usually invoiced fully upfront for the license period and the revenue is recognized over time on a straight-line basis for the license period. The typical length of a license period is 12, 24, or 36 months.

Generally, the term between invoicing and when payment is due is not significant.

Pensions

F-Secure's pension arrangements are defined contribution plans in accordance with local statutory requirements. Contributions to defined contribution plans are recognized in income statement in the period to which the contributions relate. The company recognizes the disability commitment of TyEL pension plan when disability appears.

Leases

Leases where the lessor retains substantially all the risks and benefits of ownership of the asset are classified as operating leases. Operating lease payments are recognized as an expense in the income statement on a straight-line basis over the lease term. The company has only operating leases.

Income taxes

Current income taxes are calculated in accordance with the local tax and accounting rules.

Tangible and intangible assets

Intangible assets include intangible rights and software licenses. Tangible and intangible assets are recorded at historical cost less accumulated depreciation, amortization, and possible impairment. Depreciation and amortization is recorded on a straight-line basis over the estimated useful life of an asset. The estimated useful lives of tangible and intangible assets are as follows:

Machinery and equipment	2–3 years
Capitalized development costs	3–5 years
Intangible rights	3–5 years
Intangible assets	3–15 years
Goodwill	10 years

Ordinary repairs and maintenance costs are charged to the income statement during the financial period in which they are incurred. The cost of major renovations is included in the assets' carrying amount when it is probable that the Company will derive future economic benefits in excess of the originally assessed standard or performance of the existing asset. Any gain or loss arising on derecognition of the asset (calculated as the difference between the net disposal proceeds and the carrying amount of the asset) is included in the income statement in the year the asset is derecognized.

Subsidiary shares

Subsidiary shares in the balance sheet are measured at historical cost less impairment losses. The carrying amounts of the subsidiary shares are assessed annually as part of the Group's impairment testing. An impairment loss is recognised, if the carrying amount of the subsidiary shares and the amount of net loan receivables from the subsidiary exceed the recoverable amount of the corresponding assets and the impairment is considered permanent.

Research and development expenditure

Research expenditure is recognized as an expense at the time it is incurred. Development expenditures relate to new products or development of significant new features including new product versions.

Inventories

Inventories are measured at the lower of cost and net realizable value. Cost is determined by first-in first-out method. Net realizable value is the estimated selling price that is obtainable, less estimated costs of completion and the estimated costs necessary to make the sale.

Financial assets and liabilities

Cash and cash equivalents and trade receivables are considered as financial assets. Cash and cash equivalents in the balance sheet comprise cash at bank, deposits held at banks, and other highly liquid short-term investment with original maturity less than 3 months.

F-Secure classifies bank loans, trade payables and other payables as other financial liabilities which are measured at amortized cost. Financial liabilities are classified as current unless F-Secure has unconditional right to postpone their repayment by at least 12 months from the end date of the reporting period.

Presentation of expenses

Classification of the functionally presented expenses has been made by presenting direct expenses in their respective functions.

1. Revenue

EUR 1,000	2024	2023
Geographical information		
Nordic countries	41,682	39,734
Rest of Europe	46,905	48,403
North America	29,278	19,070
Rest of the world	8,049	5,671
Total	**125,913**	**112,878**

2. Other operating income

EUR 1,000	2024	2023
Government grants	221	330
Transition services	515	426
Intercompany	1,437	2,036
Other	9	57
Total	**2,181**	**2,849**

Government grants are recognized as income over those periods in which the corresponding expenses arise.

3. Depreciation and amortization

EUR 1,000	2024	2023
Depreciation and amortization of non-current assets		
Other intangible assets	8,091	3,417
Goodwill	6,079	3,546
Capitalized development	2,650	2,098
Intangible assets	**16,821**	**9,062**
Machinery and equipment	33	27
Tangible assets	**33**	**27**
Total depreciation and amortization	**16,854**	**9,089**
Depreciation and amortization by function		
Sales and marketing	53	44
Research and development	3,726	2,221
Administration	13,075	6,824
Total depreciation and amortization	**16,854**	**9,089**

Amortization of goodwill and most of amortization of other intangible assets relate to acquisition of mobile consumer security business from Lookout Inc. See group Note 12. Acquisitions.

4. Personnel expenses

EUR 1,000	2024	2023
Personnel expenses		
Wages and salaries	16,011	18,128
Pension expenses	3,803	3,829
Other social expenses	524	754
Total	**20,337**	**22,711**

EUR 1,000	2024	2023
Compensation of key management personnel		
Wages and other short-term employee benefits	1,405	2,341
Total	**1,405**	**2,341**

EUR 1,000	2024	2023
Wages and other short-term employee benefits		
CEO and President	334	500
Members of the Board of Directors	267	270

Wages and other short-term employee benefits of the Board of Directors and CEO and President: see group Note 24. Related party disclosures.

The CEO's retirement age and the determination of his pension conform to the standard rules specified by Finland's Employee Pension Act (TYEL). The pension cost of the CEO during the financial period was 58 thousand euro (82 thousand euro). The period of notice for the CEO is six (6) months both ways and CEO is entitled to severance payment equivalent of six (6) months' salary.

	2024	2023
Average number of personnel	273	291
Personnel by function 31 Dec		
Sales and marketing	68	81
Research and development	165	185
Administration	35	33
Total	**268**	**299**

Previously separately reported function Delivery is merged to Sales and marketing function in connection with the change in calculation method for gross margin. Comparison period is also revised.

5. Audit fees

EUR 1,000	2024	2023
Audit fees, PricewaterhouseCoopers	148	187
Audit related fees, PricewaterhouseCoopers	21	
Tax consulting, PricewaterhouseCoopers	11	
Other consulting, PricewaterhouseCoopers	126	1,233
Total	**306**	**1,420**

Other consulting includes, among others sustainability advisory and CSRD assurance.

6. Financial income and expenses

EUR 1,000	2024	2023
Interest income	442	378
Interest expense	-10,657	-8,675
Other financial income		86
Dividends	6,169	1,108
Exchange gains and losses	73	4,929
Other financial expenses	-443	-315
Total	**-4,417**	**-2,488**

7. Appropriations

EUR 1,000	2024	2023
Change in depreciation difference	-2,726	-7,566
Total	**-2,726**	**-7,566**

8. Income taxes

EUR 1,000	2024	2023
Income tax for the year	-2,488	-2,535
Total	**-2,488**	**-2,535**
Result before appropriations and tax	**21,754**	**21,667**

9. Non-current assets

	Intangible assets						Tangible assets		
EUR 1,000	Other intangible	Goodwill	Capitalized development	Incomplete development	Advance payments	Total	Machinery & equip.	Other tangible	Total
Acquisition cost Dec 31, 2022	588		7,162	1,441	548	9,739	37	33	69
Additions	87,438	60,791		1,917	5708	155,853	39	18	57
Transfers	1,544		1,917	-3,357	-103				
Acquisition cost Dec 31, 2023	89,570	60,791	9,079	-	6,152	165,592	76	50	126
Additions	1,725			9,172	1,813	12,710	20	2	22
Transfers	7,237		8,425	-8,425	-7,237				
Acquisition cost Dec 31, 2024	**98,533**	**60,791**	**17,504**	**747**	**728**	**178,302**	**96**	**52**	**148**
Acc. depreciation Dec 31, 2022			-675			-675	-5	-4	-9
Depreciation for the period	-3,395	-3,546	-2,098			-9,040	-27	-22	-49
Acc. depreciation Dec 31, 2023	-3,395	-3,546	-2,773	-	-	-9,715	-32	-26	-58
Depreciation for the period	-8,070	-6,079	-2,650			-16,800	-33	-21	-54
Acc. depreciation Dec 30, 2024	**-11,466**	**-9,625**	**-5,424**	-	-	**-26,515**	**-65**	**-47**	**-112**
Book value as at Dec 31, 2023	86,175	57,244	6,305	-	6,152	155,877	45	24	69
Book value as at Dec 31, 2024	**87,067**	**51,165**	**12,080**	**747**	**728**	**151,788**	**32**	**4**	**36**

Goodwill and most of other intangible assets additions relate to acquisition of mobile consumer security business from Lookout Inc. See group note 12. Acquisitions.

10. Investments in group companies

EUR 1,000	Shares in group companies	Total
Book value as at Jan 1	66,821	66,821
Additions	456	456
Decreases	-3,446	-3,446
Book value as at Dec 31	**63,831**	**63,831**

Name	Country of incorporation	Share of ownership (%)
Parent F-Secure Corporation, Helsinki	Finland	100
F-Secure Data Oy, Helsinki	Finland	100
F-Secure Inc., Palo Alto	United States	100
F-Secure (UK) Ltd, Buckinghamshire	United Kingdom	100
F-Secure GmbH, Munich	Germany	100
F-Secure Pvt Ltd, Mumbai	India	100
F-Secure Iberia SL, Barcelona	Spain	100
F-Secure s.r.o, Bratislava	Slovakia	100

11. Inventories

EUR 1,000	2024	2023
Other inventories	29	35

12. Receivables

EUR 1,000	2024	2023
Non-Current receivables		
Other financial assets	36	-
Total	**36**	
Current receivables		
Trade receivables	17,515	18,001
Income tax receivable	677	1,174
Other receivables	1,156	325
Prepaid expenses and accrued income	9,021	6,885
Total	**28,369**	**26,386**
Receivables from group companies		
Trade receivables	779	5,063
Other receivables	345	1,206
Total	**1,124**	**6,269**
Current receivables total	**29,493**	**32,655**

Material items included in prepaid expenses and accrued income		
Prepaid royalty	918	879
Grant receivables	192	382
Other prepaid expenses	6,552	4,564
Accrued income	1,359	1,060
Total	**9,021**	**6,885**

13. Cash and short-term deposits

EUR 1,000	2024	2023
Cash at bank and in hand	5,395	12,935

14. Statement of changes in shareholders' equity

EUR 1,000	Share capital	Unrestricted equity reserve	Retained Earnings	Total Equity
Equity 31 December 2022	**80**	**9,590**	**13,285**	**22,956**
Result of the financial year			11,566	11,566
Dividends paid			-12,227	-12,227
Equity 31 December 2023	**80**	**9,590**	**12,624**	**22,294**
Result of the financial year			16,539	16,539
Dividends paid			-12,227	-12,227
Equity 31 December 2024	**80**	**9,590**	**16,936**	**26,607**

15. Shareholders' equity

Issued and fully paid

EUR 1,000	Number of shares	Share capital	Unrestricted equity reserve
1 January 2024	174,673,165	80	9,590
31 December 2024	**174,673,165**	**80**	**9,590**

The share capital amounted to 80,000 euro was formed in the demerger on 30 June 2022. The number of shares was 174,673,165 (no own shares) at the end of 2024.

Company has made two directed share issues in March 2023 to the plan participants of the company's Performance Share Plan and Restricted Share plan. The shared issued account for the rewards earned from the performance period 2020–2022 and retention period 2021–2022.

A share has no nominal value. Accountable par value is EUR 0.01.

Distributable shareholders' equity on 31 December 2024

EUR 1,000	
Unrestricted equity reserve	9,590
Retained earnings	397
Result of the financial year	16,539
Less capitalized development expense	-12,827
Distributable shareholders' equity on 31 December 2024	**13,700**

16. Share-based payment transactions

See group Note 19. Share-based payment transactions.

17. Liabilities

EUR 1,000	2024	2023
Non-current liabilities		
Deferred revenue	4,952	5,715
Bank loans	132,000	162,000
Total	**136,952**	**167,715**
Liabilities to the group companies		
Cash pool	811	1,356
Total	**811**	**1,356**
Total non-current liabilities	**137,763**	**169,071**
Current liabilities		
Deferred revenue	18,617	15,544
Trade payables	1,512	3,863
Bank loans	38,000	30,000
Provision		200
Other liabilities	876	654
Accrued expenses	9,666	8,062
Total	**68,671**	**58,324**
Liabilities to the group companies		
Trade payables	2,189	1,118
Other liabilities	5,087	10,017
Total	**7,276**	**11,136**
Total current liabilities	**75,947**	**69,459**

EUR 1,000	2024	2023
Material amounts shown under accruals and deferred income		
Accrued personnel expenses	5,826	4,278
Restructuring	685	1,108
Accrued expenses	3,155	2,675
Total	**9,666**	**8,062**

18. Financial risk management

See group Note 21. Financial risk management.

19. Operating lease commitments

The Group has commercial leases on office space and on motor vehicles. Leases have an average life of two to three years with renewal terms included in the contracts.

In the second quarter of 2024, F-Secure signed a new lease agreement for headquarter office premises and the lease commitment already exists following the agreement. The four-year contract value is EUR 5.1 million.

Future minimum rentals payable under non-cancellable operating leases as at 31 December are as follows:

EUR 1,000	2024	2023
As lessee		
Within one year	940	922
After one year but not more than five years	5,042	85
Total	**5,982**	**1,007**

Signatures of the Board of Directors' report and Financial statements

The financial statements, prepared in accordance with the applicable accounting regulations, give a true and fair view of both the company and the group of companies included in its consolidated financial statements, in terms of assets, liabilities, financial position, and profit and loss.

The management report provides an accurate description of the development and results of the company's operations on one hand, and the business development and results of the group of companies included in the consolidated financial statements on the other. It also includes a description of significant risks, uncertainties, and other aspects of the company's state. Additionally, the sustainability report included in the management report has been prepared in accordance with the reporting standards referred to in Chapter 7 and Article 8 of the Taxonomy Regulation.

Helsinki, 25 February 2025

Pertti Ervi
Chair

Risto Siilasmaa

Tommi Uitto

Thomas Jul

Petra Teräsaho

Katja Kuusikumpu

TImo Laaksonen
CEO and President

Auditors' note

Our auditors' report has been issued today.

Helsinki, 26 February 2025

PricewaterhouseCoopers Oy
Authorized Public Accountants

Samuli Perälä
Authorized Public Accountant

Information for shareholders



Contact information:

Sari Somerkallio, Chief Financial Officer

investor.relations@f-secure.com
+358 40 356 9251

Financial calendar

During the year 2025, F-Secure Corporation will publish financial information as follows:

- Interim Report for January–March 2025 on Friday 27 April 2025
- Half-year Financial Report for January–June 2025 on Thursday 18 July 2025
- Interim Report for January–September 2025 on Thursday 28 October 2025

Annual General Meeting 2025

The Annual General Meeting of F-Secure Corporation is planned to be held on 1 April 2025.

Auditor's report

(Translation of the Finnish Original)

To the Annual General Meeting of F-Secure Corporation

Report on the Audit of the Financial Statements

Opinion

In our opinion

- the consolidated financial statements give a true and fair view of the group's financial position, financial performance and cash flows in accordance with IFRS Accounting Standards as adopted by the EU
- the financial statements give a true and fair view of the parent company's financial performance and financial position in accordance with the laws and regulations governing the preparation of financial statements in Finland and comply with statutory requirements.

Our opinion is consistent with the additional report to the Audit Committee.

What we have audited

We have audited the financial statements of F-Secure Corporation (business identity code 3269349-7) for the year ended 31 December 2024. The financial statements comprise:

- the consolidated balance sheet, statement of comprehensive income, statement of changes in equity, statement of cash flows and notes, which include material accounting policy information and other explanatory information
- the parent company's balance sheet, income statement, cash flow statement and notes to the parent company Financial Statements.

Basis for Opinion

We conducted our audit in accordance with good auditing practice in Finland. Our responsibilities under good auditing practice are further described in the Auditor's Responsibilities for the Audit of the Financial Statements section of our report.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Independence

We are independent of the parent company and of the group companies in accordance with the ethical requirements that are applicable in Finland and are relevant to our audit, and we have fulfilled our other ethical responsibilities in accordance with these requirements.

To the best of our knowledge and belief, the non-audit services that we have provided to the parent company and group companies are in accordance with the applicable law and regulations in Finland and we have not provided non-audit services that are prohibited under Article 5(1) of Regulation (EU) No 537/2014. The non-audit services that we have provided are disclosed in note 8 to the Financial Statements.

Our Audit Approach

Overview



- Overall group materiality: 1.3 million euros.
- The audit of the consolidated financial statements covered the parent company and one subsidiary.
- Valuation of goodwill and intangible assets acquired in connection with the business combination
- Revenue recognition

As part of designing our audit, we determined materiality and assessed the risks of material misstatement in the financial statements. In particular, we considered where management made subjective judgements; for example, in respect of significant accounting estimates that involved making assumptions and considering future events that are inherently uncertain.

Materiality

The scope of our audit was influenced by our application of materiality. An audit is designed to obtain reasonable assurance whether the financial statements are free from material misstatement. Misstatements may arise due to fraud or error. They are considered material if individually or in aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

Based on our professional judgement, we determined certain quantitative thresholds for materiality, including the overall group materiality for the consolidated financial statements as set out in the table below. These, together with qualitative considerations, helped us to determine the scope of our audit and the nature, timing and extent of our audit procedures and to evaluate the effect of misstatements on the financial statements as a whole.

Overall group materiality	1.3 million euros
How we determined it	The materiality of the consolidated financial statements has been determined based on the profit before tax for the financial year.
Rationale for the materiality benchmark applied	We chose profit before tax as the benchmark because, in our view, it is relevant benchmark to describe the volume and profitability of the Group's operations.

How we tailored our group audit scope

We tailored the scope of our audit, taking into account the structure of the F-Secure group, the accounting processes and controls, and the industry in which the group operates.

The audit of the consolidated financial statements covered the parent company and one subsidiary. In our view, we have determined the scope of the audit of the consolidated financial statements to cover the consolidated financial statements to a sufficient extent.

Key Audit Matters

Key audit matters are those matters that, in our professional judgment, were of most significance in our audit of the financial statements of the current period. These matters were addressed in the context of our audit of the financial statements as a whole, and in forming our opinion thereon, and we do not provide a separate opinion on these matters.

As in all of our audits, we also addressed the risk of management override of internal controls, including among other matters consideration of whether there was evidence of bias that represented a risk of material misstatement due to fraud.

Key audit matter in the audit of the group	How our audit addressed the key audit matter
Valuation of goodwill and intangible assets acquired in connection with the business combination *Relevant information is presented in notes 1, 12, 13, and 14.*	
The consolidated balance sheet had a total of 89.8 million euros in goodwill as of December 31, 2024. Goodwill is not amortized but is tested annually, or more frequently if there are indications that its value might be impaired. Other intangible assets acquired in business combinations are recorded at fair value at the time of acquisition and expensed through amortization over their economic useful life. For impairment testing, goodwill is allocated to a single cash-generating unit. In the impairment test, the recoverable amount of the cash-generating unit is determined based on the present value of estimated future cash flows. Management's estimates are used to determine the present value of the forecasted cash flows. Due to the management judgment involved in valuation and the materiality of the balance sheet value, the valuation of goodwill and intangible assets acquired in connection with business combinations is a key audit matter.	Our audit procedures included, among others, the following actions: • We obtained an understanding of the methods and assumptions used in the impairment testing of goodwill, • We assessed the reasonableness and consistency of the forecasted profitability levels against approved budgets and forecasts, • We tested the mathematical accuracy of the calculations, • We evaluated the discount rates used, long-term growth forecasts, and certain other assumptions, for example, by comparing these input data to observable market information, • We assessed the adequacy of the information provided in the financial statements.

Key audit matter in the audit of the group	How our audit addressed the key audit matter
Revenue recognition *Relevant information is presented in notes 1 and 3*	
The majority of F-Secure's revenue is generated from the sale of endpoint security solutions through the partner channel, but the group also sells consumer products through resellers and F-Secure's own online store. Customers are typically granted a license to use the software for a license period and are provided access to continuously updated software. The software and accompanying services are closely related, and therefore they are treated as a single performance obligation, with revenue being recognized primarily evenly over the license period as time passes. Revenue recognition has been considered a key audit matter due to the large number of transactions and the fact that revenue is a critical measure of the company's financial performance.	Our audit procedures have included, among others, the following actions: • We assessed the adequacy of controls related to the revenue process, • We tested, on sample basis, the revenue recorded during the financial year, • We tested, on sample basis, trade receivables, • We checked the appropriateness of the of received advances on sample basis, • We examined a sample of the revenue recognition of fixed-price contracts.

We have no key audit matters to report with respect to our audit of the parent company financial statements.

There are no significant risks of material misstatement referred to in Article 10(2c) of Regulation (EU) No 537/2014 with respect to the consolidated financial statements or the parent company financial statements.

Responsibilities of the Board of Directors and the Managing Director for the Financial Statements

The Board of Directors and the Managing Director are responsible for the preparation of consolidated financial statements that give a true and fair view in accordance with IFRS Accounting Standards as adopted by the EU, and of financial statements that give a true and fair view in accordance with the laws and regulations governing the preparation of financial statements in Finland and comply with statutory requirements. The Board of Directors and the Managing Director are also responsible for such internal control as they determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the Board of Directors and the Managing Director are responsible for assessing the parent company's and the group's ability to continue as a going concern, disclosing, as applicable, matters relating to going concern and using the going concern basis of accounting. The financial statements are prepared using the going concern basis of accounting unless there is an intention to liquidate the parent company or the group or to cease operations, or there is no realistic alternative but to do so.

Auditor's Responsibilities for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with good auditing practice will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with good auditing practice, we exercise professional judgment and maintain professional skepticism throughout the audit. We also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the parent company's or the group's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.
- Conclude on the appropriateness of the Board of Directors' and the Managing Director's use of the going concern basis of accounting and based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the parent company's or the group's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the parent company or the group to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events so that the financial statements give a true and fair view.
- Plan and perform the group audit to obtain sufficient appropriate audit evidence regarding the financial information of the entities or business units within the group as a basis for forming an opinion on the group financial statements. We are responsible for the direction, supervision and review of the audit work performed for purposes of the group audit. We remain solely responsible for our audit opinion.

We communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

We also provide those charged with governance with a statement that we have complied with relevant ethical requirements regarding independence, and to communicate with them all relationships and other matters that may reasonably be thought to bear on our independence, and where applicable, related safeguards.

From the matters communicated with those charged with governance, we determine those matters that were of most significance in the audit of the financial statements of the current period and are therefore the key audit matters. We describe these matters in our auditor's report unless law or regulation precludes public disclosure about the matter or when, in extremely rare circumstances, we determine that a matter should not be communicated in our report because the adverse consequences of doing so would reasonably be expected to outweigh the public interest benefits of such communication.

Other Reporting Requirements

Appointment

We were first appointed as auditors by the annual general meeting on 31 May 2022.

Other Information

The Board of Directors and the Managing Director are responsible for the other information. The other information comprises the report of the Board of Directors and the information included in the Annual Report but does not include the financial statements or our auditor's report thereon.

Our opinion on the financial statements does not cover the other information.

In connection with our audit of the financial statements, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or our knowledge obtained in the audit, or otherwise appears to be materially misstated. With respect to the report of the Board of Directors, our responsibility also includes considering whether the report of the Board of Directors has been prepared in compliance with the applicable provisions, excluding the sustainability report information on which there are provisions in Chapter 7 of the Accounting Act and in the sustainability reporting standards.

In our opinion, the information in the report of the Board of Directors is consistent with the information in the financial statements and the report of the Board of Directors has been prepared in compliance with the applicable provisions. Our opinion does not cover the sustainability report information on which there are provisions in Chapter 7 of the Accounting Act and in the sustainability reporting standards.

If, based on the work we have performed, we conclude that there is a material misstatement of the other information, we are required to report that fact. We have nothing to report in this regard.

Helsinki 26 February 2025

PricewaterhouseCoopers Oy

Authorized Public Accountants

Samuli Perälä

Authorised Public Accountant (KHT)

Assurance Report on the Sustainability Report

(Translation of the Finnish Original)

To the Annual General Meeting of F-Secure Oyj

We have performed a limited assurance engagement on the group sustainability report of F-Secure Oyj (business identity code 3269349-7) that is referred to in Chapter 7 of the Accounting Act and that is included in the report of the Board of Directors for the reporting period 1.1.–31.12.2024.

Opinion

Based on the procedures we have performed and the evidence we have obtained, nothing has come to our attention that causes us to believe that the group sustainability report does not comply, in all material respects, with

1. the requirements laid down in Chapter 7 of the Accounting Act and the sustainability reporting standards (ESRS);
2. the requirements laid down in Article 8 of the Regulation (EU) 2020/852 of the European Parliament and of the Council on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088 (EU Taxonomy).

Point 1 above also contains the process in which F-Secure Oyj has identified the information for reporting in accordance with the sustainability reporting standards (double materiality assessment).

Our opinion does not cover the tagging of the group sustainability report in accordance with Chapter 7, Section 22, of the Accounting Act, because sustainability reporting companies have not had the possibility to comply with that requirement in the absence of the ESEF regulation or other European Union legislation.

Basis for Opinion

We performed the assurance of the group sustainability report as a limited assurance engagement in compliance with good assurance practice in Finland and with the International Standard on Assurance Engagements (ISAE) 3000 (Revised) *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*.

Our responsibilities under this standard are further described in the Responsibilities of the Authorised Group Sustainability Auditor section of our report.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Authorised Group Sustainability Auditor's Independence and Quality Management

We are independent of the parent company and of the group companies in accordance with the ethical requirements that are applicable in Finland and are relevant to our engagement, and we have fulfilled our other ethical responsibilities in accordance with these requirements.

Our firm applies International Standard on Quality Management ISQM 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Responsibilities of the Board of Directors and the Managing Director

The Board of Directors and the Managing Director of F-Secure Oyj are responsible for:

- the group sustainability report and for its preparation and presentation in accordance with the provisions of Chapter 7 of the Accounting Act, including the process that has been defined in the sustainability reporting standards and in which the information for reporting in accordance with the sustainability reporting standards has been identified
- the compliance of the group sustainability report with the requirements laid down in Article 8 of the Regulation (EU) 2020/852 of the European Parliament and of the

Council on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088;

such internal control as the Board of Directors and the Managing Director determine is necessary to enable the preparation of a group sustainability report that is free from material misstatement, whether due to fraud or error.

Inherent Limitations in the Preparation of a Sustainability Report

In reporting forward-looking information in accordance with ESRS, management of the Company is required to prepare the forward-looking information on the basis of assumptions that have been disclosed in the sustainability report about events that may occur in the future and possible future actions by the Group. Actual outcomes are likely to be different since anticipated events frequently do not occur as expected.

Responsibilities of the Authorised Group Sustainability Auditor

Our responsibility is to perform an assurance engagement to obtain limited assurance about whether the group sustainability report is free from material misstatement, whether due to fraud or error, and to issue a limited assurance report that includes our opinion. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the decisions of users taken on the basis of the group sustainability report.

Compliance with the International Standard on Assurance Engagements (ISAE) 3000 (Revised) requires that we exercise professional judgment and maintain professional skepticism throughout the engagement. We also:

- Identify and assess the risks of material misstatement of the group sustainability report, whether due to fraud or error, and obtain an understanding of internal control relevant to the engagement in order to design assurance procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the parent company's or the group's internal control.

Design and perform assurance procedures responsive to those risks to obtain evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.

Description of the Procedures That Have Been Performed

The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement. The nature, timing and extent of assurance procedures selected depend on professional judgment, including the assessment of risks of material misstatement, whether due to fraud or error. Consequently, the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed.

Our procedures included for example the following:

- We interviewed the company's management and the individuals responsible for collecting and reporting the information contained in the group sustainability report at the group level as well as at different levels and business areas of the organization to gain an understanding of the sustainability reporting process and the related internal controls and information systems.
- We familiarised ourselves with the background documentation and records prepared by the company where applicable, and assessed whether they support the information contained in the group sustainability report.
- We assessed the company's double materiality assessment process in relation to the requirements of the ESRS standards, as well as whether the information provided about the assessment process complies with the ESRS standards.
- We assessed whether the sustainability information contained in the group sustainability report complies with the ESRS standards.

Regarding the EU taxonomy information, we gained an understanding of the process by which the company has identified the group's taxonomy-eligible and taxonomy-aligned economic activities, and we assessed the compliance of the information provided with the regulations.

Helsinki 26 February 2025

PricewaterhouseCoopers Oy
Authorised Sustainability Auditors

Samuli Perälä

Authorised Sustainability Auditor

Independent Auditor's Reasonable Assurance Report on F-Secure Oyj's ESEF Financial Statements

(Translation of the Finnish Original)

To the Management of F-Secure Oyj

We have been engaged by the Management of F-Secure Oyj (business identity code 3269349-7) (hereinafter also "the Company") to perform a reasonable assurance engagement on the Company's consolidated IFRS financial statements for the financial year 01 January - 31 December 2024 in European Single Electronic Format ("ESEF financial statements") version 9845006BFDJF0375E466-2024-12-31-fi.zip.

Management's Responsibility for the ESEF Financial Statements

The Management of F-Secure Oyj is responsible for preparing the ESEF financial statements so that they comply with the requirements as specified in the Commission Delegated Regulation (EU) 2019/815 of 17 December 2018 ("ESEF requirements"). This responsibility includes the design, implementation and maintenance of internal control relevant to the preparation of ESEF financial statements that are free from material noncompliance with the ESEF requirements, whether due to fraud or error.

Our Independence and Quality Management

We have complied with the independence and other ethical requirements of the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. Our firm applies International Standard on Quality Management 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Our Responsibility

Our responsibility is to express an opinion on the ESEF financial statements based on the procedures we have performed and the evidence we have obtained.

We conducted our reasonable assurance engagement in accordance with the International Standard on Assurance Engagements (ISAE) 3000 (Revised) *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*. That standard requires that we plan and perform this engagement to obtain reasonable assurance about whether the ESEF financial statements are free from material noncompliance with the ESEF requirements.

A reasonable assurance engagement in accordance with ISAE 3000 (Revised) involves performing procedures to obtain evidence about the ESEF financial statements compliance with the ESEF requirements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material noncompliance of the ESEF financial statements with the ESEF requirements, whether due to fraud or error. In making those risk assessments, we considered internal control relevant to the Company's preparation of the ESEF financial statements.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Opinion

In our opinion, F-Secure Oyj's ESEF financial statements for the financial year ended 31 December 2024 comply, in all material respects, with the minimum requirements as set out in the ESEF requirements.

Our reasonable assurance report has been prepared in accordance with the terms of our engagement. We do not accept, or assume responsibility to anyone else, except for F-Secure Oyj for our work, for this report, or for the opinion that we have formed.

Helsinki 26 February 2024

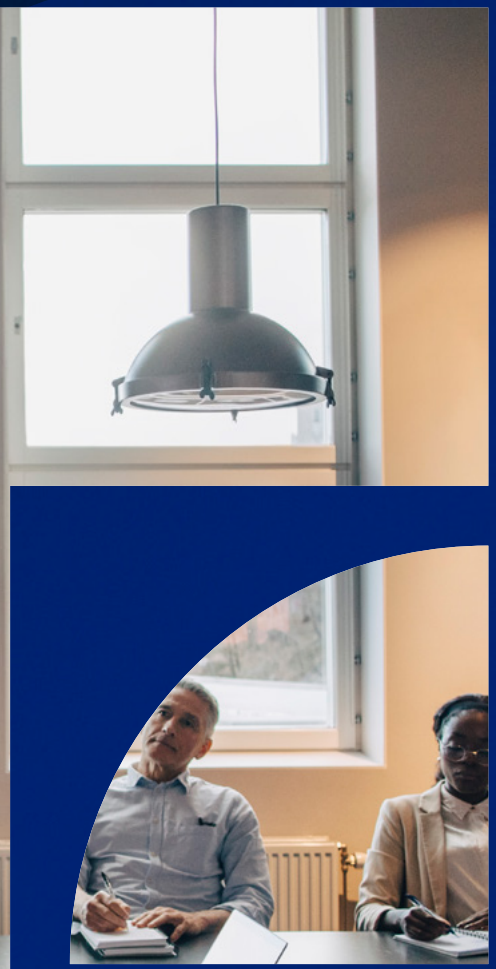
PricewaterhouseCoopers Oy
Authorised Public Accountants

Samuli Perälä

Authorised Public Accountant (KHT)

Corporate Governance





F-Secure Corporate Governance Statement



Corporate Governance at F-Secure

F-Secure corporate governance practices are based on applicable Finnish laws, the rules of Helsinki Stock Exchange (Nasdaq Helsinki Oy) and the regulations and guidelines of Finnish Financial Supervisory Authority as well as with the company's Articles of Association. This corporate governance statement (later simply referred to as 'statement') has been prepared in accordance with the Finnish Corporate Governance Code 2025 (publicly available at http://cgfinland.fi/en/) issued by the Securities Market Association of Finland.

Up-to-date information about F-Secure corporate governance is available on the company's investor website at https://investors.f-secure.com/en. This statement is issued separately from the Board of Directors' report, and is also available on the investor website, as well as is included in the 2024 Annual Report.

Governing bodies

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 Corporation and appropriate organization of its operations. 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.

General Meeting of Shareholders

Under the Finnish Companies Act, shareholders exercise their decision-making power at the General Meeting.

The General Meeting is normally held once a year as an Annual General Meeting (AGM). The AGM decides on matters stipulated by the Articles of Association and the Finnish Companies Act, including:

- adoption of the Financial Statements
- distribution of profit for the year
- discharging the members of the Board of Directors and the President and CEO from liability
- selection of members of the Board
- the decision on the remuneration of the Board members
- approval of the Remuneration Policy and the Remuneration Report
- election of the auditor and the decision on the auditor's remuneration, and
- other proposals submitted to General Meeting

Each share carries one vote in the General Meeting.

A shareholder may propose items to be included on the agenda provided they are within the authority of the General Meeting, and the Board of Directors has received the request in advance in accordance with the set schedule. The invitation to the AGM is published as a stock exchange release and is made available on the company's website.

2024:

In 2024, the Annual General Meeting of the company was held on 13 March 2024 at the company's headquarters in Helsinki, Finland.

Board of Directors

The Board of Directors is responsible for the administration of F-Secure Corporation and appropriate organization of its operations. The Board's operations, responsibilities and duties are based on the Finnish Companies Act and other applicable legislation and are supplemented by the Board Charter. These cover the following main areas:

- approving the strategy of F-Secure, overseeing its operations and annual budgets
- appointing and dismissing the President and CEO and the Chair of the Board
- approving any major investments, acquisitions, changes in corporate structure or other matters that are significant or far-reaching
- ensuring that the supervision of the company's accounting and financial management is duly organized
- ensuring that internal control and risk management systems are in place
- approving personnel policies and rewards systems
- preparing most matters to be handled at the General Meeting

The Board of Directors meets as frequently as necessary and according to the Board Charter at least five times during its term. The Board of Directors has quorum when more than half of the members are present. An annual self-assessment is carried out by the Board to evaluate its operations. The Board of Directors primarily strives at unanimous decisions. If a decision cannot be made unanimously, the decision will be made by voting and with single majority. If the votes are even, the Chair's vote is decisive.

In accordance with F-Secure's Articles of Association, the Board of Directors comprises three to seven members, who are elected at the Annual General Meeting for a period of office that extends to the end of subsequent AGM. The Board of Directors represents all shareholders.

Diversity is an essential part of F-Secure success. 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 creation of long-term shareholder value. The Diversity Principles of the Board of Directors aim to strive 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 and two Board members are female and four are male, and thus the underrepresented gender comprises 33.3% of all members of the Board. The Board members have international experience in different roles in global companies operating in different businesses and geographical market areas. More information on the educational and professional background of the Board members is available on chapter Board of Directors 31 December 2024 (see pages 204-211) of the Annual Report 2024.

To create openness, one member of the Board of Directors is proposed to be elected from among F-Secure personnel. An election is arranged annually for F-Secure personnel and each permanent F-Secure employee, except the people belonging to the company's Leadership Team, is eligible to stand as a candidate. The representatives of the Board of Directors interview three 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. Katja Kuusikumpu was appointed to the Board of Directors from among the employees in 2024.

As an employee of the company, the Board member elected from among F-Secure personnel does not participate in any matters that relate to, for example, leadership appointment (or dismissal), remuneration or other terms of employment or service, or industrial action, as the Board may handle from time to time. Board member who is appointed to the Board from among the employees serves on the Board for a period of one year, until the end of next year's Annual General Meeting.

The majority of Board members are independent from the company and from its major shareholders. For a detailed description of the members of the Board of Directors and their shareholdings see the end of this statement.

2024:

In 2024, the Board of Directors held 20 meetings, 9 of which were held without convening. Audit Committee convened 5 times. Personnel and Nomination Committee convened 5 times.

Board of Directors and the Committee members' attendance at meetings in 2024

Members	Independence of the company	Independence of major shareholders	Board of Directors (meeting attendance)	Audit Committee (meeting attendance)	Personnel and Nomination Committee (meeting attendance)
Pertti Ervi	Yes	Yes	Chair (20/20)	Member (5/5)	Chair (5/5)
Petra Teräsaho	Yes	Yes	Member (20/20)	Chair (5/5)	
Thomas Jul	Yes	Yes	Member (20/20)		Member (5/5)
Katja Kuusikumpu	No[1]	Yes	Member (14/16)[2]		
Madeleine Lassoued	Yes	Yes	Member (4/4)[4]		
Sami Salonen	No[1]	Yes	Member (4/4)		
Risto Siilasmaa	Yes	No[3]	Member (19/20)	Member (4/5)	Member (5/5)
Tommi Uitto	Yes	Yes	Member (16/16)[4]		

1) Katja Kuusikumpu was elected from among F-Secure personnel, according to the process described above in 2024. In addition, Sami Salonen who had been appointed to the Board in 2023 served on the Board until the end of 204 Annual General Meeting.

2) Excused from two meetings as employee Board member.

3) Risto Siilasmaa is the founder of F-Secure and on 31 December 2024 owned 34.37% of F-Secure shares.

4) Madeleine Lassoued served on the Board until the end of 2024 Annual General Meeting and Tommi Uitto has been serving on the Board since the 2024 Annual General Meeting.

Board Committees

The Board of Directors appoints from among itself the members and the Chairs of the committees. Each committee must have at least three members. The Board of Directors confirms the main duties and operating principles of each committee.

Audit 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, financial and sustainability reporting as well as auditing and sustainability auditing. The Audit Committee also prepares a proposal for the election of an auditor to the Board of Directors and regularly considers the need for a separate internal audit function. Members of the Audit Committee must have broad business knowledge, as well as sufficient expertise and experience with respect to the committee's area of responsibility and the mandatory tasks relating to 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. 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. Minutes of the Audit Committee meetings are made available for all members of the Board of Directors.

The Audit Committee convenes at least four (4) times a year as notified by the Chair of the Committee. Members of the Audit Committee are listed in the table above.

Personnel and Nomination Committee

The Board of Directors has in 2024 established a Personnel and Nomination Committee. The Personnel and Nomination Committee prepares material and instructs with 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 to the General Meeting of Shareholders related to these matters.

The majority of the members of the Personnel and Nomination Committee shall be independent of the company. The Committee calls in experts to its meetings when necessary for the issues to be discussed. Minutes of the Personnel and Nomination Committee meetings are made available for all members of the Board of Directors.

The Personnel and Nomination Committee convenes at least two times a year as notified by the Chair of the

Committee. Members of the Committee are listed in the table above.

President and CEO

The Board of Directors appoints and may dismiss the President and CEO and decides upon the President and CEO's remuneration and other benefits in accordance with the Remuneration Policy. The CEO is responsible for the day-to-day management of the company. The CEO's main duties include:

- managing the business according to the instructions issued by the Board of Directors
- presenting the matters to be handled in the Board of Directors' meetings
- implementing the decisions made by the Board of Directors
- other duties determined in the Finnish Companies Act

2024:

Timo Laaksonen has been F-Secure President and CEO since 30 June 2022.

The biographical details of the President and CEO including the President and CEO's shareholdings are specified at the end of this statement. The remuneration of the President and CEO is specified in F-Secure Remuneration Policy and Report.

Leadership Team

The Leadership Team supports the President and CEO in the daily operative management of the company.

2024:

Current information on the F-Secure Leadership Team can be found on our website: https://investors.f-secure. com/en/investors/ corporate_governance/ leadership_team.

For descriptions of all members of the Leadership Team during 2024 and their roles, respective membership periods and shareholdings, see the end of this statement.

Internal control and risk management

Risk management

Risk management and internal control processes at F-Secure seek to ensure that risks related to the business operations of the company are properly identified, evaluated, monitored, mitigated and reported in compliance with the applicable regulations.

F-Secure Board of Directors defines the principles of risk management and internal controls which are followed within the company. The Audit Committee assists the Board in the supervision of F-Secure risk management process. The President and CEO is accountable for ensuring that the risk management principles are implemented and applied constantly and consistently across the organization, supported by the Corporate Development function.

The primary goal of F-Secure risk management principles is to empower the organization to identify and manage risks more effectively. The potential negative impact and probability of different situations arising from business operations of the company, its markets, its customers, or its partners are monitored as part of the risk management process.

F-Secure promotes continuous risk evaluation 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 and the Leadership Team, and the Audit Committee. Company's statutory auditor reviews risks part of each interim release (quarterly). 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. The Audit Committee regularly evaluates the effectiveness of the risk management system.

Internal control

The purpose of Internal Control is to ensure that operations are effective and aligned with the strategy, and that financial reporting and management information is reliable and in compliance with applicable regulations and operating principles.

Internal control consists of all the guidelines, policies, processes, practices and relevant information about organizational structure that help ensure that the business conduct is in compliance with all applicable regulations. The purpose of internal control is also to ensure that accounting and financial information provides a true and accurate reflection of the activities and financial situation of the company.

The company constantly monitors its key financial processes linked to sales, revenue, costs and profitability as well as incoming and outgoing payment transactions. If any inconsistencies appear, the issues are handled without delay. The company's finance department is responsible for the consistency and reliability of internal control methods. The finance team, led by the CFO, works in close cooperation with businesses, providing relevant data for business planning purposes and sales estimates. The team also regularly assesses and monitors the reliability of estimates and revenue recognition.

Internal audit

Audit Committee considers the need for and appropriateness of a separate Internal Audit function on a regular basis. To date, the Audit Committee has concluded that, due to the size, organizational structure and largely centrally controlled financial management of the company, a separate Internal Audit function is not necessary.

In the absence of an Internal Audit function, attention is paid to periodical review of the written guidelines and policies concerning accounting, reporting, documentation, authorization, risk management, internal control and other relevant matters across the company. Related controls are also tested from time to time. The guidelines and policies are coordinated by the company's finance team with active involvement by the legal team.

The absence of a separate Internal Audit function is considered when defining the scope of the company's external audit. Where necessary, the Internal Audit services will be purchased from an external service provider.

To facilitate transparency and exchange of information on Internal Audit related matters, the financial management team has frequent meetings with the auditors. The auditors also participate in the meetings of the Audit Committee as permanent invitees.

The company has taken into use a Whistleblowing Channel for employees and other stakeholders to report any possibly corrupt, illegal, or other undesirable conduct.

Related party transactions

The Audit Committee defines the principles for monitoring and assessing F-Secure related party transactions. The definition of the related parties is based on IAS 24 standard. F-Secure collects information about its related parties on regular basis. The Board of Directors decides on related party transactions that are not conducted in the ordinary course of business of the company or are not implemented under arm's-length terms. Related party transactions are disclosed as part of financial statements according to the applicable legislation.

Insider management

F-Secure complies with the applicable legislation, including EU Market Abuse Regulation (MAR), the regulations of the Finnish Financial Supervisory Authority as well as Nasdaq Helsinki's Guidelines for Insiders. F-Secure has established its own insider policy to complement the regulation and guidelines above.

F-Secure maintains a list of all persons who have regular access to company's financial data. Due to the sensitive nature of financial information, persons having access to financial information before publication of an interim financial report or a year-end report shall be subject to a thirty (30) day trading restriction prior to publication of such report.

In addition, F-Secure maintains a project-specific insider list of any projects and events which, if realized, would be likely to have a significant effect on the value of F-Secure share or other financial instruments, and which have been subject to delaying of disclosure in accordance with MAR.

F-Secure has decided not to include any persons as permanent insiders. All persons with inside information regarding a project will be included in the project specific insider list.

Persons discharging managerial responsibilities comprise the Board of Directors, the President and CEO and other members of the Leadership Team. These persons have a duty to notify F-Secure and the Finnish Financial Supervisory Authority of every transaction in their own account relating to Financial Instruments of F-Secure within three business days (after a cumulative threshold of EUR 20,000 per annum). The company publishes these notifications as stock exchange releases, as specified by MAR. All releases published on managers' transactions are available on the company's website.

Auditors

The auditor is elected by the Annual General Meeting for a term of service ending at the close of the next Annual General Meeting. The auditor is responsible for auditing the consolidated and parent company financial statements and accounting. The auditor reports to the Board of Directors or the Audit Committee at least once a year.

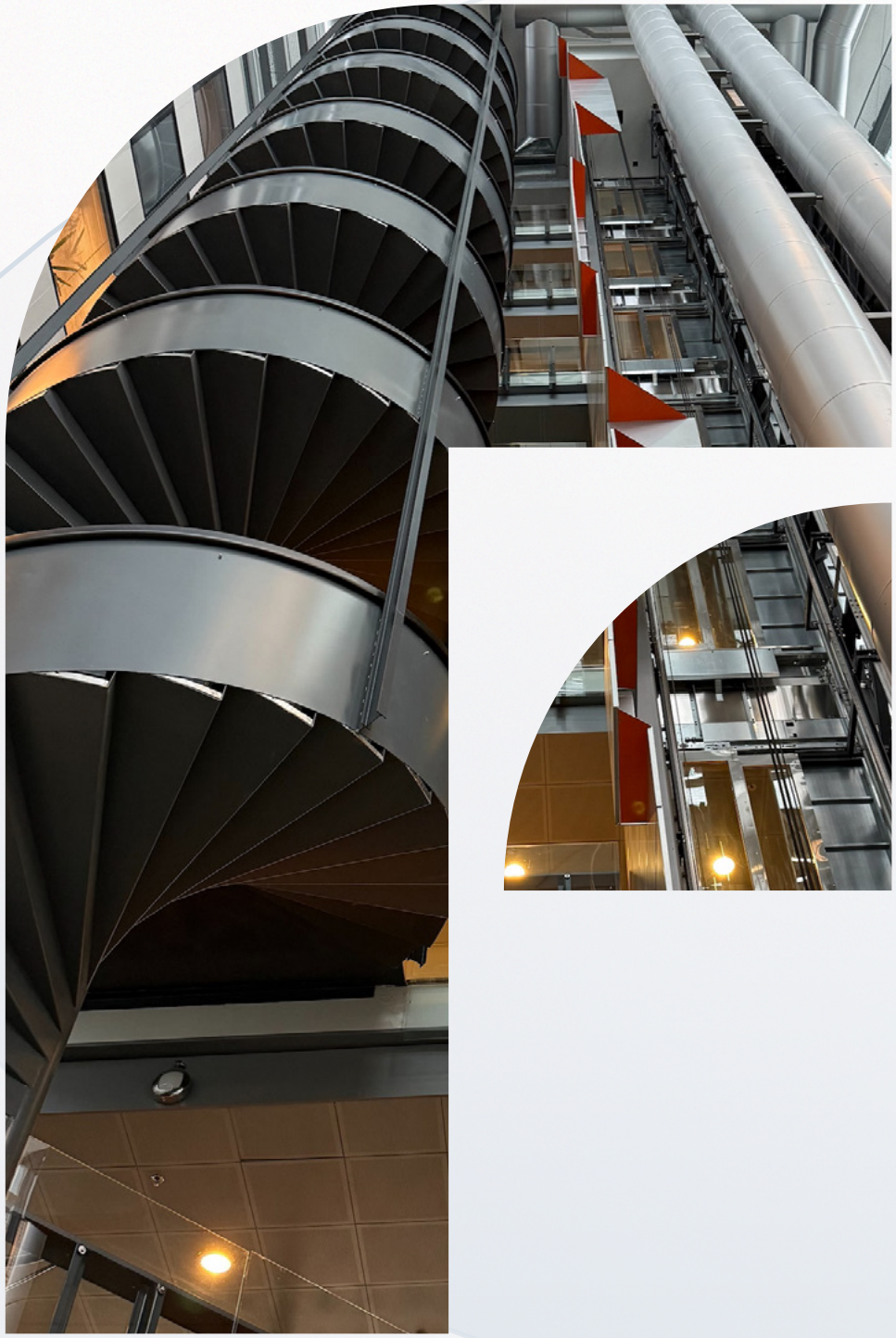
2024:

The Annual General Meeting held 13 March 2024 re-elected the audit firm PricewaterhouseCoopers Oy as the company's auditor with Authorized Public Accountant (APA) Samuli Perälä as the responsible auditor of F-Secure Corporation. The same audit firm was elected as sustainability reporting assurance provider for the financial year 2024.

F-Secure paid the auditor EUR 159 (205) thousand for the auditing services, EUR 21 thousand for audit related fees and EUR 11 thousand for tax consulting. In addition, F-Secure paid a total of EUR 126 (1,233) thousand for other advisory services unrelated to auditing. The other advisory services mainly concerned sustainability advisory and sustainability reporting assurance.

Board of Directors

31 December 2024





Pertti Ervi

born 1957, male

Chair of the Board since 2022

Member of the Audit Committee since 2022

Chair of the Personnel and Nomination Committee since 2024

Finnish citizen

Main occupation: Independent management consultant and a professional board member

Key positions of trust

QPR Software Corporation, Chair of the Board of Directors since 2021

Pointsharp Holding AB, member of the Board of Directors since 2021

Efecte Corporation, Chair of the Board of Directors between 2011 and 2024. A member of the Board of Directors since 2008.

WithSecure, member of the Board of Directors between 2003 and 2023, Chair of the Board 2004–2006 and Chair of the Audit Committee 2008–2022

Mintly Oy, founding member and Chair of the Board of Directors between 2017 and 2022

Teleste Corporation, member of the Board of Directors between 2009 and 2020, Chair 2017–2020.

Comptel Corporation, Chair of the Board of Directors between 2011 and 2017

Stonesoft Corporation, Chair of the Board of Directors between 2004 and 2007

Primary working experience

Computer 2000 AG, Co-CEO and member of the Executive Board between 1995 and 2000

Computer 2000 Finland Corporation, Co-founder and CEO between 1983 and 1995

Education

Ervi holds a Bachelor of Science degree in electronics and several management studies.

Holdings at the end of December 2024: number of shares 120,103, holding 0.07%



Thomas Jul

born 1967, male

Board member since 2022

Member of the Personnel and Nomination Committee since 2024

Danish citizen

Main occupation: CEO of KMD Group

Key positions of trust

Cellnex Nordics, Chairman of the Board from 2024

Primary working experience

Inpay, CEO between 2021 and 2024

MATTA Holding, Co-founder and CEO between 2019 and 2021 and again in 2024

Nets Group, CEO and Country Director in Denmark between 2017 and 2019

Ericsson, President and CEO of PT Ericsson Indonesia between 2014 and 2017,
as the Head of the Customer Unit in Central Europe between 2012 and 2014 and
as the President of Ericsson Austria GmbH between 2012 and 2013

Nokia Siemens Networks, Head of West Europe between 2011 and 2012,
CEO of the Danish Branch between 2007 and 2010 and
Head of Nordics between 2006 and 2009, as well as
Head of the Global Customer Business Team Deutsche Telekom between 2009 and 2011

Nokia, various position including Country Manager,
General Manager and Business Development Director between 1998 and 2007

Systematic Software Engineering, various positions between 1993 and 1998

Education

Jul holds a Master of Science degree in Software Engineering.

Holdings at the end of December 2024: number of shares 17,923, holding 0.01%



Katja Kuusikumpu

born 1977 , female

Board member since 2024

Finnish citizen

Main occupation: F-Secure, Director, Portfolio Governance & Operations

Primary working experience

F-Secure, Director, R&D 2022– 2023

WithSecure, Director, Quality Engineering, various other positions, 2019–2022

Hansen Technologies, Manager, Cloud Development 2017–2019

VR Transpoint, Quality Manager 2014–2016

Qentinel, Business Area Manager/Senior Consultant 2008–2013

Education

Kuusikumpu holds a Master of Science degree in Computer Science and Engineering.

Holdings at the end of December 2024: number of shares 7,626, holding 0.00%



Risto Siilasmaa

born 1969, male

Board member since 2022

Member of the Audit Committee since 2022

Member of the Personnel and Nomination Committee since 2024

Finnish citizen

Key positions of trust

- WithSecure (prior to demerger F-Secure), Chair of the Board of Directors since 2006 (member of the Board of Directors since 1988)
- Hamina Wireless Oy, member of the Board of Directors since 2024
  Chair of the Aalto University Fundraising Advisory Board since 2023
- Quanscient Oy, member of the Board of Directors since 2022
- CybExer Technologies, member of the Board of Directors since 2022
- Upright Oy, Chair of the Board of Directors since 2022
- Pixieray Oy, member of the Board of Directors since 2021
- Ministry of Finance's Technology Advisory Board, chair between 2020 - 2023
- Global Advisory Board of Yonsei University School of Business, member since 2020
- Komatsu International Advisory Board, member between 2020 - 2023
- International Advisory Board of IESE, member since 2019
- Futurice Corporation, member of the Board of Directors since 2018
- Global Tech Panel, an initiative of the EU High Representative for Foreign Affairs and Security Policy, member between 2018 - 2022
- Federation of Finnish Technology Industries, Chair of the Board of Directors between 2016 and 2018, Vice-Chair of the Board of Directors between 2013 and 2015 (a member of the Board of Directors between 2007 and 2019)
- Confederation of Finnish Industries EK, Vice Chair of the Board of Directors between 2017 and 2018 (a member of the Board of Directors between 2007 and 2010 and 2013 and 2016)
- Nokia Corporation member of the Board of between 2008 and 2020 (Chair: 2012– 2020)

Primary working experience
Nokia Corporation, interim CEO at between 2013 and 2014
F-Secure and WithSecure, Founder and CEO of WithSecure between 1988 and 2006

Education
Siilasmaa holds a Master of Science degree in engineering.

Holdings at the end of December 2024: number of shares 60,035,288, holding 34.37%



Petra Teräsaho

born 1966, female

Board member since 2022

Chair of the Audit Committee since 2022

Finnish citizen

Main occupation: CFO of Transmeri Group

Key positions of trust

Paulig Group, member of the Board of Directors since 2020, and Chair of Audit Committee

Primary working experience

Valmet Automotive, CFO between 2023 and 2024

Enfo Group, CFO 2022

Stora Enso, Senior Vice President, Group Controller between 2016 and 2022

Outotec Group, Vice President Group Controller between 2014 and 2015

Nokia Corporation between 1993 and 2014, Several leadership roles in Finance, Marketing, Strategy & Business Development, e.g.
CFO of Nokia Mobile Phones operations in India between 2007 and 2012
Global Finance Director, Mobile Phones & Nokia Strategic Marketing between 2004-2007
Head of Developer Business Marketing, Mobile Phones between 2003-2004
Head of Business Planning of Mobile Applications unit between 2000 and 2001
Head of Value-Based Marketing (Nokia Networks) between 1999 and 2000
Accounting Manager (Network Systems) between 1996 and 1998
Nokia Group Accounting, Financial Analyst between 1993 and 1996

United Paper Mills France SA, Paris France, Controller between 1991 and 1993

Education

Teräsaho holds a Master of Science in Accounting and Finance.

Holdings at the end of December 2024: number of shares 22,640, holding 0.01%



Tommi Uitto

born 1969, male

Board Member since 2024

Finnish citizen

Main Occupation: Nokia, President, Mobile Networks

Primary working experience

Mobile Networks, Senior Vice President, Global Product Sales, Nokia 2015–2018

Nokia Networks, Senior Vice President, West Europe, Customer Operations, 2013–2015

Nokia Siemens Networks, Head of Global 4G/LTE Radio Access Business Line, Mobile Broadband, 2011–2012

Nokia Siemens Networks, Head of Product Management, Network Systems, 2009-2010

Nokia Siemens Networks, Head of WCDMA/HSPA and Radio Platforms Product Management, 2007-2008

Nokia Networks, General Manager, Radio Controller Product Management, 2005–2007

Nokia Networks, Director, Sales & Marketing (Lead Sales Director), France Telecom/Orange 2002–2005

Nokia Networks, Operations Director, Northeast Europe, Central & Eastern Europe and Middle East, 1999–2002

Nokia Networks, Manager, Product Business Management and Logistics, Cellular Transmission, 1996–1999

Valmet Logging Americas Inc., Director, Production and Development, 1994–1995

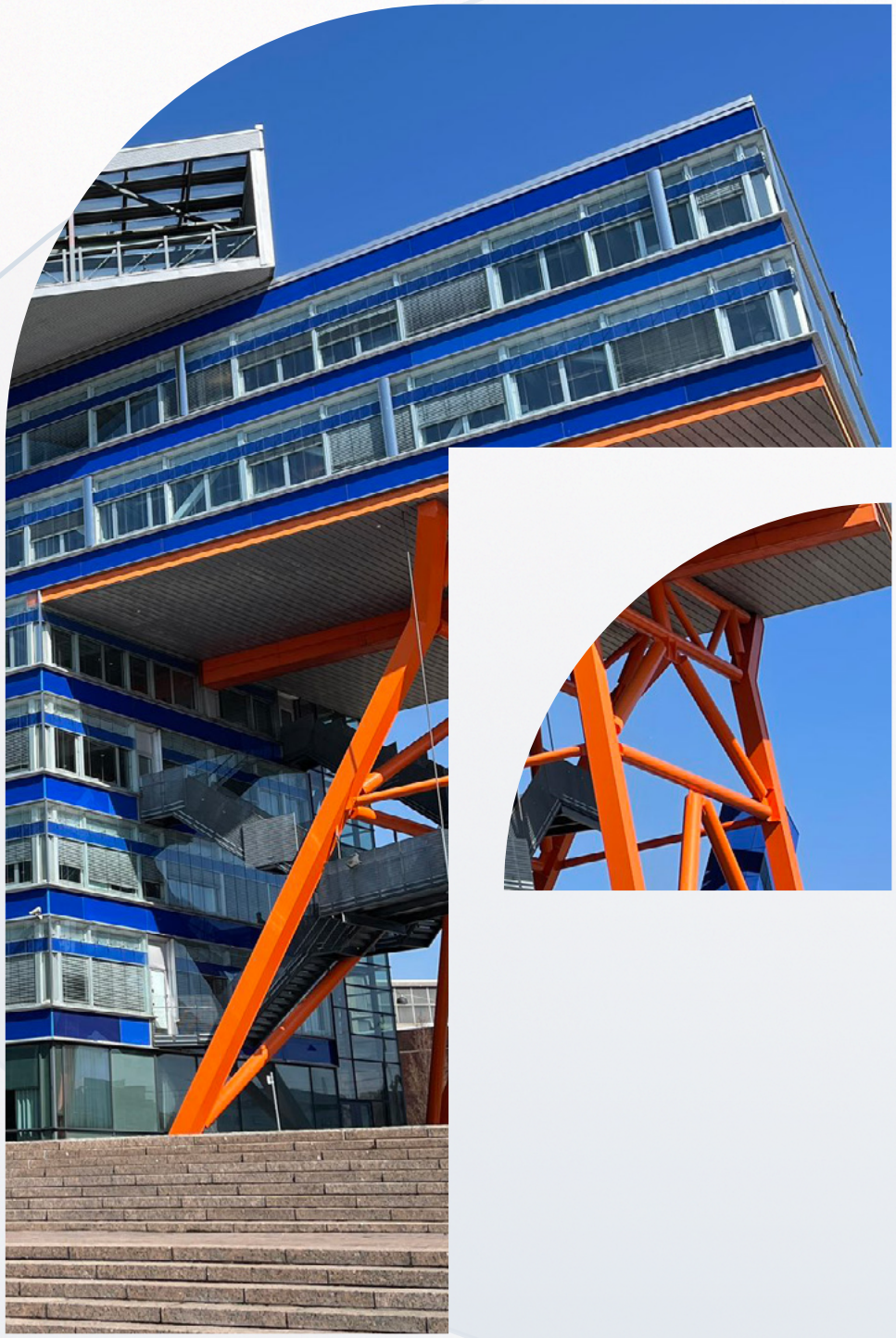
Education

Uitto holds a degree of Master of Science in Industrial Management and a degree of Master of Science in Operations Management from Michigan Technological University.

Holdings at the end of December 2024: number of shares 8,431, holding 0.00%

Leadership Team

31 December 2024





Timo Laaksonen

born 1961 , male

President and Chief Executive Officer since 2022

Finnish citizen

Primary working experience

WithSecure, Executive Vice President of Consumer Security, and various other positions between 2012 and 2022

Tecnotree, Chief Commercial Officer between 2010 and 2012

Xtract, CEO between 2008 and 2010

First Hop, CEO between 2001 and 2008

Sonera SmartTrust, Executive Vice President between 1998 and 2001

Teamware Group, Vice President between 1993 and 1998

ICL Travel Systems, Marketing Manager between 1992 and 1993

Key positions of trust

Finnish Information Security Cluster (FISC), member of the Board since 2024

Helsinki Region Chamber of Commerce, member of the Commission since 2024

Broadband Forum Executive Advisory Board member since 2023

Finnish American Chamber of Commerce in New York, member of the Board of between 2018 and 2019

Broadband Multimedia Marketing Association (USA), a member of the Board of Directors between 2018 and 2019

Education

Laaksonen holds a Master of Science degree in Economics (International Marketing and International Trade Law).

Holdings at the end of December 2024: number of shares 38,282, holding 0.02%



Richard Larcombe

born 1974, male

Chief Marketing Officer since 2022

British citizen

Primary working experience

WithSecure, Vice President of Global Marketing between 2019 and 2021

ismybillfair.com, co-founder and Chief Marketing Officer between 2017 and 2019

Tesco Bank, Brand and Marketing Director between 2015 and 2017

Virgin Media, Chief Marketing Officer and Director of Advertising and Sponsorship between 2010 and 2015

The Times, Sunday Times and Times Online, Head of Marketing between 2004 and 2010

AMV BBDO, Account Director between 1998 and 2004

Grey, Account Director between 1996 and 1998

Education

Larcombe holds a degree in Psychology (BA Hons).

Holdings at the end of December 2024: number of shares 12,079 holding 0.01%



Nina Lehto

born 1976, female

Senior Vice President, Services since August 2024

Finnish citizen

Primary working experience

Nokia, Head of Mediation Business Line, and various other positions between 2018 and 2024

Comptel, VP, Delivery & Support, and various other positions between 2006 and 2017

Roschier, Attorneys, Lawyer between 2002 and 2006

Education

Lehto holds a Master of Laws degree.

Holdings at the end of December 2024: number of shares 0.



Antero Norkio

born 1972, male

Senior Vice President, Corporate Development
since 2022

Finnish citizen

Primary working experience

WithSecure, Vice President Product Management (Consumer Business), and various other positions between 2011 and 2022

Airwide Solutions, Head of Global Channel Partners and Director of Product Management between 2002 and 2011 (including the acquisition of First Hop 2007)

Taika Technologies, Vice President of Product Management 2001 and 2002

Sonera SmartTrust, Director of Product Management between 1997 and 2001

Education

Norkio holds a Master of Science degree in Industrial Engineering and Management (Strategy and International Business).

Holdings at the end of December 2024: number of shares 69,329, holding 0.04%



Bruno Rodriguez

born 1973, male

Chief Revenue Officer since October 2024

Spanish citizen

Primary working experience

Bitdefender, Global VP Sales Service Providers and Technology Licensing and Strategic Partnerships Director between 2012 and 2024

Panda Security, Global Product Management Director, Global Business Development Director, Business Unit Director and other positions between 2006 and 2012

Euskaltel, Business Development Manager between 2000 and 2006

Education

Rodriguez holds a Master of Science degree in Business Administration and a Bachelor Degree in Computer Engineering.

Holdings at the end of December 2024: number of shares 0.



Sari Somerkallio

born 1972, female

Chief Financial Officer since 2022

Finnish citizen

Primary working experience

WithSecure (prior to demerger F-Secure), Head of Finance in Consumer Security from February to June 2022

Fiskars Group, several manager and VP positions such as Vice President of Business Finance,
Senior Vice President of Finance & Business Development, and
Manager of Development Projects between 2008 and 2021

Wärtsilä Corporation, Project Manager and Process Manager between 2002 and 2008

Wärtsilä Corporation, Investor Relations Manager between 1999 and 2002

Merita Stockbrokers, Analyst between 1997 and 1999

Interbank, Analyst between 1996 and 1997

Education

Somerkallio holds a Master of Science degree in Mathematics and a Master of Science degree in Economics (Finance).

Holdings at the end of December 2024: number of shares 15,481, holding 0.01%



Kaisa Tikka-Mustonen

born 1978, female

Chief People Officer since September 2024

Finnish citizen

Primary working experience

Helvar, Chief People Officer between 2020 and 2024

Nordcloud, VP, Talent Acceleration & People Operations between 2018 and 2020

Nets Group, Merchant Services, HR Director between 2015 and 2018, HR Business Partner between 2014 and 2015

Tieto, various Human Resources positions between 2007 and 2013

Education

Tikka-Mustonen holds a master's degree in Education.

Holdings at the end of December 2024: number of shares 0.



TL Viswanathan

born 1979, male

Chief Product Officer since 2023

Indian citizen

Primary working experience

F-Secure, Vice President, Embedded security, 2022

Nokia, Head of Digital Operations Portfolio, between 2018 and 2022

Comptel, Director & Vice President Global Alliances, between 2014 and 2018

Oracle, Senior Account Manager APAC, between 2013 and 2014

Nokia Siemens Networks, various leadership and business development roles for Applications, Systems integration business between 2006 and 2013

Siemens Communications, Solution Consultant between 2000 and 2006

Education

Viswanathan holds a Master's degree in Business Administration (International Business).

Holdings at the end of December 2024: number of shares 3,394, holding 0.00%



Toby White

born 1977, male

Chief Technology Officer since 2022

British and Finnish citizen

Primary working experience

WithSecure, Vice President for Research & Development in Consumer Security 2020–2022

Wärtsilä, Vice President of Digital Engineering between 2017 and 2020

GlobalData Plc, Group CTO between 2014 and 2017

Timetric, Founder and CTO between 2008 and 2014

Cambridge University, Researcher between 2002 and 2008

Education

White holds a Master of Chemistry degree in Chemistry and a Doctor of Philosophy degree in Theoretical Chemistry.

Holdings at the end of December 2024: number of shares 32,085, holding 0.02%

Remuneration



Remuneration Report

Introduction

This Remuneration Report 2024 has been prepared in accordance with the Finnish Corporate Governance Code 2025 (publicly available at http://cgfinland.fi/en/) and contains comprehensive information on remuneration of the Board of Directors and the President and CEO. All remuneration information in this report is from 1 January 2024 until 31 December 2024, except that the Board of Directors remuneration is based on their term of office that began in 2024 and will expire at the end of the 2025 Annual General Meeting (as explained in further detail in the F-Secure Corporate Governance Statement 2024).

F-Secure Remuneration Policy, which has been applicable since June 2022, describes the remuneration for the Board of Directors and the President and CEO and the considerations of determining the policy and operation of the policy. Remuneration Policy of F-Secure complies with the recommendations of the Finnish Corporate Governance Code for listed companies, Shareholders' Rights Directive legislation and any other regulations and guidelines concerning remuneration in listed companies. The Remuneration Policy is available at F-Secure website.

According to F-Secure Remuneration Policy, the remuneration for F-Secure management is designed to advance the business objectives and long-term profitability of the company. F-Secure remuneration in general is based on rewarding for performance and talent. Remuneration is designed to be competitive compared to relevant reference markets, to increase commitment and work engagement and to be consistent across the organization. Incentive schemes are developed to support the company's strategy by aligning the interests of the shareholders and the key employees for strong performance and short and long-term value creation of the company. The remuneration of employees across the company is reviewed regularly with the intention that all employees are paid appropriately in the context of the market and considering their individual performance and competencies.

These principles have been considered in the company's remuneration in the financial year 2024. In 2024, the remuneration of the Board of Directors and the President and CEO complied with the Remuneration Policy, and there were no deviations.

The President and CEO's remuneration follows the same principles as the remuneration of all other employees, and this is evident in the performance criteria set for the variable remuneration. Approximately half of the President and CEO's remuneration package is based on performance. The existing short- and long-term incentive plans are based on the company's financial performance, employee engagement and shareholder value development to ensure a strong link between the company's performance and CEO remuneration. The President and CEO is recommended to hold at least 50% of the shares received as rewards from the long-term incentive programs and to accumulate the shares from the incentive programs until the value of the shares received from the share programs equals the annual gross base salary of the President and CEO. There are no other restrictions set for the shares received from the share-based incentive programs.

Remuneration in 2024

The Board of Directors of F-Secure Corporation decided on the establishment of share-based long-term incentive plans targeted to the management and selected key employees of F-Secure. The share-based long-term incentive plans include a Performance Share Plan ("PSP") as the main plan and Restricted Share Plan ("RSP") as a complementary share-based incentive plan for individually selected key employees in specific situations. New plan periods 2024–2026 for PSP and RSP commenced at the beginning of 2024 and include a three-year performance period followed by a possible reward payment.

The ongoing LTI programs prior to demerger from WithSecure continue. All LTI allocations (PSP and RSP) made originally in the shares of WithSecure were adjusted to be the allocations of F-Secure Corporation. Adjustments to PSP 2022–2024 were made using the reference prices of the two new companies.

The total remuneration paid to the President and CEO in 2024 was EUR 333,840 of which EUR 9,600 was in the form of variable pay related to the Lookout Life acquisition. No short-term incentives were paid out.

At the end of 2024, the President and CEO held 38,282 shares of F-Secure.

Annual remuneration in 2024

F-Secure's paid average remuneration in 2024 is described in the table below.

Average annual remuneration (EUR)	2024	2023
President and CEO[1]	333,840	500,342
Chair of the Board	80,000	80,000
Other Board Members[2]	40,500	40,500
Average employee[3]	76,836	73,241

1) Remuneration paid during the financial year, including the base salary as well as short- and long-term incentives and transaction bonus.
2) The average remuneration paid to the Board Members, excluding the employee Board member.
3) The total wages and salaries, including sales and non-sales incentives, paid / average full-time equivalent headcount during the same period in all countries. The amount excludes end of employment related severances.

Remuneration of the Board of Directors

F-Secure's General Meeting, held on 13 March 2024, decided that the remuneration for the Board of Directors of F-Secure shall be paid as follows: EUR 80,000 for the Chairman of the Board of Directors, EUR 48,000 for the Chairman of each Committee, EUR 38,000 for other members of the Board of Directors, and EUR 12,667 for a member of the Board of Directors employed by F-Secure.

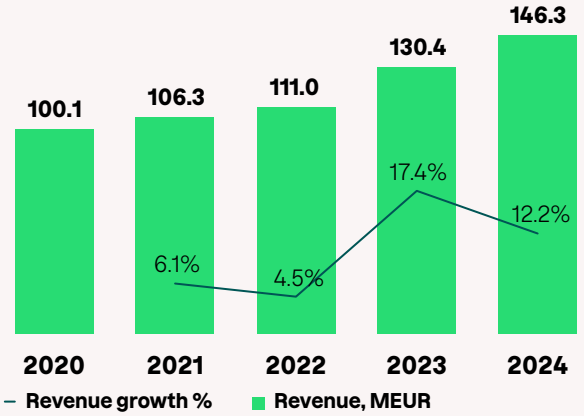
Pursuant to the decision by F-Secure's General Meeting in March 2024, F-Secure Corporation repurchased its shares from the market on the 29th and 30th April and 2 May (2024) for and on behalf of F-Secure Board members, in such quantity that represents approximately 40 per cent of the Board's remuneration.

For the Members of the Board of Directors, changes in the holdings of the company shares and rewards paid in shares are reported according to the Market Abuse Regulation. Related stock exchange releases are available on the company's website.

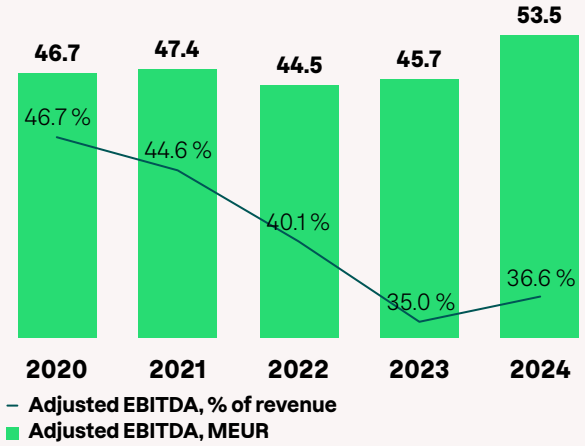
The travel expenses and other costs of the members of the Board of Directors of F-Secure directly related to board work are paid in accordance with F-Secure compensation policy in force from time to time.

Each member of the Board of Directors of F-Secure is paid a predetermined travel fee in addition to travel expenses for meetings held outside their country of residence. A separate meeting fee of EUR 1,000 is paid to the Board members travelling from another country to an on-site meeting within the European continent. If inter-continental travel is required, the fee is EUR 2,000. The travel expenses and other costs directly related to the Board work of the members of the Board of Directors are paid in accordance with the company's compensation policy in force at any given time.

Revenue development 2020-2024



Adjusted EBITDA development 2020–2024



The key figures are presented combining actuals and carve-out basis for 1-12/2022 and on an actuals basis for financial position at 31 December 2022. For periods 2020-2021 financial information is on carve-out basis.

The Board of Directors Remuneration in 2024

Remuneration for the board term 2024-2025.

Member	Annual fee paid in cash, EUR	Annual fee paid in shares, EUR	Annual fee paid in shares, pcs	Meeting fees paid EUR[1)]	Total, EUR
Pertti Ervi	48,001	31,999	15,434	6,000	86,000
Madeleine Lassoued (1.1.-13.3.2024)				1,000	1,000
Risto Siilasmaa	22,801	15,199	7,331		38,000
Thomas Jul Pfeiffer	22,801	15,199	7,331	5,000	43,000
Petra Teräsaho	28,801	19,199	9,260		48,000
Sami Salonen (1.1.-13.3.2024)					
Tommi Uitto (13.3.-31.12.2024)	22,801	15,199	7,331		38,000
Katja Kuusikumpu (13.3.-31.12.2024)	7,602	5,065	2,443		12,667
Total	152,806	101,861	49,130	12,000	266,667

1) The remuneration presented includes travel allowance granted from abroad to board meetings.

Remuneration of the President and CEO

The remuneration of the President and CEO is decided by the Board of Directors. The main components of the President and CEO's total remuneration are base salary and short- and long-term incentives. In addition, he may participate in the voluntary Employee Share Savings Plan (ESSP) as approved by the Board of Directors. The aim of the ESSP is to encourage employees to acquire and own F-Secure shares, and it is intended to align the interests of the shareholders and the employees as well as to increase employees' long-term commitment to the company.

Salaries and financial benefits paid in and accrued based on 2024 are described below:

EUR	Payments in 2024
Base salary, including fringe benefits	324,240
Pension / Other financial benefits	
Transaction bonus	9,600
Short-term incentive (STI	-
Long-term incentive (LTI)	-
Total	333,840

Short-term incentive (STI) payout for the President and CEO is 50% of annual base salary if targets are met, maximum payout being equal to the annual base salary.

F-Secure Short Term Incentive plan objectives were set for the period of 1 January–31 December 2024. The STI Plan of 2024 for the President and CEO was based on F-Secure 2024 combined revenue and adjusted EBITA growth with 80% weight and employee Net Promoter Score with 20% weight of total. The overall performance for these two criteria was evaluated and resulted in 78% weighted performance outcome.

In 2024, the President and CEO, Timo Laaksonen did not receive a STI payment in February due to objectives related to F-Secure Short Term Incentive plan objectives of January–December 2023 were not met. The objectives of the plan were 2023 combined revenue growth and adjusted EBITA growth with 80% weight and employee Net Promoter Score growth with 20% weight. The weighted performance for these three criteria for 2023 was 0%. The reward was in total EUR 0.

There was no long-term incentive (LTI) payment made to the President and CEO in 2024. In 2024 the President and CEO was granted 82,555 shares within the Performance Share Plan (PSP) 2024–2026 according to the guidelines defined in the company's Remuneration Policy. This grant represents the target level reward, the maximum reward being two times the target allocation. Final reward is determined based on the extent to which the targets have been reached during the performance period.

In December 2024, the Board of Directors approved a customary transaction bonus to some key individuals for the closing of the Lookout Life acquisition. The President and CEO received a bonus of EUR 9,600.

STI Plan 2024	STI Target (% of base salary)	Performance Criteria	Weight	Performance	Total Weighted Performance	Payment
STI 2024 (January–December)	50%	Revenue and adjusted EBITA Growth	80%	73%	78%	Q1/2025
		Employee Engagement (eNPS)	20%	100%		

STI Plan 2023	STI Target (% of base salary)	Performance Criteria	Weight	Performance	Total Weighted Performance	Payment
STI 2023 (January–December)	50%	Revenue and adjusted EBITDA growth	80%	0%		February 2024
		Employee Engagement (eNPS)	20%	0%		

The key terms of service of the President and CEO

The contract of the President and CEO is an indefinite contract with a six-month period of notice both ways. If the company terminates the contract for reasons other than a breach of the contract, the President and CEO shall be entitled to receive severance pay equivalent to six months' salary in addition to the salary for the notice period.

The company has obtained a life insurance for the President and CEO with an amount equaling the annual gross salary of the President and CEO.

The President and CEO does not have a supplementary pension plan, and the determination of his pension conforms to the standard rules specified by Finland's Employee Pension Act (TYEL). The President and CEO's retirement age is also determined by the statutory pension system and is 65 years under the applicable Finnish legislation.

President and CEO Pay mix 2024

President and CEO Pay mix in 2024 consisted purely of base pay, including fringe benefits and a transaction bonus. There were no short-term and long-term incentive payments due to the payout thresholds were not met.

The President and CEO – Current LTI Plans

Share Plan	LTI Target (pcs of shares)	Performance Criteria	Weight	Performance	Payment
PSP 2021–2023	43,160	Absolute Total Shareholder Return	100%	–	H1 / 2024
PSP 2022–2024	41,562	Absolute Total Shareholder Return	100%	– / Plan ongoing	H1 / 2025
		Absolute Total Shareholder Return	70%		
PSP 2023–2025	47,000	Profitable growth (average revenue growth 2023–2025 (%) and adjusted EBITA 2025 (%))	30%	– / Plan ongoing	H1 / 2026
RSP 2023–2025	12,373	Fixed share reward amount and a retention period of three years	–	– / Plan ongoing	H1 / 2026
PSP 2024–2026	82,555	Absolute Total Shareholder Return	50%	– / Plan ongoing	H1/2027
		Earnings per share sum	25%		
		Revenue growth (EUR in 2026 vs proforma 2023)	25%		



F-Secure Corporation
Tammasaarenkatu 7
00180 Helsinki
Tel. +358 9 2520 0100
helsinki@f-secure.com
www.f-secure.com