Group Sustainability Report

Table of content

Group Sustainability Report

GROUP SUSTAINABILITY REPORT -

General

Reporting principles

BP-1 Basis for preparation

This group sustainability report has been prepared in accordance with the Accounting Act Chapter 7 and European Sustainability Reporting Standards (ESRS). The F-Secure group sustainability report has been prepared on a consolidated basis, and it covers the F-Secure Group with the same scope as our financial statements. The statement includes information on material Impacts, Risks and Opportunities (IROs) connected with our direct and indirect business relationships in our upstream and downstream value chain.

F-Secure has not omitted any information corresponding to intellectual property, know-how or innovation results, nor used the exemption from disclosure of impending developments in negotiations.

BP-2 Disclosures in relation to specific circumstances

Planning horizon

F-Secure defines short-term as 0-1 years, medium-term as 1-3 years, and long-term as 3+ years, aligning with our strategic planning cycles.

Value chain estimation

For GHG emissions, we use value chain estimations where actual data is unavailable, following GHG Protocol methodology. We aim to improve data quality by moving from estimations to actual emission data through stakeholder collaboration.

The quantification of GHG emissions in F-Secure's 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 to use estimations and sector averages in GHG calculation in cases where actual data is unavailable.

Section E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions provides more detailed information on methodology and value chain estimation.

Sources of estimation and outcome uncertainty

GHG emission calculations contain uncertainty, particularly for Scope 3. Our limitations include restricted site-specific consumption data for Scope 2 and spend-based calculations for key Scope 3 categories. In Scope 1, leased cars data is limited, and the calculations have been done based on estimating contract kilometres and average consumption of car models. Section *E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions* provides more detailed information on methodology and estimation uncertainty. Additional uncertainties exist in cybersecurity metrics objectivity. Section *S4-5 Progress towards targets* provides more detailed information on methodology and estimation uncertainty. Finally, the measurement of the metrics in this group sustainability report has not been validated by an external body apart from the assurance of this Group sustainability report, unless specifically stated otherwise under the disclosure requirement section of such metrics.

The reported Code of Conduct training target excludes individuals for whom employee status information is unavailable.

Forward-looking statement

Forward-looking information should be considered with caution as it's subject to risks and uncertainties that could impact our ability to achieve the described objectives or anticipated results.

Changes in preparation or presentation of sustainability information

F-Secure has chosen to change the E1 scope 3 related target of absolute emission reduction of 42% to emission intensity reduction of 52% between 2024 and 2030. The change has been made due to business growth compatibility, and it allows for better comparisons between different companies. We will continue to report absolute emission reduction of scope 3 in section E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions.

Continue to report qualitative information but drop from Consumers and end-users S-4 targets the "*Ratio of externally reported vulnerabilities compared to internally reported vulnerabilities*" due to data quality issues affecting annual comparability.

The 2024 cybersecurity training completion rate initially excluded employees on extended leave. This has been corrected in 2025, and the 2024 cybersecurity training completion rate has been updated to include all employees.

Reporting errors in prior periods

The nature of the error was that calculation method for disclosure in table S1-9 Gender distribution was updated based on approved targets. In prior period section S1-5 Own workforce targets gender diversity (directors including leadership team, %) percentage for females was 25,1% and male 74,9%. Those were corrected this reporting period and corrected figures are female 23,5% and male 76,5 %.

The nature of the error was that calculation method for disclosure S1-13 Training was updated. In prior period section S1-5 Own workforce targets and career review target percentage was 82%. That was were corrected this reporting period and corrected figure is 88%.

Disclosures stemming from other legislation or reporting pronouncements

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

1. Cybersecurity policy-related metrics and targets including cybersecurity training, cybersecurity incidents and bug bounty program, based on

- EU General Data Protection Regulation
- 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)

- 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 Organization on Fundamental Principles and Rights at Work

Incorporation by reference

F-Secure calculates GHG intensity based on net revenue by dividing total GHG emissions (t CO_2eq) by net revenue (€). Net revenue is based on our financial statement (Cross-reference to financial section 3. Revenue).

The measures provided in the group sustainability report 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).

Phase-In provisions

As a company with fewer than 750 employees in reporting year of 2025, we've omitted certain information required by ESRS E1 and ESRS S1 in accordance with Appendix C of ESRS 1.. F-Secure has chosen to omit the information prescribed by ESRS 2 SBM-3 paragraph 48(e) anticipated financial effects based on European Sustainability Reporting Standards 'quick-fix' delegated act of 11 July 2025. In addition, F-Secure has in our 2025 statement decided to omit 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 Group sustainability report, 'supervisory bodies' refer to the F-Secure Board of Directors, its Audit Committee and Personnel and Nomination Committee. 'Management body' refers to the F-Secure Leadership Team, including the CEO and leadership team members. The Board oversees company administration and appoints the CEO, who manages daily operations per Board instructions.

The highest decision-making body is the General Meeting of Shareholders, which elects Board members. The Board is responsible for F-Secure Group administration and the appropriate organization of its operations. The Board's duties are defined according to the Articles of Association, Finnish Companies Act, and other applicable laws and regulations, including overseeing business conduct and compliance, and approving significant governance policies.

Roles and Responsibilities

The Board has established an Audit Committee and a Personnel and Nomination Committee to enhance efficiency. The Audit Committee monitors risk management, internal controls, IT strategy, sustainability, and financial reporting, as well as auditing. Most committee members must be independent from the company, and at least one must be independent from significant shareholders. The Personnel and Nomination Committee prepares matters on Board composition and compensation, actively seeking qualified new Board members.

The Board and Leadership Team are supported by the Legal Team, which maintains business conduct policies and provides related training. Each Leadership Team member supervises policy implementation in their respective functions.

Composition and Diversity Information

As of 31 December 2025, F-Secure had 9 executive members in its management body and 7 non-executive members in its supervisory body (Board of Directors).

Board of Directors composition	2024	2025
Non-executive members	6 non-executive	6 non-executive
Employee representation	One Board member elected from personnel with term ending at next AGM	One Board member elected from personnel with term ending at next AGM
Experience relevance	Board members have international experience from technology, telecom, and cybersecurity sectors across Europe, North America, APAC/Japan	Board members have international experience from technology, telecom, and cybersecurity sectors across Europe, North America, APAC/Japan
Board gender diversity	Female: 33.3 (2), Male: 66.7% (4)	Female: 42.8% (3), Male: 57.2% (4)
Independent Board members	~67% (4 of 6 members independent from company and major shareholders)	~85.7% (6 of 7 members independent from company and major shareholders)

Table1. Composition and Diversity Information.

The Diversity Principles established by the Board strive for appropriately balanced gender distribution and diverse backgrounds. The Board comprises members aged 44-68 years with five different nationalities represented.

Access to Expertise on Sustainability Matters

The Board of Directors has received ESG training in 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 Group sustainability report.

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 the F-Secure Audit Committee. F-Secure Sustainability Council drives 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.

ESG Governance Structure

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 sustainability 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 Sustainability Council

- Identify and assess ESG impacts, risks and opportunity
- Develop and implement sustainability 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 Sustainability Council and facilitating sustainability 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.

Wellbeing[1]
Reviews and sets ambition on wellbeing related plans. Evaluates and provides feedback on progress.

Environment
Driving environmental initiatives and climate change related targets.

Topics covered by Sustainability council

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

Customers and end-users
Reviews and sets ambition on stakeholder sustainability. 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

ESG oversight is organized in layers:

1. Board of Directors: Reviews/approves strategy with ESG elements; updated at least annually on ESG progress
2. Audit Committee: Monitors ESG reporting, risks, and internal controls; reviews group sustainability report preparation and external assurance
3. Leadership Team: Establishes ESG strategy, ensures integration with company culture, approves policies and principles
4. Sustainability Council: Facilitates ESG strategy implementation, identifies/assesses ESG impacts and risks, drives sustainability reporting
5. Sustainability Function: Leads Sustainability Council and facilitates sustainability strategy implementation and ensures regulatory compliance
6. ESG Committees: Drive specific ESG initiatives (DEI, Wellbeing, and Environment)

The Sustainability Council typically meets monthly with key members, including the CFO, CPO, Legal Counsel, SVP of Corporate Development, and the Sustainability function lead. The Council includes participants from other functions like sales and product management.

The ESG Committees works in close collaboration with the sustainability function lead. ESG committees drive initiatives related to their respective topics through committee meetings to define and progress actions. Each ESG committee reports to the Sustainability Council at least twice annually. These progress updates include reviews of actions and targets. The ESG committees also participate in the annual IRO review process.

ESG activities are fully integrated with the company strategy and based on F-Secure values, Code of Conduct, and related policies. Management of identified IROs is conducted at least once a year by the Sustainability Council, with results shared with the Audit Committee for review and oversight. In the sustainability council, targets related to the IROs are proposed, and they are reviewed by the Audit Committee and Board of Directors and approved by the Leadership team. Targets are monitored in sustainability council meetings at least twice a year and reviewed by the Audit Committee and Board of Directors at least once a year.

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

Information flow and frequency

The F-Secure Board reviews ESG annually, while the Audit Committee discussed ESG in 2 of 5 meetings during 2025. 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 based on input from the monthly Sustainability Council meetings, which include key management representatives (CFO, CPO, Legal Counsel), the sustainability function, and other function representatives. Updates include F-Secure ESG plans and actions, policies and targets, and reports on their progress, as well as implementation of due diligence.

Consideration of IROs when overseeing company strategy and risk management

Sustainability-related risks and impacts are managed as part of F-Secure's risk management process. The primary goal is to enable the organization to identify and manage risks effectively by monitoring potential negative impacts and the likelihood of various situations arising from operations, markets, customers, and partners.

F-Secure encourages continuous risk assessment by personnel. Operational risks identified through this process are regularly reviewed by each function, including bi-annual reviews with the CEO, Leadership Team, and Audit Committee. Positive impacts and opportunities are embedded into the strategy process and considered during operating plan reviews.

Trade-offs related to IROs are evaluated during strategy development, weighing costs and benefits of different options to ensure alignment with organizational goals and stakeholder expectations. This approach ensures that sustainability considerations are integrated into company decision-making while balancing potential risks and opportunities.

Material Topics Addressed in 2025

In addition to the F-Secure Sustainability Council and its ESG committees, the respective management members and supervisory bodies have addressed the following material topics:

Standard	Type	Description	Supervisory	Management
Environment	Potential positive impact (OO)	Implementation of green coding principles can reduce battery use in consumer devices and computational power in cloud environments	No	Yes
	Risk (DVC/OO)	Failure to meet climate change mitigation targets may negatively impact channel business	Yes	Yes
Social	Actual positive impact (OO)	Protect consumers' digital moments with relevant, effective cybersecurity solutions	Yes	Yes
	Actual positive impact (DVC, OO)	Create awareness about cybercrimes through campaigns, and events	No	Yes
	Actual positive impact (OO)	Family leaves (sometimes exceeding local requirements) and enhancing work life balance of employees.	No	Yes
	Actual positive impact (OO)	Promote gender equality through recruitment and gender pay gap mitigation	No	Yes
	Actual positive impact (OO)	Further ramp up strategic learning and development activities and track investment into learning activities.	Yes	Yes
	Actual positive impact (OO)	Foster inclusive culture with speak-up environment where workplace is safe for everyone	Yes	Yes
	Potential positive impact (OO)	Continuously identify the internal competencies critical to our strategy	No	Yes
	Opportunity (OO)	Evolving threat landscape, protecting consumers against evolving threat landscape (for example scams) benefits both F-Secure and partners	Yes	Yes
	Opportunity (OO)	Use data and AI in security applications, for more effective protection and better user experience. AI-powered (network) monitoring tools can track user behavior, detect anomalies, and react accordingly.	Yes	Yes
	Opportunity (OO)	Enhance employer reputation through DEI activities to attract younger generations	Yes	Yes
	Opportunity (OO)	Use of AI in workforce development, including process improvements, competency maturity and AI sentiment	Yes	Yes
	Risk (DVC)	Channel strategy, significant agreement changes or existing partner loss can negatively impact outlook	Yes	Yes

Standard	Type	Description	Supervisory	Management
Governance	Risk (OO)	Decreasing consumer willingness to pay for premium security due to competition/economic situation	No	Yes
	Risk (OO)	Talent acquisition and retention, loss of key persons or inability to acquire new talent	Yes	Yes
	Risk (OO, DVC/UVC)	Security vulnerabilities from suppliers and partners, relying on external vendors, especially vendors who are one step removed in the supply chain, adds layers of vulnerability.	Yes	Yes
	Risk (OO)	Cybersecurity attacks impacting reputation and business	Yes	Yes
	Risk (OO)	Mental health related absences detected.	No	Yes
	Risk (OO)	AI increases risk of security breach, effective AI experimentation and roll-out dependent on high quality data sources and may also increase risk of a security breach.	Yes	Yes
	Actual positive impact (OO/DVC)	Whistleblower channel available to all employees and business partners, with awareness raised through mandatory internal training	Yes	Yes
	Actual positive impact (OO)	F-Secure is strengthening its culture by reviewing people and culture structures to reflect the desired culture, supporting leadership and team development, and fostering a culture of experimentation	No	Yes
	Risk (DVC)	Partnership business, use of agents and other intermediaries increases bribery and corruption risk.	Yes	Yes
	Risk (DVC/UVC ,OO)	Anti-Bribery and Corruption risks increase as a result of M&A transactions due to limited understanding of the target.	No	No

Table 2. Material topics addressed by management and supervisory bodies.

Specifically, with regard to Audit Committee and Board of Directors engagement and in addition to what is described under “ESG Governance Structure”, any changes in the DMA and/or IROs, and updates to targets have been reviewed by the Audit Committee during 2025. In addition, the decision was taken to commit to SBTi during this reporting year, and the decision to commit was reviewed by the Audit Committee.

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 designed to reward achievement of financial and operational objectives, foster a performance culture, and focus on business plan execution.

The Leadership Team is also eligible for share-based long-term incentives (LTI), aligning shareholder and Leadership Team interests. Similar LTI plans apply to certain members of our administrative and supervisory bodies.

Role of sustainability-related targets in incentive schemes

The 2025 non-sales STI Plan includes Company Business Results (combined growth % and profitability %) and Company Employee Engagement (eNPS). These elements connect to our material sustainability drivers - growth indicates consumers are protected globally (building trust in digitality), while eNPS reflects employee well-being and satisfaction.

The non-sales STI Plan is included in the remuneration policy, with goals approved annually by the Board. Share-based LTI programs may be based on long-term

financial/strategic performance or share value increase, with criteria focused on strategic financial targets.

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

The non-sales STI consists of:

- Business Results (combined growth % and profitability %): 60-80% weight
- Function-specific targets (may include sustainability-related targets): 0-20% weight
- Company Employee Engagement (eNPS): 20% weight

The Long-Term Incentive criteria for performance periods are based on strategic financial targets.

The Board of Directors approves annual STI designs and company-level targets based on Leadership Team proposals. For LTI programs, the Board determines terms, conditions, performance criteria, and objectives for each performance/vesting period.

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

GOV-4 Statement on Due Diligence

F-Secure's due diligence process identifies, mitigates, and addresses actual and potential negative impacts connected to our business, operations, value chain, offering, and business partners. This ongoing practice informs changes in our ESG governance, strategy, business model, operations, and sourcing activities.

Core elements of due diligence paragraphs in the Group sustainability statement

a) Embedding due diligence in governance, strategy and business model

ESG governance at F-Secure is described in the GOV-1 and GOV-2 sections. Our Leadership Team and Board of Directors oversee due diligence processes, with the Sustainability Council driving implementation. Due diligence considerations are integrated into our strategy and business model decisions.

b) Engaging with affected stakeholders in all key steps of due diligence

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, as described further under IRO-1 section.

c) Identifying and assessing adverse impacts

We identify potential impacts through our IRO assessment process outlined in the IRO-1 section. Our risk management is aligned with ISO-31000:2018 guidelines. No adverse impacts as described under "F-Secure impacts on people and the environment" have been identified.

d) Taking actions to address those adverse impacts

We address identified risks according to F-Secure's risk management policy, where risks have designated owners driving mitigation activities. We use risk modeling and quantification methods to identify and manage risks effectively, with proactive monitoring to build strategic resilience.

e) Tracking the effectiveness of these efforts and communicating

Each function tracks mitigation effectiveness and coordinates with relevant stakeholders. The Leadership Team and Audit Committee review risks biannually, while the Audit Committee regularly evaluates risk management process effectiveness. We communicate progress through our annual group sustainability report and regular stakeholder updates.

GOV-5 Risk management and internal controls over sustainability reporting

Control over sustainability matters is organized through policies, procedures, and processes developed by the sustainability function in collaboration with the Sustainability Council and relevant functions. These controls are approved by appropriate supervisory and management levels to support reliable and transparent sustainability reporting. The Audit Committee reviews Board-level policies and the group sustainability report preparation process, with the Code of Conduct and annual group sustainability report being approved by the Board of Directors.

Risk management and control processes in relation to sustainability reporting

F-Secure's internal control framework follows the Finnish Corporate Governance Code, covering policies, procedures, control activities, and monitoring. ESG is identified as a key process with specific internal controls for material topics. For sustainability reporting, we've implemented dedicated controls to ensure data accuracy, completeness, and reliability, including review procedures for ESG metrics before disclosure.

Internal control monitoring includes:

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

Risk assessment approach and main risks and mitigation strategies

The main identified risk related to sustainability reporting is the risk of reporting errors occurring, especially related to data points. Key risks related to data management and their controls are identified for each material topic and integrated into our internal controls matrix. Risks include ensuring climate change model updates are aligned with changes in accounting policy, talent acquisition/ retention data validation, business approvals outside of workday, validation of reported vulnerabilities data accuracy, assessing the number of security breaches/incidents involving AI tools, etc. Each data point has a defined person of responsibility, control, and testing mechanism. The Sustainability Council reviews these controls annually, ensuring alignment between our materiality assessment, risk management approach, reported data, and related controls.

The scope of reported data points has not changed since 2024. Some controls have been updated to better focus on the part of the process of data management where we have identified the greatest risk.

Main risks, mitigation strategies and controls:

Risk Identified	Management and Mitigation	Controls and Tracking
Risk of reporting errors, especially related to data points.	We have developed more detailed internal descriptions of datapoints for Own workforce in 2025 to mitigate risks of error.	Comprehensive internal controls for metrics and targets, which have been updated in 2025 from lessons learned last year.

Table 3. Main risks, mitigation strategies and controls.

Integration with company processes

Our internal controls support reliable reporting and regulatory compliance. Sustainability-specific data collection procedures and verification processes have been established for material ESG metrics to ensure accuracy. Risk management is integrated across all levels, from function-specific reviews to Leadership Team and Audit Committee oversight of the preparation of the group sustainability report. The ESG controls are owned and implemented by the sustainability function and developed in collaboration with control owners and the CFO office. The findings of the controls are documented by control owners and reviewed by the sustainability function. Failure of a control triggers control and/or process improvement, and this is evaluated on a case-by-case basis. The updated control catalogue is shared with the CFO office responsible for the group control matrix. The CFO office reports control findings to the Audit Committee.

Furthermore, every employee at F-Secure who is responsible for producing data or narrative for the group sustainability report is invited to several information sessions where process instructions are shared. In addition, a writing instruction document has been created to support the functions responsible for producing the narrative. To support functions responsible for data management, a step-by-step description of how to conduct internal controls has been made available. Each function takes responsibility and ensures instructions and processes are followed. The ESG governance, in conjunction with the risk management policy and internal controls, and detailed process descriptions, ensures that the relevant internal functions remain aware of their responsibilities and that actions are taken to mitigate the risk of reporting errors, with proper oversight from the Audit committee, Leadership Team and Sustainability Council.

Strategy

SBM-1 Strategy, business model and value chain

Product and services offering

F-Secure provides cybersecurity solutions for consumers to protect their digital moments. Our portfolio offering includes Security Suite (F-Secure Total) with endpoint security, scam protection, privacy protection, password management, and identity protection capabilities. Our Embedded Security offering is embedded in partners' existing or new apps to protect consumers. During the reporting period, F-Secure has expanded the protection capabilities in its portfolio, especially in scam protection.

While F-Secure sells Total directly to consumers, the entire portfolio is built to be "fit to channel sales" and allows the customer experience to be seamlessly integrated with our partner's go-to-market model, including co-branding and billing.

Furthermore, to support our partners, we offer a cloud-based Security Business Platform to drive growth, such as data-led business insights, marketing support and customer care support. In addition, our Partner Success teams support partners' go-to-market activities such as Marketing & Sales Enablement and Lifecycle Messaging Services.

Markets and customer groups served

Our end-customers are consumers seeking holistic, easy-to-use security solutions. We serve consumers directly and through approximately 200+ Service Provider partners (communication service providers, retailers, banks, and insurance companies). Revenue in 2025 was 82% through partners and 18% direct, with a geographical distribution shown in Table 4.

Revenue per geographic regions

Regions	2024 Revenue (M€)	2025 Revenue (M€)
Nordic countries	42.0	44.8
Rest of Europe	48.1	45.4
North America	45.5	44.3
Rest of the world	10.6	11.3
Total	146.3	145.7

Table 4. Revenue geographical distribution.

F-Secure belongs to the Technology - Software & IT Services ESRS sector. Our operations and profitability are reported as a single operating segment, and F-Secure's revenue in 2025 is 145.7 M€.

Employees per geographic regions

Regions	Employees 2024	Employees 2025
Nordic countries	280	274
Rest of Europe	67	58
North America	33	30
Rest of the world	149	187
Total	529	549

Table 5. Employees per geographic region.

Sustainability-related goals

Our strategy focuses on understanding human behavior to deliver effective security experiences and becoming the number #1 security experience company. We've shifted from point solutions to delivering all-in-one, holistic, and easy-to-use security applications or embedded protection in partners' offerings. Our portfolio strategy and delivering "brilliantly simple security experiences" approach allows us to ensure that we protect consumers and improve our product satisfaction scores (Net Promoter Score, NPS).

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.

Our channel-based go-to-market model through Service Providers creates the potential to reach hundreds of millions of consumers, prioritizing win-win partner relationships measured by revenue and partner satisfaction. 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 selling subscription-based consumer cybersecurity software products and services directly through our own e-commerce platform and app stores, as well as through our channel partners such as Communication Service Providers. Our high-level value chain, including notable actors, operations and stakeholders are visualized in the Value Chain and Actors figure below.

Upstream Operations

1. **Human Resources and Talent:** Attracting scarce cybersecurity expertise through strong employer branding
2. **Suppliers (Technology):** Strategic mix of in-house capabilities and third-party solutions
3. **Suppliers (IT):** Cloud infrastructure and business system providers
4. **Partnerships:** Collaborations with industry organizations and academia
5. **Financial:** Access to funding and addressing investor needs through profitable growth
6. **Regulatory Compliance:** Monitoring ESG, AI and data privacy regulations

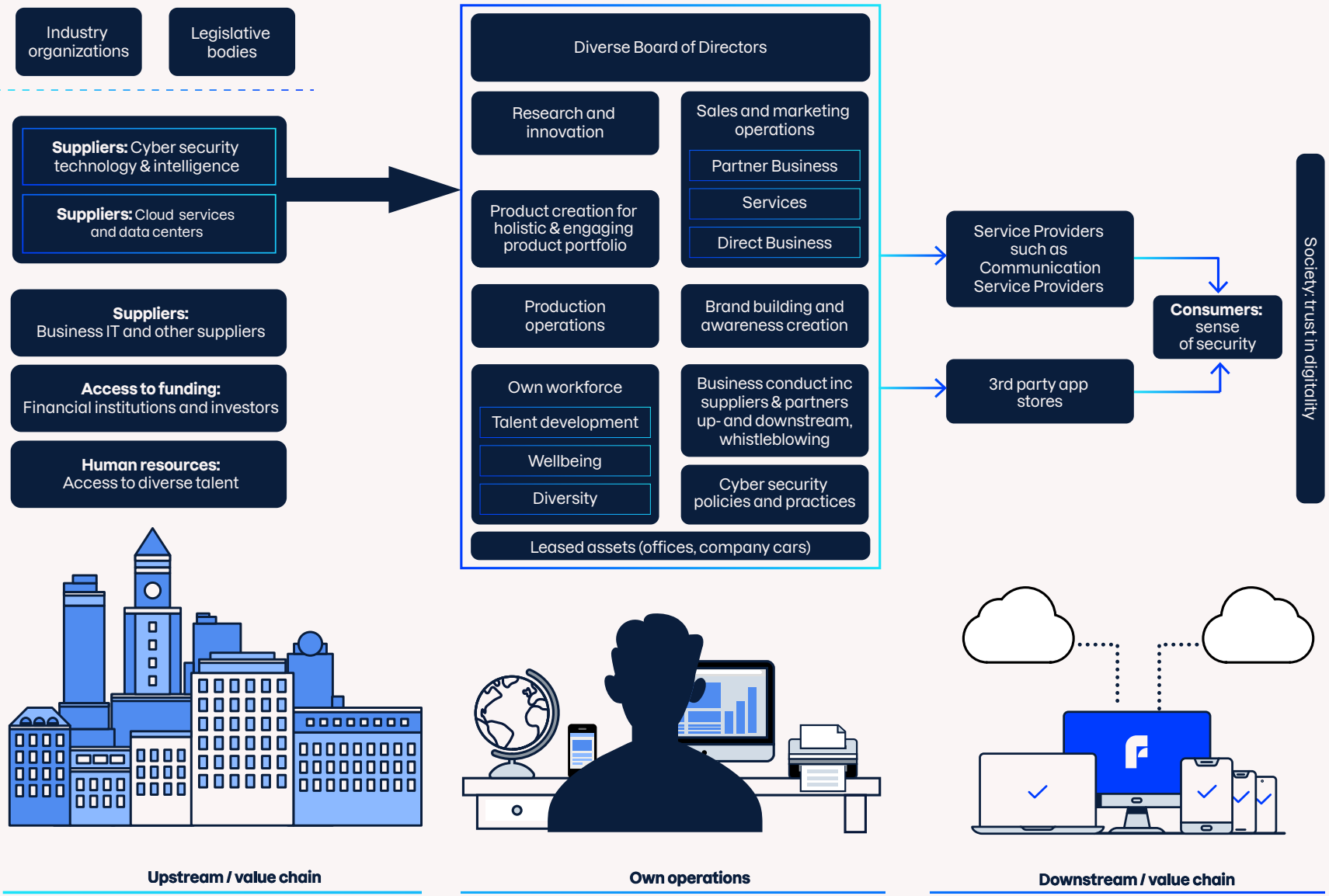
Core Operations

1. **Product Development:** Research and innovation, setting portfolio vision, roadmap, and product creation and maintenance
2. **Partner Sales:** Primary sales channel through Service Providers
3. **Direct Consumer Sales:** Revenue source and consumer insight generator
4. **Services:** Delivery, production, operations, customer care, and partner success services
5. **Trust Foundation:** Secure data handling, operations and ethical business conduct
6. **Talent Development:** Employee well-being and diversity initiatives
7. **Business Support:** Finance, HR, Legal and other enabling functions
8. **Governance:** Board-level strategic direction and oversight

Downstream Operations

1. **Partner Channel**: Partnerships with Service Providers to deliver security as a core service or a value-added service, creating a new revenue stream and positively impacting their core business, customer retention, and brand relevancy
2. **Direct Distribution Channels**: Consumer security services made available through our own e-Commerce platform and third-party app stores (Apple and Google)

Figure 2. F-Secure Value Chain.



SBM-2 Interest and views of stakeholders

	Stakeholder expectations	How engagement is organized	F-Secure actions and outcome from engagement
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 Renewing relevant ESG ratings, ESG targets and progress available on webpagese
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 Wellbeing and Committee Employee-elected board member Townhalls and trainings	Increase internal Sustainability communication Organize first Sustainability day Improvement of personal development dialogues Update of of Wellbeing committee and launch of wellbeing hour every week Development of F-Secure sustainable AI framework.
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 updated ESG training of sales improving dialogue with partners ESG training of sales improving dialogue with partners SBTi Commitment
Consumers 	High level of protection for good price Understanding customer needs Knowledge about cybercrime Reliable and simple solution	Customer support and guidance Surveys	ProduESG webpage update Improve EcoVadis rating 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	Flexibility to changing regulatory environment Value creation and risk mitigation
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 Procurement policy of conduct covering main sustainability topics Launch of supplier environmental data gathering program as part of GHG emission mitigation strategy

Table 6. F-Secure stakeholder map.

Through ongoing dialogue and engagement with our stakeholders, we strive to understand our stakeholders' 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. As part of our Double Materiality Assessment review, we engaged key stakeholders, including financial institutions, our workforce, end-customers, the Board, and sales providing channel partners, while also analyzing regulatory requirements.

While the DMA review didn't result in material changes to our strategy or business model, we expect stronger stakeholder relationships through regular dialogue and complementary ESG agendas, particularly with Service Providers. We'll continue acting transparently, pursuing our goals and fostering future stakeholder collaboration.

Informing internal stakeholders on stakeholder interests

Stakeholder feedback has been reviewed by the Sustainability Council, which includes several Leadership team members. Our Sustainability Council regularly reviews and updates DMA and IROs, and management bodies will be informed of any significant stakeholder feedback changes affecting strategy and business model. We'll continue considering feedback in our risk management process and annual strategy reviews.

Consumer interests

For clarity, within the context of this Group sustainability report, the terms "consumer" and "end-user" should be treated as synonyms unless explicitly stated otherwise.

F-Secure conducts regular consumer and market surveys to align product roadmaps with needs, gathering additional feedback through customer care and Service Providers. Market studies and consumer insights inform both product and channel strategies, with 81% of consumers expecting security services from internet providers. We simplify security by embedding it in partners' apps, eliminating the need for consumers to download new applications.

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

Own Workforce interests

F-Secure involves its workforce in the Double Materiality Assessment, regularly gauges well-being, and obtains feedback on current events and company strategy. These results are reviewed 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 respects its value chain workers' human rights through supplier Code of Conduct and partner agreements, focusing on fair labor practices, safe working conditions, and 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 creates positive social impact through its core business of protecting people from cybersecurity threats via its consumer security products and services. The company extends this impact by providing free tools and educational resources to raise society-wide awareness of cyber threats.

For its workforce, F-Secure prioritizes employee well-being through equal treatment and professional development opportunities. The company fosters an open culture where employees are encouraged to speak up, supported by a whistleblower channel that ensures concerns can be raised without fear of retribution.

Environmentally, while F-Secure currently deploys solutions on climate-neutral platforms like AWS, the company recognizes future challenges as AI adoption and customer growth increase energy demands. This drives the company's focus on green coding practices to minimize environmental impact as operations scale.

Standard	Type	Description	Time horizon
Environment	Potential positive impact (OO)	Implementation of green coding principles can reduce battery use in consumer devices and computational power in cloud environments	Long-term
Social	Actual positive impact (OO)	Protect consumers' digital moments with relevant, effective cybersecurity solutions	Short-term, mid-term and long-term
	Actual positive impact (DVC, OO)	Create awareness about cybercrimes through campaigns, and events	Short-term, mid-term and long-term
	Actual positive impact (OO)	Family leaves (sometimes exceeding local requirements) and enhancing work life balance of employees.	Short-term
	Actual positive impact (OO)	Promote gender equality through recruitment and gender pay gap mitigation	Short-term
	Actual positive impact (OO)	Further ramp up strategic learning and development activities and track investment into learning activities.	Short-term
	Actual positive impact (OO)	Foster inclusive culture with speak-up environment where workplace is safe for everyone	Short-term
	Potential positive impact (OO)	Continuously identify the internal competencies critical to our strategy	Mid-term
Governance	Actual positive impact (OO/DVC)	Whistleblower channel available to all employees and business partners	Short-term, mid-term and long-term
	Actual positive impact (OO)	F-Secure is strengthening its culture by reviewing people and culture structures to reflect the desired culture, supporting leadership and team development, and fostering a culture of experimentation	Short-term

Table 7. F-Secure impacts.

Standard	Type	Description	Time horizon
Environment	Risk (DVC/OO)	Failure to meet climate change mitigation targets may negatively impact channel business	Mid-term and Long-term
Social	Opportunity (OO)	Evolving threat landscape, protecting consumers against evolving threat landscape (for example scams) benefits both F-Secure and partners	Short-term, mid-term and long-term
	Opportunity (OO)	Use data and AI in security applications, for more effective protection and better user experience. AI-powered (network) monitoring tools can track user behavior, detect anomalies, and react accordingly.	Short-term, mid-term and long-term
	Opportunity (OO)	Enhance employer reputation through DEI activities to attract younger generations	Mid-term and Long-term
	Opportunity (OO)	Use of AI in workforce development, including process improvements, competency maturity and AI sentiment	Long-term
	Risk (DVC)	Channel strategy, significant agreement changes or existing partner loss can negatively impact outlook	Short-term, mid-term and long-term
	Risk (OO)	Decreasing consumer willingness to pay for premium security due to competition/ economic situation	Short-term, mid-term and long-term
	Risk (OO)	Talent acquisition and retention, loss of key persons or inability to acquire new talent	Short-term, mid-term and long-term
	Risk (OO, DVC/UVC)	Security vulnerabilities from suppliers and partners, relying on external vendors, especially vendors who are one step removed in the supply chain, adds layers of vulnerability.	Short-term, mid-term and long-term
	Risk (OO)	Cybersecurity attacks impacting reputation and business	Short-term, mid-term and long-term
	Risk (OO)	Mental health related absences detected.	Mid-term and Long-term
	Risk (OO)	AI increases risk of security breach, effective AI experimentation and roll-out dependent on high quality data sources and may also increase risk of a security breach.	Short-term, mid-term and long-term
Governance	Risk (DVC)	Partnership business, use of agents and other intermediaries increases bribery and corruption risk.	Short-term, mid-term and long-term
	Risk (DVC/UVC ,OO)	Anti-Bribery and Corruption risks increase as a result of M&A transactions due to limited understanding of the target.	Mid-term and Long-term

Table 8. F-Secure risks and opportunities.

Interaction with strategy and business model

F-Secure sustainability commitments

The positive impacts related to consumers and end-users are directly linked to F-Secure's purpose, the reason why we exist, and thereby with our business model and strategy. We are in the business of protecting consumers' digital moments against cyber threats, especially scams, directly and through our partners.

F-Secure's ambition for the long term is to increase our positive impact further globally based on our growth strategy of i) continuously expanding how we protect consumers' digital moments and ii) increasing reach and scale through our Service Provider partners. We continue to see end-customers turning to Service Providers for protection, while our partners see consumer security as an integral part of their brand promise and a business opportunity. Therefore, in every aspect of our operations, we emphasize responsible business as trust is foundational in our industry and applies to both our partners and consumers.

Positive social sustainability- and governance-related impacts have already materialized, and we see them having an increasingly positive impact also in the long term. 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 strategy is directly informed by our most material positive impact: Protecting consumers' digital moments. Our continuous and comprehensive analysis of the threat landscape and consumer needs guides product investments, go-to-market and marketing strategies, and channel partnerships. We also see the rapidly evolving threat landscape as a growth opportunity, creating further need for effective scam protection and leveraging AI capabilities.

Employees turn our strategy into cohesive execution plans. To support these plans, our culture program, DEI initiatives, and employee well-being strategies mitigate risks related to talent acquisition and retention while making positive impacts on our workforce. We've implemented gender pay gap adjustments and are fostering an inclusive culture with speak-up values.

To maintain trust in the cybersecurity industry, we've improved vulnerability management processes and maintain high standards supported by our ISO27001 certification, which was validated again during 2025. Our Code of Conduct awareness programs address business ethics risks, which is fundamental in building trust.

For climate change, we're developing reduction pathways across Scope 1-3 emissions, focusing on supplier engagement, green energy use and electric vehicle adoption to reach our 2030 reduction targets.

Effects on F-Secure's financial position

Management has not recognized that F-Secure's material risks and opportunities have affected the undertaking's most recently reported financial performance, financial position and cash flow, or identified any material risks and opportunities for which there is a significant risk of a material adjustment within the next annual reporting period to the carrying amounts of assets and liabilities reported in the related financial statements.

Resilience addressing material IROs

F-Secure's strategy and business model are considered resilient to address material impacts and risks, and leverage opportunities identified as part of our strategy process for the next strategy period (2026–2028), 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 and mitigate key risks.

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, see Section *S4-5 Progress towards targets* for more detailed information on methodology and estimation uncertainty. 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 exceed the threshold for financial impact (see section IRO-1).

In short, and based on our double-materiality analysis, these entity-specific disclosure requirements apply to S4 Consumers and End-Users, see table *Consumers and end-users list of IROs* for the specification of those impacts, risks and opportunities.

Changes to the material impacts, risks and opportunities compared to the previous reporting period

Change	Description	Topic
Risk (DVC) removed	Removing: DEI Partner retention and acquisition related to DEI requirements", risk due to change in US politics.	Own Workforce
Risk (OO) added	"Effective AI experimentation and roll-out dependent on high quality data sources and may also increase risk of a security breach."	Consumers and end-users
Risk (DVC) Removed	Tier 1 partnership risk removed as it is seen as more of a pure business risk rather than a sustainability-related risk.	Consumers and end-users
Opportunity (OO) removed	Set policy for e-cars opportunity removed as it was more of an impact and as such does not reach the financial threshold of materiality.	Climate change
Opportunity (OO) removed	Expand use of worktime tracking at APAC level removed as it does not reach the threshold of financial materiality.	Own Workforce
Opportunity (OO) changed to potential positive impacts	Critical strategic competences opportunity changed to potential positive impact as it represents a potential positive effect on people.	Own Workforce
Opportunity (OO) changed to actual positive impacts	Learning and development changed to actual positive impact as it has a positive impact on our employees as it represents a positive effect on people.	Own Workforce
Opportunity (OO) added	Use of AI in workforce development: Process improvements, competency maturity and AI sentiment	Own Workforce
Opportunity (OO) changed to actual positive impacts	F-Secure is strengthening its culture by reviewing people and culture structures to reflect the desired culture, supporting leadership and team development, and fostering a culture of experimentation	Governance

Table 9. Changes in impacts, risks and opportunities since last reporting year.

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 2022 and refined it in 2023-2024, aligning with the final European Sustainability Reporting Standards and EFRAG guidance. The assessment follows these principles:

- ESG matters based on EFRAG standards, with SFRD and NFI regulations reviewed
- Sector and entity-specific topics assessed when relevant, particularly for cybersecurity
- Double materiality approach considering impacts on F-Secure and F-Secure's impacts on sustainability
- Use of quantitative and qualitative thresholds for IROs
- Engagement with affected stakeholders to inform the process
- Cross-cutting matters reported regardless of materiality assessment outcome

Critical input came from dialogue with key stakeholders, including Service Provider partners, investors, bankers, our workforce, consumers, suppliers, and regulators, as described under 1.3.2 SBM-2 Interest and views of stakeholders. We applied EFRAG guidance and expert interpretation to develop scoring matrices identifying material sustainability matters.

F-Secure recognizes that impacts, risks, and opportunities are interdependent and form an interconnected system. This understanding shapes the company's approach to sustainability management and governance, which is integrated into business strategy and risk management. For example, understanding that consumer protection impact depends on partner relationships, which creates both risks towards partnership channel and opportunities through, for example, increasing awareness, which can increase positive impacts.

In 2025, we reviewed the Double materiality assessment with internal relevant functions and conducted stakeholder engagement with our own workforce, financial institutions, and sales to get the partner point of view to ensure all IROs are up to date.

Material ESG Topics

Based on our assessment, we identified the following material 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 10. F-Secure material topics.

After screening the locations, we did not identify material impacts, risks or opportunities related to pollution, water resources, biodiversity, or resource use. We have no operations near biodiversity-sensitive areas or activities negatively impacting land. Both own operations and value chain have been assessed as part of the double materiality assessment. The assessment methodology was the same for all topics and has been described in section IRO-1, *Double Materiality Assessment Methodology.*

The scope of topics assessed as material has not changed since 2024.

Business Conduct Assessment

We assessed business conduct on a global level, considering M&A activities and operations in countries with elevated corruption risks. The financial impact of potential unethical behavior is estimated to reach the thresholds of materiality, but the likelihood is assessed as low. 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.

Financial Effects of Risks and Opportunities

The assessment of risks and opportunities with potential financial effect was based on thresholds for financial materiality (magnitude) and likelihood. 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.

Assessment Process

When assessing IROs, we focused on areas where impacts, risks and opportunities are likely to arise based on our activities, relationships, and geographies. Both own operations and value chain have been assessed as part of the double materiality assessment. We indicate whether impacts and risks are in our own operations (OO) or value chain; Downstream (DVC) and Upstream (UVC), and whether impacts are positive or negative. Impacts were assessed using the scale and scope criteria presented in Table 11. Where impacts were potential rather than actual, likelihood was also assessed. For negative impacts, the assessment additionally considered remediability.

Material items exceeded one or more thresholds: strong stakeholder request, financial impact, scope/scale of event impact, or likelihood. A topic was considered material if it scored '3' in any category or met the financial impact threshold. The Double materiality assessment has been reviewed by the Sustainability Council and the Audit Committee and approved by the Board of Directors. The assessment process and methodology have not changed since the last reporting period.

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.

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 11. Description of assessment methodology.

Decision-Making Process and Internal Controls

Our Sustainability Council reassesses our DMA and IROs regularly. Updating of controls is presented to the Sustainability Council and Financial Controlling. The Council is informed of any control failures and presents risk mitigation actions. Depending on the nature of the control failure, the Audit Committee may be informed. The internal control procedure is described in more detail in section *GOV-5 Risk management and internal controls over sustainability reporting.*

F-Secure's risk management is a continuous process, with material sustainability risks included in our company-wide top 9 risk map. Each Leadership Team member is accountable for risk management in their functions.

Integration with Risk Management Process

Our Risk Management Policy explicitly requires evaluating the short-, medium- 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 responsibility of keeping our DMA relevant and up to date lies with F-Secure's Sustainability Council, through annual reviews. 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.

Process to identify and assess climate-related impacts, risks and opportunities

F-Secure conducted a systematic assessment of climate-related impacts, risks, and opportunities as part of the double materiality assessment process. The identification process incorporated collaboration with internal functions, stakeholder engagement, and review by the Sustainability Council.

Physical Risk Assessment

F-Secure screened climate-related hazards to determine whether assets or business activities may be exposed to these hazards. The assessment considered F-Secure's operational footprint across different geographic locations, evaluating vulnerability based on regional climate risk profiles. Given the company's limited physical asset base as a cloud-based software provider, physical risks were assessed as having limited materiality. The analysis considered both acute events, such as flooding, and chronic conditions, such as heat stress, particularly for locations with higher vulnerability, such as India and Malaysia.

Transition Risk Assessment

The process to identify transition risks evaluated policy and legal developments, technology shifts, market changes, and reputational factors. F-Secure assessed potential impacts across short-term, medium-term, and long-term horizons, aligned with standard financial planning periods. The assessment considered F-Secure's value chain, with particular focus on Scope 3 emissions representing over 90% of total emissions.

Use of scenarios in the process and consideration of limiting global warming to 1,5 degrees

F-Secure developed three climate scenarios aligned with IPCC AR6 pathways to test strategy resilience: Orderly Transition (SSP1-2.6), Disorderly Transition (SSP2-4.5), and Hot House World (SSP5-8.5). This scenario analysis examined how climate-related risks might materialize under different futures, with specific consideration of pathway limiting global warming to 1.5-2°C consistent with Paris Agreement objectives.

The scenarios evaluated critical uncertainties, including policy implementation speed, stakeholder expectations evolution, and supply chain decarbonization pace. Through this process, F-Secure identified reputational risk from failing to meet emission reduction targets as the primary material climate risk, given stakeholder expectations and the company's dependency on supply chain emission reductions to achieve its target by 2030. The scenarios confirmed that physical risks exist and may increase over time, but they remain below the materiality threshold compared to transition risks.

IRO-2 Disclosure requirements

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

Topic	Disclosure requirements	Index
General disclosure		
Basis for preparation	BP-1 – General basis for preparation of sustainability statements	05
Basis for preparation	BP-2 – Disclosures in relation to specific circumstances	05-06
Governance	GOV-1 – The role of the administrative, management and supervisory bodies	07-09
Governance	GOV-2 – Information provided to and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies	09-11
Governance	GOV-3 - Integration of sustainability-related performance in incentive schemes	11-12
Governance	GOV-4 - Statement on due diligence	12-12
Governance	GOV-5 - Risk management and internal controls over sustainability reporting 3. Strategy	12-13
Strategy	SBM-1 – Strategy, business model and value chain	12
Strategy	SBM-2 – Interests and views of stakeholders	17
Strategy	SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model	19-22
Impact, risk and opportunity management	IRO-1 - Description of the processes to identify and assess material impacts, risks and opportunities	23
Impact, risk and opportunity management	IRO-2 – Disclosure requirements in ESRS covered by the undertaking's sustainability statement	26-33

Topic	Disclosure requirements	Index
Environment		
Climate change	GOV-3 Integration of sustainability related performance in incentive schemes	11-12
Climate change	E1-1 Transition plan for climate change mitigation	46
Climate change	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	19-22
Climate change	IRO-1 Description of the processes to identify and assess material climate-related impacts, risks and opportunities	25-26
Climate change	E1-2 Policies related to climate change mitigation	48
Climate change	E1-3 Actions and resources in relation to climate change policies	49-50
Climate change	E1-4 Targets related to climate change mitigation	50-51
Climate change	E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions	51
Social		
Own workforce	SBM-2 Interests and views of stakeholders	18-18
Own workforce	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	19-22
Own workforce	S1-1 Policies related to own workforce	58-60
Own workforce	S1-2 Processes for engaging with own workers and workers' representatives	60-61
Own workforce	S1-3 Processes to remediate negative impacts and channels for own workers to raise concerns	61

Topic	Disclosure requirements	Index
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	61-64
Own workforce	S1-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	64-65
Own workforce	S1-6 Characteristics of the undertaking's employees	66-66
Own workforce	S1-9 Diversity metrics	68
Own workforce	S1-13 Training and skills development metrics	69
Own workforce	S1-14 Health and safety metrics	69
Own workforce	S1-15 Work-life balance metrics	69
Own workforce	S1-16 Remuneration metrics	70
Own workforce	S1-17 Incidents, complaints and severe human rights impacts	70
Consumers and end-users	SBM-2 Interests and views of stakeholders	71-81
Consumers and end-users	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	71
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	73
Consumers and end-users	S4-3 Processes to remediate negative impacts and channels for consumers and end-users to raise concerns	75
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	76-79
Consumers and end-users	S4-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	79-81
Governance		
Business conduct	GOV-1 The role of the administrative, supervisory and management bodies	07-09
Business conduct	IRO-1 Description of the processes to identify and assess material impacts, risks and opportunities Impact, risk and opportunity management	23
Business conduct	G1-1 Corporate culture and business conduct policies	85-86
Business conduct	G1-3 Prevention and detection of corruption or bribery	86-87
Business conduct	G1-4 – Confirmed incidents of corruption or bribery	87-87

Table 12. Topic Disclosure requirements Index.

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]		07
ESRS 2 GOV-1 Percentage of board members who are independent paragraph 21 (e)			Delegated Regulation (EU) 2020/1816, Annex II		07
ESRS 2 GOV-4 Statement on due diligence paragraph 30	Indicator number 10 Table #3 of Annex 1				12
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)	46
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		47

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		50
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)		51
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)		54
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 2025
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 2025

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 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 2025
ESRS E1-9 Degree of exposure of the portfolio to climate related opportunities paragraph 69			Delegated Regulation (EU) 2020/1818, Annex II		Omitted 2025
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
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

Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
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 applicable to F-Secure
ESRS 2- SBM3 - S1 Risk of incidents of child labour paragraph 14 (g)	Indicator number 12 Table #3 of Annex I				Not applicable to F-Secure
ESRS S1-1 Human rights policy commitments paragraph 20	Indicator number 9 Table #3 and Indicator number 11 Table #1 of Annex I				59
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		58-60
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				60
ESRS S1-3 grievance/complaints handling mechanisms paragraph 32 (c)	Indicator number 5 Table #3 of Annex I				61
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		69
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 2025
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		70
ESRS S1-16 Excessive CEO pay ratio paragraph 97 (b)	Indicator number 8 Table #3 of Annex I				70

Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS S1-17 Incidents of discrimination paragraph 103 (a)	Indicator number 7 Table #3 of Annex I				70
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)	70-70
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 applicable to F-Secure
ESRS S2-1 Human rights policy commitments paragraph 17	Indicator number 9 Table #3 and Indicator n. 11 Table #1 of Annex 1				18
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				Not material
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				73

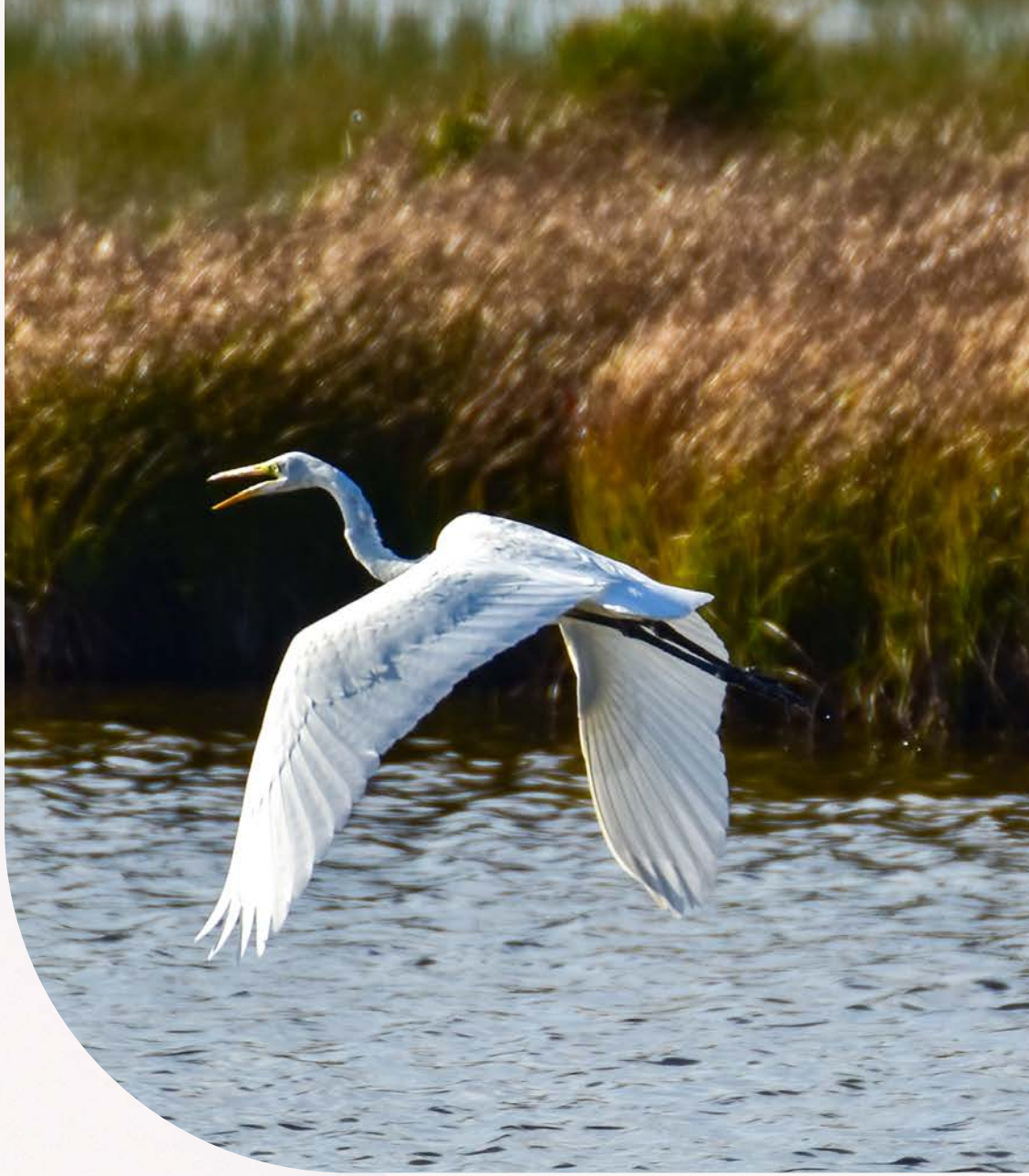
Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS S4-1 Non-respect of UNGPs on Business and Human Rights and OECD guidelines paragraph 17	Indicator number 10 Table #1 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II Delegated Regulation (EU) 2020/1818, Art 12 (1)		73
ESRS S4-4 Human rights issues and incidents paragraph 35	Indicator number 14 Table #3 of Annex 1				78
ESRS G1-1 United Nations Convention against Corruption paragraph 10 (b)	Indicator number 15 Table #3 of Annex 1				85-86
ESRS G1-1 Protection of whistle-blowers paragraph 10 (d)	Indicator number 6 Table #3 of Annex 1				85-86
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		87
ESRS G1-4 Standards of anti-corruption and anti-bribery paragraph 24 (b)	Indicator number 16 Table #3 of Annex 1				87

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).

Table 13. Disclosure Requirement and related datapoint SFDR reference.

GROUP SUSTAINABILITY REPORT -

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 offers. 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 the 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. 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.

EU Taxonomy disclosure, reporting change from 2024; IFRS 16 Leases are included in Capex instead of Opex. At the same time right-of-use assets related depreciations are excluded in Opex.

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 is based on our financial statement (Cross-reference to financial section 3. Revenue).

Turnover

Financial year 2025		2025		Substantial contribution criteria						DNSH criteria									
Economic Activities	Code(s)	Turnover	Proportion of Turnover 2025	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		145,739	100.0 %																
TOTAL		145,739	100.0 %																

Operating expenditure

The operating expenses (0.720 MEUR) included in the taxonomy assessment are defined as direct non-capitalized 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 the maintenance of premises are included. F-Secure utilizes the third-party cloud platforms of Amazon Web Services (AWS) and Microsoft Azure for the majority of its operations. Cloud hosting costs are not included in the operating expenses, subject to the 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 2025		2025			Substantial contribution criteria						DNSH criteria									
Economic Activities	Code(s)	OpEx	Proportion of OpEx 2025	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		720	100.0 %																
TOTAL		720	100.0 %																

F-Secure

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 are 17.799 MEUR in total. Capital expenditure includes capitalizations of development expenditure on new products or product versions with significant new features, partially or completely internally developed intangible assets that relate, for example, to platforms and software licenses. These are intangible assets according to the IAS 38 accounting standard. Capital expenditure also includes right-of-use assets according to IFRS16 Leases. A minor part of capital expenses relates to capitalization of employee laptops and other hardware, as well as office furniture and 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 is based on our financial statement (Cross-reference to financial section 14. Non-current assets).

Capital expenditure

Financial year 2025		2025			Substantial contribution criteria						DNSH criteria									
Economic Activities	Code(s)	CapEx	Proportion of CapEx 2025	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		17,799	100.0 %																
TOTAL		17,799	100.0 %																

F-Secure

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

Table 14. Involvement with nuclear energy and fossil fuel generating activities.

E1 – Climate change

SBM-3 Material impacts, risks and opportunities

	Material impact, risk or opportunity	Description
Climate change mitigation		
Risk (OO)	Failure to meet climate change mitigation targets may negatively impact channel business	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.

Table 15. Climate change list of IROs.

Interaction with strategy and business model

F-Secure's climate resilience analysis covers its own operations, upstream and downstream value chain activities. The resilience analysis covers transition risks, including policy and regulatory developments, technology changes, market requirements, and reputational risks related to climate mitigation targets. Physical risks assessed are marked with "x" in *Table 16, Climate SBM-3 physical risks*. Physical risks in locations with fewer than 20 employees have been excluded from the analysis due to limited operational footprint and the absence of owned assets in these areas. 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 physical risks

F-Secure has assessed and defined its strategic response to climate change through scenario analysis aligned with limiting global warming to 1.5°C in accordance with the Paris Agreement. The assessment confirms that F-Secure's existing business model remains compatible with this pathway when complemented by targeted climate mitigation measures integrated into current operational processes and strategy. The details of this strategic response are disclosed in the section *Ability to adapt strategy and business model to climate change.*

	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 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. National and international policies will be crucial in promoting GHG emission reductions and supporting renewable energy adoption.

Key Transition Events

Using the STEEP framework, we identified the following key driving forces that could impact F-Secure's climate strategy:

STEEP Category	Driving Force
Social	Rate of change in partner and investor climate expectations Increasing stakeholder pressure for transparency
Technological	Pace of decarbonization in IT supply chains Energy efficiency improvements in data centers
Economic	Evolution of carbon pricing mechanisms Cost of human labor
Environmental	Physical climate impacts on operations in vulnerable regions Supply chain disruption from extreme events
Political	Speed and stringency of global climate policy implementation Degree of divergence in regional climate approaches

Table 17. Key driving forces.

The only material transition risk identified is reputational risk from failing to meet mitigation targets aligned with the Paris Agreement, which could affect stakeholder expectations. This risk is significant because 97% of F-Secure's emissions come from Scope 3 categories, making emission reduction heavily dependent on supply chain performance.

Time horizons, climate scenarios and reduction targets

F-Secure has set a GHG reduction target for 2030 and developed a transition plan with defined reduction pathways and annual actions. We use scenarios as a tool to analyze environmental resilience, with time horizons for 2030. Our scenario analysis follows TCFD methodology and incorporates the latest IPCC AR6 findings to evaluate three distinct scenarios:

1. **Orderly Transition (SSP1-2.6)**: Coordinated global climate policy with gradual carbon price increases by 2030. Partner SBTi commitments rise steadily from approximately half by mid-decade to a significant majority by 2030. Supply chain costs increase moderately. F-Secure's 52% intensity reduction target is achievable with systematic supplier engagement requiring moderate annual investments, generating positive returns through market differentiation and potential modest revenue premiums in enterprise segments.
2. **Disorderly Transition (SSP2-4.5)**: Fragmented policy until 2027-2028, then sudden, stringent responses. Carbon prices spike dramatically within 18 months. Partner requirements accelerate abruptly, potentially threatening material revenue if unmet. Supply chain costs surge significantly. Target achievement faces a moderate to high failure probability, requiring substantially increased emergency investments from 2027. Non-compliance penalties could reach material percentages of global turnover.
3. **Hot House World (SSP5-8.5)**: Weak, fragmented policy with low carbon prices. Market segmentation creates divergent standards: a significant minority of partners (primarily EU/US West Coast) require science-based targets, while others maintain business-as-usual. Physical disruptions cause several days of annual supply chain disruption by 2030, moderately increasing costs. F-Secure risks exclusion from a portion of EU/Nordic enterprise RFPs without climate credentials. Target achievement depends on internal commitment, requiring higher annual investments justified primarily through market access rather than regulatory compliance.

Physical risks were not found to be significant as F-Secure has no assets in high-risk regions. The majority of employees are located in Finland and other Nordic countries with relatively mild projected climate impacts, while some limited exposure exists in India and Malaysia. For transition risks, we identified reputational risk if we fail to meet Paris Agreement-aligned targets.

Utilization of scenario analysis and transition plan

The utilization of F-Secure scenario analysis is to answer the focal and secondary questions that F-Secure has on climate change related to its own business and strategy:

Focal Question:

- "If F-Secure fails to meet its climate change mitigation target of reducing emission intensity by 52% by 2030, what would be the strategic and financial implications under different climate futures, and what actions should be taken to address these risks?"

Secondary focal questions:

- "How will climate-related transition risks, particularly stakeholder expectations, evolve over different time horizons and scenarios?"

- "What strategic and operational adjustments are needed to ensure F-Secure can meet its climate targets under different climate futures?"
- "What climate-related opportunities might emerge for F-Secure under different scenarios?"

A climate transition plan is utilized as a strategic roadmap that guides a company's pathway toward aligning its business model and operations with the transition to limit global warming to 1.5°C in line with the Paris Agreement. The transition plan translates climate commitments into actions, resource allocations, and governance mechanisms across business functions through clear decarbonization levers and implementation timelines.

Anticipated financial effects

Regarding material transition risks related to supply chain dependency, F-Secure may face economic impacts if we fail to meet climate targets aligned with stakeholder expectations. While specific financial impacts vary across scenarios, our analysis shows that meeting our 52% intensity reduction target requires different levels of investment and supplier engagement in each scenario, with the disorderly transition presenting the highest potential costs.

Results of the resilience analysis

F-Secure is considered climate resilient due to our business nature as a software company. Our current strategy aligns well with an orderly transition scenario, providing sufficient time to implement emissions reductions methodically. However, our strategy would face some challenges in a disorderly transition due to abrupt policy changes and rapidly evolving partner requirements. In a hot-house world scenario, our strategy would likely not meet its targets due to limited transition pressure in the supply chain.

Key strengths include our current emissions tracking approach and early work on emissions inventory. Vulnerabilities include heavy supply chain dependency in reaching the scope 3 target.

Performance Under Orderly Transition: F-Secure's current strategy aligns well with this scenario, providing sufficient time to implement emissions reductions in a measured way.

Performance Under Disorderly Transition: F-Secure's current strategy would face challenges in this scenario due to the abrupt policy changes and rapidly evolving partner requirements.

Performance Under Hot House World: The current strategy would likely not meet its targets in this scenario due to limited transition pressure in the supply chain, and would face increasing physical impacts, particularly in vulnerable locations.

Strategic response: ability to adapt strategy and business model to climate change

F-Secure's ability to adapt is embedded in our dynamic strategy process. Based on the scenario analysis, F-Secure has identified strategic measures to enhance climate resilience:

1. **Enhanced Supplier Emissions Data Collection**: Implementing systematic data collection from major suppliers and integrating climate criteria into supplier selection.
2. **Climate Governance Strengthening**: Establishing clear responsibilities through our Environment Committee and maintaining voluntary climate disclosure regardless of F-Secure is in scope of CSRD.
3. **Formal Science-Based Target Commitment**: Submitting commitment to the Science-Based Targets initiative near-term target and considering long-term net-zero target for the future.
4. **Low-Carbon Service Differentiation**: Developing green coding initiatives and a sustainable AI use framework.
5. **Climate Transition Contingency Planning**: Maintaining rapid response protocols for policy changes and financial reserves for climate initiatives.
6. **Partner Requirement Anticipation**: Establishing early warning systems for changing partner requirements through sales surveys.
7. **Distributed Work Enhancement**: Maintaining a strong remote work infrastructure and flexible arrangements for climate disruptions.

Our strategic response includes near-term (0-2 years, 2024-2026) actions like enhanced supplier emissions data collection and climate governance strengthening, alongside medium-term (2-5 years, 2026-2029) initiatives such as establishing a long-term net-zero target and implementing climate transition contingency planning.

We track emerging trends and adapt our strategy accordingly, ensuring ongoing resilience to evolving climate risks and opportunities.

Conclusion of scenario analysis

The scenarios highlight the importance of supplier engagement, given that over 90% of F-Secure's emissions are in Scope 3 categories. They also underscore the need for flexibility in implementation timelines and approaches, as the pace and nature of the climate transition remain uncertain.

Drawing on the IPCC AR6 finding that "there is a rapidly closing window of opportunity to secure a liveable and sustainable future for all," F-Secure's recommended strategy emphasizes early action on governance, sudden changes in requirements, and supply chain management while building capabilities to adapt to different potential futures. By implementing this strategy, F-Secure can enhance its climate resilience while positioning itself to thrive in a range of possible futures.

This scenario analysis will be reviewed annually to account for new developments in climate science, policy, technology, and market expectations, ensuring F-Secure's strategy remains resilient to evolving climate risks and opportunities.

E1-1 Transition plan for climate change mitigation

During 2025, F-Secure has continued to develop the details of the transition plan for climate change mitigation covering Scope 1, 2 and 3. The transition plan implementation is in the initial phase, with the four decarbonization levers disclosed under section *E1-3 and E1-4 and key actions planned,* which include operationalized implementation roadmaps. Governance oversight is established through the Environment Committee (operational Q3 2024), with bi-annual Sustainability Council reviews and annual Board reporting, ensuring accountability. Each decarbonization lever has assigned functional ownership, time-bound milestones, and defined expected impact by 2030.

Reference to GHG emission reduction targets: Paris Agreement

F-Secure has set key greenhouse gas (GHG) emissions reduction targets in line with the Paris Agreement, limiting global warming to 1.5°C. We've adopted the Greenhouse Gas Protocol and CSRD as our framework for measuring and managing emissions, targeting 42% absolute reduction across Scope 1, 2, and 52% emission intensity reduction of Scope 3, between 2024 and 2030, with 2024 as our base year. These targets align with IPCC 1.5°C Pathways. Sectoral decarbonization standards are not yet available for IT and Software companies.

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

Decarbonization Lever	2025	2026-2027	2028-2030	Expected Impact by 2030
Fuel switching	Begin phasing in electric and hybrid vehicles	Continue fleet transition to hybrid/electric	Complete transition to 100% electric/hybrid fleet	55% reduction in fleet emissions (17 tCO_2e)
Renewable energy and energy efficiency	Prefer renewable energy in current and new lease agreements, especially in controlled facilities			40% reduction from 2024 baseline (75tCO_2e)
Supply chain decarbonization	Include sustainability into F-Secure procurement policy	Include sustainability in supplier selection process	Widen scope of suppliers included in supplier sustainability program	52% reduction in emission intensity of Scop 3
Green coding principles	Develop sustainable AI framework Begin developer training	Implement architecture cost review for energy efficiency Support and enhance sustainable AI framework Monitor developments in the sector to uncover technical opportunities for improving sustainability Engage strategic partners' engineering teams around green software practices	Regular efficiency reporting Regular code and system architecture Reviews considering efficiency All Engineering Fellows have awareness of green software engineering	Keep 2024 emission levels

Table 18. Key actions planned.

F-Secure transition plan does not necessitate material dedicated investments or funding beyond normal business operations. The implementation of the four primary decarbonization levers is executed within existing operational budgets and business processes.

Changes in product portfolio

Our main emission sources from production and technologies are in Scope 3 Category 1, including data centers and other purchased services. We're primarily using AWS for cloud computing and plan to continue this approach, as AWS offers near-zero-emission solutions.

We'll emphasize developing efficient, high-quality code to improve product performance, customer experience, and overall efficiency. The integration of AI and machine learning technologies will enhance product functionality and drive competitiveness. We'll partner with major AI providers who commit to reducing emissions, ensuring our overall emission profile remains unchanged despite increased energy use from AI models.

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. This topic is not considered material for F-Secure as the impacts are small due to actions already taken, and our implementation of green coding further reduces locked-in 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 cybersecurity 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

Resource Area	Requirements	Integration with Business Planning
Supply Chain Engagement	Dedicated supplier management resources	Procurement processes to integrate supplier emissions considerations
Energy Efficiency	Investments in office upgrades at controlled premises	Integrate energy consideration in office space leasing decisions
Green Coding	Developer training and performance optimization	Development of sustainable AI framework
Fuel switching	Achieve 100% e-/hybrid fleet	Policy to enforce change

Table 19. Transition plan alignment with strategy and financial planning.

ESG is integrated into our company strategy rather than being a separate initiative. Our transition plan actions will be implemented by appropriate functions with consideration to their annual budgets, with progress tracked by our Environment Committee and Sustainability Council. The transition plan will be further developed as part of the SBTi process. In 2026, it will be reviewed by the Audit Committee and approved by the Board of Directors.

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, we have adopted several policies that address climate-related impacts, risks and opportunities.

The Climate Change Policy is based on the values and principles defined in F-Secure's Code of Conduct and informed by stakeholder input from our materiality assessment. Our Supplier Code of Conduct explicitly requires suppliers to commit to working in an environmentally responsible and efficient manner and strive to minimize the environmental footprint of operations.

Policy	Key Contents	Scope	Responsibility	Link to IROs
Climate Change Policy	Targets across Scopes 1, 2, and 3 Alignment with Paris Agreement and IPCC 1.5°C pathways Process for identifying climate impacts, risks and opportunities Renewable energy deployment in offices and operation (excluding energy efficiency) Climate change mitigation and adaptation	All employees, operations and value chain across all relevant geographies	CEO with implementation by Sustainability Council and Environment Committee	Failure to meet climate change mitigation targets may negatively impact channel business
Supplier Code of Conduct	Sustainable usage of natural resources Increasing energy efficiency and renewable energy use Reducing environmental impact of global operations	Suppliers (only apply where included or referenced in agreement)	Procurement with monitoring by F-Secure	Failure to meet climate change mitigation targets may negatively impact channel business
Procurement policy	Establish clear standards for all procurement activities Ensuring vendor evaluation, compliance with listed F-Secure policies, counterparty screening procedure, Regulatory and Industry Compliance and promoting environmental, social, and governance responsibilities	Suppliers and employees	Approved by CEO with monitoring by Procurement function	Failure to meet climate change mitigation targets may negatively impact channel business

Table 20. Climate policies.

E1-3 Actions and resources

To achieve Climate change policy targets and mitigate emissions, we have implemented four decarbonization levers linked to our environmental IROs.

To further strengthen our transition plan, F-Secure has committed to set near-term, company-wide greenhouse gas emission reduction targets in line with climate science through the Science Based Targets initiative (SBTi). By joining the SBTi, F-Secure is taking a clear step toward aligning its climate strategy with what science says is necessary to limit global temperature rise to 1.5°C. This commitment reflects F-Secure's ambition to act responsibly and be a sustainable, long-term partner for customers, partners, and society.

Fuel switching

For the opportunity to set a policy for e-vehicles, several cars have already been replaced with hybrid or electric models, 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 leased cars are electric.

Renewable energy and energy efficiency

In 2025, F-Secure's headquarters in Helsinki moved to new office spaces. In the process, renewable energy was considered, and the electricity used in the new Helsinki office is 100% renewable. Our plan is to ensure all large offices, as well as smaller facilities where energy contracts can be controlled, use 100% renewable energy by 2030.

Supply chain decarbonization

Regarding the risk that F-Secure would fail to meet mitigation targets, as emission reduction is heavily reliant on suppliers, we have initiated actions to mitigate emissions in our value chain. In 2025, we set up our supplier climate mitigation program to reduce our emissions. The program focuses on supplier engagement and climate data gathering from suppliers. We've also implemented our Procurement policy, which requires suppliers to work in an environmentally responsible manner, continuously improve energy efficiency, and reduce waste and emissions. No quantitative emission reductions are available for these actions in 2025, but we expect a 52% emission intensity reduction by 2030.

Efficient coding principles

For the potential positive impact of implementing green coding principles, emissions for sold products are calculated based on the number of products sold annually. During 2025, actions towards this lever include developing and launching our company-wide framework for Sustainable AI use and training the organization on these principles. AI is a strategic priority at F-Secure, and we are moving fast. This framework provides the guardrails we need for rapid, responsible innovation. The framework clarifies what F-Secure does to ensure sustainable AI implementation and what we expect from our workforce. In addition, we organized a panel discussion on AI innovation and sustainability in software development with external experts joining. This panel discussion aimed to share knowledge about the scale of environmental impact of software and AI, learn strategies for green coding and sustainable AI in production, and understand how to make the business case for responsible development. While no quantitative emission reductions are expected in 2025 due to the low material impact. By 2030, we do not expect emission reductions as the number of sold products is projected to grow, while we optimize energy consumption.

For more specific information on progress towards climate targets, see Disclosure Requirement E1-4 – Targets related to climate change mitigation and adaptation. No significant monetary amounts of Capex and Opex have been required to implement these actions.

Resource Allocation

The management of impacts, risks and opportunities is conducted by the F-Secure Environment committee, including internal stakeholders for each decarbonization lever.

Metrics and targets

E1-4 Targets

F-Secure describes its sustainability-related baseline measures and targets in the table below. 2024 is established as a baseline year, and progress will be reported annually.

Methodologies and frameworks

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 with data collected 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.

Our 2025 energy-related emission factors were updated by an external consultant. Metrics were selected based on legislative requirements, material ESG topics, and stakeholder feedback. In 2025, we have updated our Scope 3 target from actual emission reduction to 52% reduction in emission intensity (GHG emissions (t CO_2eq) by net revenue (€)) of Scope 3. Targets have been approved by the Board of Directors.

In the event of significant structural changes such as acquisitions, divestments, mergers, or changes in calculation methodologies, F-Secure will evaluate whether baseline recalculation is necessary. Recalculation would be conducted if structural changes result in a material impact on the baseline emissions, following GHG Protocol guidance. Any baseline adjustments will be transparently disclosed, documenting the rationale, methodology, and quantitative impact of the recalculation to maintain comparability and integrity of target tracking over time. In 2025, baseline recalculation has not been conducted as there have not been significant changes. F-Secure has not adopted new technologies in 2025, which would significantly affect the emission reduction targets.

We track our actions' effectiveness using total GHG emissions (tons of CO_2eq), emissions intensity per revenue, and their impact. We disclose combined GHG emission reduction targets for Scope 1 and 2 emissions. Scope 2 emissions are calculated using both market-based and location-based methods, with market-based used for the 2030 target. Our targets align with GHG inventory boundaries and don't include GHG removals, carbon credits or avoided emissions.

E1-4 Climate targets & progress

	2024 base year	2025	Target values	2030 target
Gross Scope 1 & Scope 2 (market-based) (tCO2eq)	220	195	127	42% emission reduction
Scope 3 (tCO2-ekv./MEUR) emission intensity	57	57	27	52% emission intensity reduction

Table 21. 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. After 2030, the base year is set every five years. The 2024 baseline values are described in chapter E1-6.

Framework and methodology for target setting

F-Secure has established GHG emission reduction targets compatible with limiting global warming to 1.5°C by 2030. In 2030, Scope 1&2 emissions aim to be 127 tons of CO_2eq, and the Scope 3 target of 52% reduction in emission intensity (GHG emissions (t CO_2eq) by net revenue (€)). The GHG Protocol and IPCC's cross-sector pathway serve as our framework. Future technological advancements, regulatory changes, and market shifts have been considered in our target setting. 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. The targets are defined by the Sustainability Council and approved by the Board of Directors.

Decarbonization levers and their contributions to achieve reduction targets.

- **Fuel switching:** We plan to transition to hybrid and electric vehicles, with a projected 50/50 split by 2030. In 2025, the emissions of Scope 1 were 33 tCO_2eq. Emissions will be within the 42% decrease target by 2027.
- **Renewable energy and energy efficiency:** The Scope 2 emissions have decreased 14% during 2025, mostly due to removal of Poland office and the decrease of Helsinki office heating.
- **Supply chain decarbonization:** This lever includes Scope 3 category 1, which represented over 80 % of our Scope 3 emissions in 2025. Our purchased goods and services (excluding data center services) were 6610 tCO_2eq. Our cloud computing and data center services increased from 2024 due to an increase in the AWS services.
- **Efficient coding principles:** No material reduction expected as customer base growth will likely cancel out energy efficiency improvements. This covers Scope 3 category 11. We are still in the early stages of implementation, and assessing the effectiveness of the actions and policies cannot be quantified at this early stage.

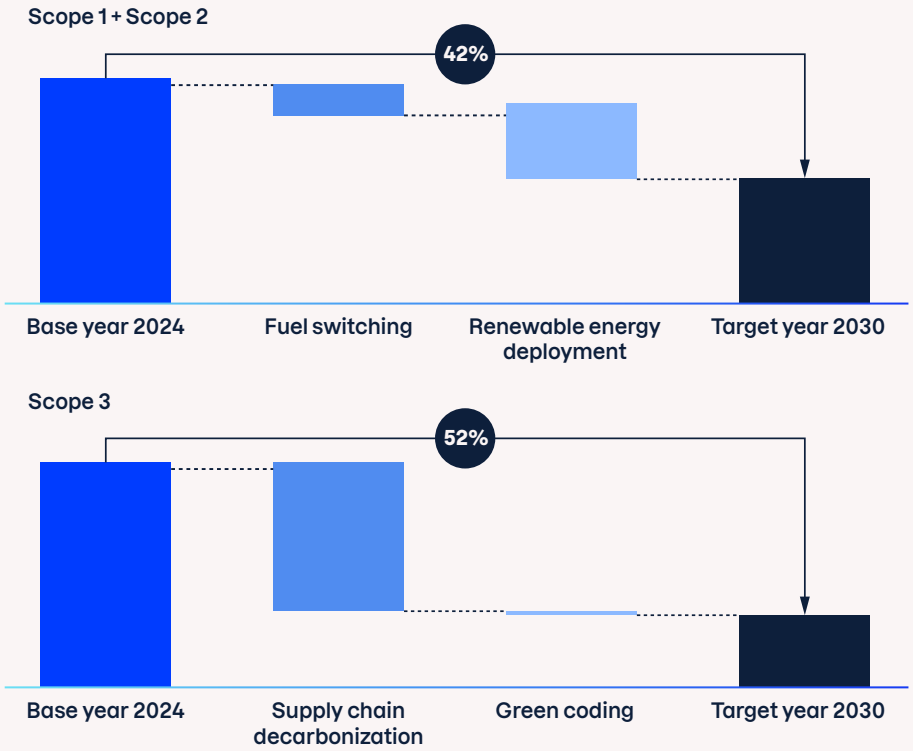


Figure 3. Graphical pathway waterfall shows the development of emissions in line with the Transition plan.

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

In our GHG emission calculations, we've considered the GHG Protocol Corporate Standard for principles, requirements and guidance. We use primary data where available (currently only from AWS, representing <1% of total Scope 3 emissions) and standardized emission factors for the remainder. Our emissions consolidation approach follows the operational control method.

	Retrospective				Milestones and target years			
	Base year 2024	Comparative	2025	% N / N-1	2025	2030	(2050)	Annual % target / Base year
Scope 1 GHG emissions								
Gross Scope 1 GHG emissions (tCO_2eq)	31	31	33	6%	-	18[1]	-	8.70%[2]
Percentage of Scope 1 GHG emissions from regulated emission trading schemes (%)	0%	0%	0%		-	-	-	-
Scope 2 GHG emissions								
Gross location-based Scope 2 GHG emissions (tCO_2eq)	233	233	198	-15%	-	-	-	-
Gross market-based Scope 2 GHG emissions (tCO_2eq)	189	189	162	-14%	-	110[1]	-	8.70%[2]
Scope 3 GHG emissions								
Total Gross indirect (Scope 3) GHG emissions (tCO_2eq)	8330	8330	8282	-1%	-	NA[3]	-	-
1. Purchased goods and services (excluding data center services)	6466	6466	6610	2%	-	-	-	-
Sub-category: Cloud computing and data center services	43	43	318	640%	-	-	-	-
3. Fuel and energy-related activities	49	49	43	-12%	-	-	-	-
5. Waste generated in operations	2	2	3	50%	-	-	-	-
6. Business travel	1675	1675	1211	-28%	-	-	-	-
7. Employee commuting	23	23	22	-4%	-	-	-	-
8. Upstream leased assets	11	11	15	36%	-	-	-	-
11. Use of sold products	61	61	61	0%	-	-	-	-
Total GHG emissions								
Total GHG emissions (location-based) (tCO_2eq)	8594	8594	8513	-1%	-	-	-	-
Total GHG emissions (market-based) (tCO_2eq)	8550	8550	8477	-1%	-	NA[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) An absolute value cannot be given because an accurate revenue estimate cannot be made.

Table 22. Gross scopes and total emissions.

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

Scope 1

F-Secure's Scope 1 emissions originate from fuel combustion in company vehicles. Emissions are calculated using fuel consumption data from leasing car systems and directly from individuals leasing the vehicles. Emission factors from Statistics Finland convert fuel data into GHG emissions in metric tons of CO2e. F-Secure's operations do not generate biogenic Scope 1 GHG emissions from biomass combustion or decomposition.

Scope 2

F-Secure uses both market-based and location-based methodologies. Data on purchased electricity is collected from five sites via country or site representatives. Emissions from heating and cooling are calculated using the office area and heating/cooling factors. Compared to the 2024 calculations, the Poland office no longer exists, and Helsinki offices moved to larger facilities within the same building. Emission factors are sourced from multiple authorities, including Energy Authority, Association of Issuing Bodies, Ember, Energiateollisuus, Statistics Finland, CO2Emissiefactoren, Defra, and Our World in Data.

Scope 3

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 23. Scope 3 categories.

Category 1: Purchased goods and services (excluding data center services) Values derived from financial reports representing expenditure on goods and services. Emissions from some vendors are calculated separately by comparing their emissions to revenue. These vendor expenses are excluded from financial report data to avoid double-counting. Emission factors from Lenovo and Exiobase.

Category 1 sub-category: Data center services 3-month delay in retrieving AWS figures. VPN energy usage is primarily from Ficolo (Finnish VPN server provider). Other VPN providers' electricity usage is extrapolated based on known traffic. Emission factors from AWS, EEA, Australian government, Carbon Footprint, Government of Canada, Ficolo, Climate Transparency, Singapore government, EPA and Vietnam government.

Category 3: Fuel and energy-related activities Calculated based on Scope 1 and Scope 2 values. Emission factors from GLEC, Defra and the UK Government.

Category 5: Waste generated in operations Waste amounts are estimated by extrapolating general waste amounts in a conventional office. Laptop and monitor data collected from Finnish offices and extrapolated to other offices. Emission factors from Fujitsu and the Environmental Protection Agency.

Category 6: Business travel Flight data from two travel agencies and from the company HR system. For HR system data emission calculators used for emissions or flight lengths. Emissions regarding business travel decreased around 30% from 2024. Emission factors from travel agencies, including Defra.

Category 7: Employee commuting Work travel distance, and type based on external data sources and estimations. Office workdays are calculated based on Helsinki and Oulu office data. Emission factors from Defra, Statistics Finland, GreenTech Malaysia and Carbon Footprint.

Category 8: Upstream leased assets Emissions from home offices and coworking spaces are assumed from electricity consumption of ICT equipment. Home offices and coworking spaces are not separated as they work similarly. Emission factors from Carbon Footprint.

Category 11: Use of sold products Assumed all sold products are taken into use. Emission factor from Statistics Finland.

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

Emission factors used are carbon dioxide equivalents, including greenhouse gases listed in the Kyoto Protocol (CH4, N2O, HFCs, PFCs, SF6, and NF3). Equivalents are calculated using a 100-year time horizon for CO_2eq emissions of non-CO_2 gases.

E1-6 GHG intensity based on net revenue

F-Secure calculates GHG intensity based on net revenue by dividing total GHG emissions (t CO_2eq) 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	2025
Total GHG emissions (location-based) per net revenue in millions (tCO_2eq/MEUR)	58.76	58.41
Total GHG emissions (market-based) per net revenue in millions (tCO_2eq/MEUR)	58.46	58.17
Net revenue used to calculate GHG intensity		
Total net revenue (in financial statements) MEUR	146.30	€ 146

Table 24. GHG intensity per net revenue.

GROUP SUSTAINABILITY REPORT -

Social

S1 – Own workforce

SBM-3 Material impacts, risks and opportunitites

	Material impact, risk or opportunity	Description
Working conditions		
Work-life balance		
Actual positive impact (OO)	Family leaves	Family leaves for F-Secure employees exceeding local requirements in some countries.
Health and safety		
Risk (OO)	Workload and mental wellbeing	Mental health related absences detected.
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 mitigating the gender pay gap.
Training and skills development		
Opportunity (OO)	Use of AI in workforce development	Process improvements, competency maturity and AI sentiment
Actual positive impact (OO)	Learning and development	Further ramp up strategic learning and development activities and track investment into learning activities.
Potential positive impact (OO)	Critical strategic competences	Continuously identify the internal competencies critical to our strategy.
Risk (OO)	Talent acquisition and retention	Loss of key persons or inability to acquire new talent
Measures against violence and harassment in the workplace		
Actual positive impact (OO)	Inclusive culture with a speak up-culture	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 need to ensure that F-Secure meet expectations.

Table 25. Own workforce IROs.

F-Secure has identified key impacts, risks, and opportunities (IROs) related to working conditions, equal treatment, and career development. The company aims to support an inclusive culture, promote equality, and encourage a healthy work–life balance in order to provide conditions that enable employees to perform effectively.

No material negative impacts have been identified related to our workforce, whether widespread, systemic, or linked to individual incidents.

F-Secure material impacts, risks, and opportunities are related to all people in its workforce.

Interaction with strategy and business model

F-Secure's actual and potential workforce impacts—covering working conditions, equal treatment, well-being, and career development—originate directly from its strategy and people-driven business model. Through ESG materiality assessments and HR processes, these impacts, risks, and opportunities are systematically identified and evaluated.

Positive impacts, such as inclusive practices, skill development, and work–life balance initiatives, strengthen the company's ability to attract and retain talent and therefore support strategic execution. Similarly, risks such as burnout or turnover inform workforce planning and guide improvements to employment practices. The insights gained from these assessments contribute to adapting the strategy and business model, ensuring alignment between workforce impacts and long-term business performance.

Disclosure scope

All employees who can be materially impacted by F-Secure are included in this disclosure scope, encompassing impacts connected with their own operations.

Types of employees

F-Secure measures full-time employees by FTEs (full-time equivalent) with no "non-guaranteed hours" employees. Employee categories include:

- **Permanent employees:** Employed with no predefined contract end date
- **Fixed-term employees:** Hired for a specific duration with defined end dates
- **Contractors:** All non-employees, including Employee-like (integral team participants), Consultants (project-based supplementary workforce), and Other (facility access without system access)

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

Employee-like (also called "Fellowlike"):

- An integral part of the F-Secure teams, participating in daily activities and team meetings. Usually, contracts are fixed and time-based. Regardless of the contractor status, our contract with any non-employee 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-employee 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.

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, maintaining transparency and alignment with F-Secure's sustainability objectives.

In developing workforce-related policies, F-Secure considers the interests and needs of employees through continuous feedback mechanisms such as employee surveys, development discussions, consultation with employee representatives, and insights gathered through internal materiality assessments. These inputs help ensure that policies address the most relevant impacts, risks, and opportunities identified by the workforce. All workforce-related policies are made available to employees through the company intranet. Policy updates are communicated through internal channels, and managers are responsible for ensuring employees are aware of policy requirements. Mandatory training modules (e.g., Code of Conduct) ensure that key policies are understood and implemented across the organization.

Additional details on F-Secure's Code of Conduct are provided in *ESRS G1-1*.

F-Secure supplier code of conduct includes provisions addressing the safety of workers, precarious work, human trafficking, the use of forced labour or child labour, and is fully in line with applicable ILO standards.

Policy	Key Contents	Scope	Responsibility	Link to IROs
DEI Policy	Promotes diversity, equity, and inclusion aligned with values and Code of Conduct Anti-harassment and non-discrimination guidelines Targets for talent acquisition and accountability mechanisms Training, targeted recruitment, programs supporting vulnerable groups and leadership development DEI Committee	All employees, employee-like contractors, leadership.	CPO (Chief People Officer)	Employer reputation Promoting gender equality Inclusive culture with a speak up-culture
Recruitment Policy	Fair and transparent hiring processes Adherence to local requirements and non-discrimination laws Background checks and compliance factors Recruitment process, employer branding, metrics, legal considerations Aligned with ILO principles on non-discrimination and equal opportunity Addresses training and skills development aligned with DEI goals	All employees, leadership and employee-like contractors	CPO	Promoting gender equality Learning and development Critical strategic competences Talent acquisition and retention

Policy	Key Contents	Scope	Responsibility	Link to IROs
Health and Well-being Policy	Principles and practices for employee health and well-being Healthy work culture, leadership role, local health compliance Health activities, continuous learning, flexible work environments Monitoring success of activities Adherence to local legislation and regulatory standards Addresses work-life balance, health and safety (ILO standards)	All employees and leadership	CPO	Family leaves Workload and mental wellbeing Talent acquisition and retention Inclusive culture with a speak up-culture
Learning and Development Policy	Continuous learning to enhance workforce expertise Foster collaboration and structured learning frameworks Training definition, roles and responsibilities Learning framework, data management and reporting Measuring effectiveness of learning efforts Addresses training and skills development	All employees and leadership	CPO	Use of AI in workforce development Critical strategic competences Talent acquisition and retention
Rewards and Recognition Policy	Fair and transparent rewarding principles and practices Job architecture, base salary, benefits, incentive plans Recognition and pensions Rewards framework consistent with global standards Aligned with OECD and ILO principles Addresses fair and equal treatment and transparent working conditions	All employees and leadership	CPO	Promoting gender equality Critical strategic competences Talent acquisition and retention

Table 26. Own workforce policies.

Human Rights Policy Commitments

F-Secure's workforce policies align with international standards, including OECD Guidelines for Multinational Enterprises, UN Global Compact, UN Guiding Principles on Business and Human Rights, ILO Declaration on Fundamental Principles and Rights at Work, and the International Bill of Human Rights. These principles are embedded throughout our policies as detailed below. Human rights are incorporated in our Code of Conduct, with which all F-Secure employees must comply.

Our commitment focuses on three core areas:

- **Respect for Human Rights** - Uphold global standards, respect freedom of opinion, expression, conscience, and religion; act swiftly on adverse impacts; protect digital lives by combating scams.
- **Labor Rights & Safety** - Ensure compliance with laws, safe working conditions, freedom of association, and zero tolerance for child labor, forced labor, or trafficking.
- **Application of Standards -** 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 for compliance. F-Secure suppliers and partners are also expected to act responsibly and comply with principles set in the Code of Conduct and local laws.

Furthermore, F-Secure does not operate in industries/sectors where the risk of forced, compulsory, or child labour 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 during the hiring process as part of our Recruitment Policy, which reduces the risk.

Engagement with our workforce

F-Secure has established systematic workforce engagement methods, including regular Townhalls, personnel surveys, and workers' representative consultations. Detailed engagement processes are described in section *S1-2 Processes for engagement about impacts.*

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

F-Secure provides multiple channels for employees to raise human rights concerns, including direct contact with managers, HR, Legal, or via the Whistleblowing channel. All concerns are handled confidentially. For detailed information on reporting channels and remediation processes, see section *S1-3 Processes to remediate negative impacts and channels to raise concerns.*

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 HR systems, where all incidents are reported and monitored for compliance with local laws and regulations. While physical injuries are rare in the software and cybersecurity industry, any workplace accident or harm is recorded and managed according to country-specific practices. Our intranet provides employees with detailed workplace safety information. We define occupational accidents as unexpected events resulting in injury, including incidents within the workplace, during business trips, or while carrying out employer-ordered errands. We address injuries such as muscle or tendon pain, which may be compensable under certain conditions.

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

S1-2 Processes for engagement about impacts

F-Secure actively incorporates the perspectives of its employees into the management of workforce-related impacts, risks, and opportunities. Senior leadership—comprising the CEO, Chief People Officer, and Leadership Team —leads employee engagement through regular Townhalls and monthly Leadership Forums.

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

1. **Employee Engagement**: Monthly Townhalls with Q&A, function-specific all-hands meetings, Leadership Lab for Team Leaders, and digital suggestion channel promote inclusive participation.
2. **Employee Feedback**: Biannual anonymous personnel surveys are conducted to gather feedback from all employees. The results are analyzed and presented at company, function, and team levels (where at least five responses are available). Other feedback mechanisms such as the whistleblowing channel, exit interviews and HR consultations.
3. **Project-Based Engagement**: Employees participate in specific processes or projects, such as people processes or cultural initiatives.
4. **Workers' representatives**: People and Culture Operations Director organize monthly meetings with Shop Steward to address current topics. HR Board meets monthly with Shop Steward and country-specific elected representatives (People & Culture Advisor)
5. **Collective Bargaining Compliance**: F-Secure adheres to collective bargaining agreements in Finland, France, and Spain, maintaining alignment of policies and practices through the People & Culture Operations Director.

Accessibility and Inclusivity

In addition to the engagement methods described above, F-Secure places strong emphasis on accessibility and inclusivity as essential components of workforce engagement. The company ensures equal participation by offering accessible Learning Management Systems and survey tools with screen reader compatibility, text-to-speech features, and closed captioning. Virtual Townhalls include real-time captions and recorded transcripts in audio and text formats. Wheelchair-accessible facilities and clear, easy-to-understand language across all communications enable employees with mobility or cognitive disabilities to engage fully. These measures reflect F-Secure's commitment to ensuring that every employee can contribute and participate without barriers.

Insights from these channels are used to identify and reassess material workforce IROs, including topics such as well-being, workload, equal treatment, skills development, and workplace culture. Employee feedback directly informs decisions related to improvement actions, for example, updates to hybrid work practices, development of well-being initiatives, targeted training programs, and adjustments to career development frameworks.

This process ensures that employee needs and expectations are considered when designing and implementing measures to manage both actual and potential impacts on the workforce.

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

F-Secure strongly encourages employees to speak up regarding concerns related to their employment or daily work. We aim to avoid adverse human rights impacts and take actions to remediate them when they occur. Every employee at F-Secure has the right and obligation to raise concerns about Code of Conduct violations, including human rights.

Our organization assesses potential negative impacts through structured processes. We assess the effectiveness of the remedy provided through follow-up reviews with the affected individuals, monitoring for recurrence of the issue, and evaluating whether the corrective actions have addressed the root cause. Feedback from employees, case-closure criteria, and ongoing monitoring help us confirm that the remedy has achieved its intended outcome.

Primary Reporting Channels

Concerns should primarily be reported through:

- Team leader, local People & Culture advisor, legal or personnel surveys
- Verbal or electronic communication methods
- Team leader's leader or People & Culture if issues relate to the direct team leader
- Shop Steward or employee representatives
- Direct contact with the CEO or Board of Directors

The Whistleblowing Channel serves as a way for anonymous reporting (see G1-1 for details). All concerns are handled confidentially, reviewed thoroughly, and addressed through appropriate measures for any Code of Conduct violations, including human rights. Retaliation against anyone raising a good-faith concern is strictly prohibited. We actively communicate and train team leaders and employees on the available reporting channels, which are regularly updated on our intranet.

Our whistleblowing channel is operated through a third-party provider to ensure independence, confidentiality, and anonymity. The channel is made available and maintained by F-Secure, but the reporting mechanism itself is administered externally.

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

Assessment and Continuous Improvement

We assess awareness and trust in our structures and processes through:

- Regular employee surveys (biannual personnel surveys)
- Feedback mechanisms (1-on-1 meetings with team leaders and Townhalls)
- Trust metrics tracking, such as eNPS (employee Net Promoter Score)

These surveys and feedback channels gauge employees' understanding of internal processes and confidence in the company's commitment to transparency, ethics, and fairness. Results are used to identify areas for improvement and drive continuous enhancement of our practices. All reporting channels are easily accessible to employees across all levels of the organization.

S1-4 Actions and resources

Scope: All employees globally; targeted initiatives for underrepresented groups.
Time Horizon: Ongoing; programs launched and maintained in 2025.

Actions to address material impacts

F-Secure actively implements measures to enhance positive impacts on its workforce while managing related risks and opportunities identified in the materiality assessment. The company's initiatives focus on maintaining a stable,

equitable, and inclusive working environment, as outlined below. No actual or potential negative impacts related to F-Secure's own workforce have been identified that exceed the threshold defined in the impact, risk, and opportunity assessment conducted as part of the DMA.

Family leaves

F-Secure is committed to creating an inclusive and supportive work environment where employees can balance personal and professional responsibilities. We ensure equal access to parental and caregiving leave so that no one is disadvantaged for prioritizing family. Our Wellbeing Strategy focuses on strengthening physical, mental, and emotional health through proactive programs and initiatives. Comprehensive support is provided across Finland, India, the US, and Malaysia, addressing risks such as stress and burnout while promoting long-term health and satisfaction. In addition, the Culture, Health & Well-being Committee ensures compliance with both global and local health and safety standards, embedding well-being into our culture and everyday practices.

Learning and Development

Targeted training for R&D and leadership roles supports upskilling, addresses skill shortages, and promotes career growth. F-Secure enhances workforce competencies through capability and competence analysis, employee surveys, and centralized training via the Learning Management System (LMS).

Gender Equality

A diverse workforce is a strategically important topic for F-Secure, and due to this, we have implemented targeted recruitment for underrepresented groups.

Culture Building

We take action to foster a speak-up culture via training and feedback mechanisms, which we have continued to develop in 2025. We have linked our monthly superheroes to our cultural values, and they are presented at our Townhalls. This creates a clear link between the desired behavior of a Fellow and the culture we want to develop.

Secure Employment and Flexible Workplace

F-Secure offers stability by prioritizing permanent contracts over fixed-term agreements, minimizing uncertainty for employees. Remote/ Hybrid work allows employees to work from home several days a week, promoting work-life balance and improving well-being. In regions like India and Malaysia, where commuting can be time-consuming, remote/hybrid work enhances employee satisfaction and productivity. Progress: Engagement with DEI rate.

Fair Working Environment

We continuously evaluate and update policies and procedures across all locations for full compliance with local, regional, and national regulations. This maintains a fair and transparent work environment, fostering trust and inclusivity. Comprehensive benefits suite includes health insurance and vacation/leaves, offering mental health and personal well-being resources.

Prevention of Negative Impacts on Workforce

F-Secure has assessed its practices and confirms that it does not cause or contribute to material negative impacts on its own workforce. Our employment practices are governed by global HR policies, the Code of Conduct, and data protection standards, which ensure fair, safe, and responsible working conditions.

To ensure we do not cause or contribute to negative impacts, we monitor workforce well-being, engagement, development, and workplace conditions through surveys, absence trend analysis, performance processes, and established grievance and whistleblowing channels. No tensions were identified between preventing negative impacts and other business pressures during the reporting period.

We expect to continue monitoring and assessing key workforce areas—including employee well-being, engagement, development, and the effectiveness of HR processes—throughout the strategy period (2026–2028). These activities did not require any material operating (Opex) or capital expenditures (Capex) in 2025, and we expect this to remain unchanged during the strategy period.

Tracking Effectiveness

Systematic Tracking Methods:

- **Employee Surveys**: Anonymous engagement surveys, including eNPS, to monitor workforce satisfaction
- **Policy Reviews**: Regular evaluations for compliance with labor laws and international standards
- **Gender Equality Monitoring**: Pay gap analyses conducted before and after salary reviews
- **Culture Assessment**: Biannual surveys measuring eNPS, retention rates, and leadership effectiveness
- **Sustainability Council reviews**: Updates on Own workforce related topics through DEI and Wellbeing Committee.

Actions related to material opportunities

Actions related to our material opportunities were executed during 2025. We continue to see them as relevant also for the current strategy period (2026-2028):

Opportunity	Actions 2025	Effectiveness Measures and expected outcomes
Employer Reputation	DEI development projects DEI talks platform Mothers in business Program Women in Tech Initiatives	Strengthened talent, attraction, and retention. Employer brand engagement metrics
Use of AI	Implement AI tools to enhance employee experience and processes	Improved efficiency & consistent solutions across the organization

Table 28. Actions to pursue own workforce opportunities.

Actions to mitigate material risks

We have identified two risks with corresponding mitigation strategies as listed in the table below. These mitigation activities were executed in 2025 in our own workforce, and we see them as relevant during the strategy period (2026-2028):

Risk	Actions 2025	Effectiveness Measures and expected outcomes
Employee Workload and Well-being	Provide well-being programs, support resources, and regular check-ins. Monitor health trends and ensure adequate healthcare coverage. Occupational Health Care (Finland). Comprehensive health coverage (India, US, France and Malaysia)	Engagement and Fellow survey feedback Well-being initiative participation rates Absence and Mental health-related tracking Ensure wellbeing in workforce
Talent Acquisition and Retention	Recruitment aligned with strategic workforce planning and strengthened pre/onboarding & development Programs Support career growth and leadership development through centralized learning Management system.	Time-to-hire metrics Total attrition and HiPo retention rates Engagement, training & Performance review completion rates. Talent density % & Succession pipeline % Build a future-ready workforce by attracting the right talent, accelerating development, and improving retention through strategic hiring, effective onboarding, and continuous learning

Table 27. Actions to mitigate own workforce risks.

Resource Allocation:

- **People and Culture function:**

Manages all material impacts, risks, and opportunities related to our workforce, covering all employees globally. This includes oversight of the full employee experience, from recruitment and onboarding to talent development, performance management, diversity and inclusion, well-being initiatives, payroll and rewards, HR systems, and support for all regional offices. In addition, well-being and DEI activities are coordinated through cross-functional committees that represent employees across the organization.

Metrics and targets

S1-5 Targets

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

Methodologies and frameworks

Methodologies for collecting and tracking targets are based on F-Secure's HR systems as described under each target. Metrics have been selected based on alignment with material F-Secure ESG topics, ESG regulation, DMA, and stakeholder feedback. Targets have been approved by the Board of Directors.

S1-5 Own workforce targets

Target	Baseline 2023	2024	2025	2030 target
Gender Diversity (directors including leadership team, %)	F: 23 M: 77	F: 23,5% ; M: 76,5 %[1]	F: 25.81%; M: 74.19%	F: 33 M: 67
Gender Diversity (all employees)	*Third gender not implemented, F: 30% M: 70%*	M- 69.19%; F- 30.62%	F: 30,29%; M: 69,71%; ND:0,18%	No gender should represent more than 65% of workers.
Nationality among senior management	24	28	28	> 20
Age target (all employees, age groups 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%	Under 30: 20,77%, under 40: 36,98%, under 50: 29,14%, under 60: 11,66%, above: 60 1,46%	No age group should represent more than 35% of the total
eNPS evolution	2	40	33	> 50
Performance and career review target	*Baseline year is 2024*	88%[2]	98.91%	98%

1) The percentage for Gender Diversity directors including leadership team, % target has been corrected for 2024 reported numbers (F: 25.1% ; M: 74.9%).

2) The percentage for Performance and career review target has been corrected for 2024 reported numbers (82.04%).

Table 29. Own workforce targets.

S1-5 Progress towards targets

Diversity (DEI) related targets

These targets help make intentional hiring and promotion decisions based on skills and competencies in alignment with our values, driving inclusion and equality. Targets are set by the F-Secure Chief People Officer and apply globally. We review progress regularly and build remediation plans when negative trends or issues are identified.

1. Gender Diversity - Directorss: We have set a 2030 gender target that 33% of senior leaders at the director level should be female. This target applies globally to all F-Secure employees, excluding contractors and employee-like consultants. The baseline year is 2023 with 23% female representation. Our 2025 outcome is 25.81% female and M: 74.19%% male representation among senior leaders.

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

2. Gender Diversity - All Employees: This target reinforces F-Secure's commitment to gender inclusivity beyond binary categories, maintaining fair representation of all genders. We have set a target that no gender (including third gender) should represent more than 65% of the workforce by 2030. The baseline year is 2023 with 70% male representation. Our 2025 outcome is 69,71% male representation.

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

3. Nationality Among Senior Management: Maintaining nationality diversity provides global representation in decision-making and fosters inclusive environment where leadership reflects our diverse workforce. F-Secure maintains or exceeds 20 nationalities within senior leadership positions. Our baseline year is 2023 with 24 nationalities represented. Our 2025 outcome is 28 nationalities.

4. Age Target: Age diversity fosters a vibrant workforce with wide-ranging experiences. By preventing single age group dominance, we create space for intergenerational learning, innovation, and mentorship. We have set a 2030 target that no single age group represents more than 35% of total workforce. Our baseline year is 2023 where the largest age group represented 35.7% of workforce (30-40y). Our 2025 outcome shows one age group exceeding 35%, specifically the 30-40y group at 36,98%.

Employee well-being and satisfaction (eNPS)

The eNPS target relates to our health and well-being policy. Employee NPS score directly reflects company culture health, leadership effectiveness, and employee well-being. Higher eNPS indicates more engaged and satisfied workforce, aligned with cultivating healthy and inclusive work environment.

We have set a target to reach an eNPS above 50 in 2030, excluding contractors. This absolute target is measured on a scale from -100 to +100. Our baseline year is 2023 with an eNPS score of 2. Our 2025 outcome is 33.

eNPS is measured through regular anonymous employee surveys using the same survey tool globally. The eNPS target is defined by F-Secure's CPO, and when part of remuneration plans like a non-sales STI plan, also with the CEO.

Performance review

This target supports the company's Performance Dialogue policies and process, maintaining that employees actively set and follow up on development goals. It fosters continuous professional growth by aligning individual aspirations with organizational vision and strategy.

Our target is to achieve 98% completion rate of performance and career target setting for all employees by 2030. This applies to all company employees globally, excluding employee-like contractors unless specified otherwise. 2024 is the first year to capture data, serving as baseline year. Our 2025 outcome is 98.91%.

Target setting process and engagement with the workforce

Overall company-level targets for short term (fiscal year) and 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, Sustainability Council and the CEO for part of incentive schemes.

Employee input into target setting is considered based on surveys conducted during the year or experts participating in target setting within respective functions. Progress is shared with workforce through monthly Townhalls and internal communications, where feedback is gathered to improve actions or policies aimed at achieving targets.

Employee engagement (eNPS) is measured through regular anonymous employee surveys using a standardized global tool. Corrective actions are identified based on survey results at the company, function, and individual team levels.

Individual performance and development goals are jointly defined by line managers and employees at year start, aligned with company and function plans. Progress is tracked through regular 1:1 meetings and team discussions. Mid-year reviews assess organizational progress, and end-of-year reviews reflect on goal achievement, alignment with company values, and future development plans 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 serves as the single source of truth for all workforce data, maintaining accuracy and consistency across all reporting metrics.

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 with regular validation steps, including cross-checks by HR teams to confirm data accuracy
- **Data Reporting**: Metrics are directly derived from the HR system and extracted through consolidated reporting tools to reduce errors and maintain reliability

The reporting period is annual, and workforce data is captured through the HR system, providing real-time data on headcount. Data reflects status at the end of the reporting period.

Cross-reference with financial statements

The measures provided in the group sustainability report 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	Number of employees, 2025
Male	366	382
Female	162	166
Non-Binary	0	
Not reported	1	1
Total Employees	529	549

Table 30. Employee gender.

S1-6 Employee per country

Country	Number of employees, 2024	Number of employees, 2025
Finland	270	266
India	70	105
Malaysia	74	76
Total	**414**	**447**

Table 31. Employee per country.

S1-6 Employee turnover

Employee turnover is calculated as 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, 2025.

Employee turnover in the reporting period, by number of employees	2024	2025
Total number	107	103
Rate, %	20.23%	18.76%

Table 32. Employee turnover.

S1-6 Employee per contract

2024

Employee per contract type, head count	Female	Male	Other[1]	Not disclosed	Total
Number of employees	162	366	0	1	529
Number of permanent employees	160	364	0	1	525
Number of temporary employees	2	2	0	0	4
Number of non-guaranteed hours employees	0	0	0	0	0
Number of full-time employees	153	359	0	1	513
Number of part-time employees	9	7	0	0	16

1) Gender as specified by the employee themselves.

Table 33. Employee per contract 2024.

2025

Employee per contract type, head count	Female	Male	Other[1]	Not disclosed	Total
Number of employees	166	382	0	1	549
Number of permanent employees	164	378	0	1	543
Number of temporary employees	2	4	0	0	6
Number of non-guaranteed hours employees	0	0	0	0	0
Number of full-time employees	159	373	0	1	533
Number of part-time employees	7	9	0	0	16

1) Gender as specified by the employee themselves.

Table 34. Employee per contract 2025.

S1-6 Employee per region

2024

Employee per region, head count	Europe	North America	Asia[1]	Total
Number of employees	347	33	149	529
Number of permanent employees	343	33	149	525
Number of temporary employees	4	0	0	4
Number of non-guaranteed hours employees	0	0	0	0
Number of full-time employees	331	33	149	513
Number of part-time employees	16	0	0	16

1) Gender as specified by the employee themselves.

Table 35. Employee per region 2024.

2025

Employee per region, head count	Europe	North America	Asia[1]	Total
Number of employees	332	30	187	549
Number of permanent employees	328	30	185	543
Number of temporary employees	4	0	2	6
Number of non-guaranteed hours employees	0	0	0	0
Number of full-time employees	316	30	187	533
Number of part-time employees	16	0	0	16

1) Gender as specified by the employee themselves.

Table 36. Employee per region 2025.

S1-9 Diversity metrics

Methodology

Age Distribution by Job Grade: Employees under 30, 30–50, and over 50 years.

Gender Distribution by Job Grade and Compensation Grade: Gender representation across all F-Secure's job grades, and 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.

Data includes employees only and excludes contractors.

Our HR system allows employees to self-identify their gender as female, male, other, or not declared, ensuring inclusivity and respect for all gender identities. The term "other" refers to individuals whose gender identity does not fall strictly within the categories of male or female.

S1-9 Gender distribution

Gender distribution of top management, 2024	Female	Male	Other
Total number	12	39	0
Percentage, %	23.5%	76.5%	0
Gender distribution of top management, 2025	**Female**	**Male**	**Other**
Total number	16	46	0
Percentage, %	25.81%	74.19%	0

Table 37. Gender distribution.

S1-9 Age distribution

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%
Distribution of employees by age group, 2025	**Under 30 years old**	**30 - 50**	**Over 50**
Total number	114	363	72
Percentage, %	20.77%	66.12%	13.11%

Table 38. Age distribution.

S1-13 Training and skills development metrics

Methodology

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: mid-year and end-of-year reviews assessing goal achievement and overall performance.

S1-13 Training

2024	Female	Male	Other	Total
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	1.68	1,70		1.7
Average number of training hours per employee (h)				1.84

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

Table 39. Training and skills development metrics 2024.

2025	Female	Male	Other	Total
Percentage of employees that participated in regular performance and career development reviews (%)	98.78%	98.95%	100%	98.91%[1]
Number of performance reviews per employee	2.79	2.70	3.00	2.72
Average number of training hours per employee (h)				1.48

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

Table 40. Training and skills development metrics 2025.

Performance and career development review percentage is calculated based on all employees as of December 31, 2025, counting each employee once regardless of whether they had 1 or 2 reviews during the year, excluding employees terminated during 2025.

S1-14 Health and safety metrics

During autumn 2024, we introduced a dedicated form within our HR system to systematically track work-related accidents and resulting absences. This initiative enhances monitoring of workplace incidents with a proactive approach to employee health and safety. For 2024, employees were requested to retrospectively record any accidents that occurred earlier in the year. Beginning in 2025, all accident reports are expected to be submitted promptly following incident occurrence.

In Finland, where we have a large portion of employees, all health-related data is managed by our occupational health care provider, providing valuable insights into workforce health and safety and guiding preventive measures and policies.

S1-14 Health and safety

	2024	2025
Percentage of people in its own workforce who are covered by the undertaking's health and safety management system based on legal requirements and/or recognized standards or guidelines,%	100%	100%
Number of fatalities as a result of work-related injuries and work-related ill health	0	0
Number and share of recordable work-related accidents	0	0

Table 41. Health and safety metrics.

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

S1-15 Work-life balance metric

All employees are entitled to take family leave as outlined by applicable laws of the countries, company policies, and collective agreements where relevant. F-Secure supports work-life balance culture, maintaining that employees can access and utilize family leave without barriers. F-Secure actively monitors these metrics to ensure equitable access to family 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.

S1-15 Work-life balance

Data point	2024	2025
Percentage of employees entitled to family leave	100%	100%
Percentage of employed personnel who took family leave, broken down by gender	Male: 3.2% Female: 2.6% Total: 5.86%	Female: 3.46%; Male: 4.55%; Total: 8.01%

Table 42. Work-life balance metrics.

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).The CEO is excluded from pay gap calculation.

S1-16 Remuneration

Remuneration	2024	2025
Gender pay gap, %	12.74%	8.15%
The annual total remuneration ratio of the highest paid individual to the median annual total remuneration for all employees	5.11	7.17

Table 43. Remuneration metrics.

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

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**, accessible 24/7 to all employees and stakeholders. This platform supports transparent and ethical business conduct by enabling the safe reporting of concerns related to discrimination, harassment, or unfair treatment. All reports are handled in accordance with F-Secure's governance framework, privacy standards, and applicable local legislation, reinforcing our dedication to integrity, accountability, and respect for human rights.

S1-17 Incidents

	2024	2025
Harassment & discrimination		
Total number of incidents of discrimination, including harassment, reported in the reporting period	0	0
Number of complaints made through channels available to the company's own employees (including grievance mechanisms)	0	0
Total amount of material fines, penalties, and compensation for damages as a result of the incidents and complaints disclosed above	0	0
Severe human rights incidents		
Number of severe human rights incidents connected to the undertaking's workforce in the reporting period	0	0
Total amount of fines, penalties and compensation for damages for the incidents described above	0	0

Table 44. Incidents, complaints and severe human rights impacts.

S4 – Consumers and end-users

SBM-3 Material impacts, risks and opportunities

F-Secure confirms that all consumers impacted by F-Secure are in the scope of S4 disclosure. "Consumers" and "end-users" are used as synonyms unless stated otherwise.

	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 monitoring tools observe user behavior, detect anomalies, and react accordingly
Opportunity (OO)	Evolving threat landscape	Scams have become commonplace. Opportunities 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 (DVC)	Channel strategy	Significant agreement changes or loss of a major Service Provider account, or Direct Business decline
Actual positive impact (OO)	Protecting digital moments	According to our product questionnaire, consumers are worried about their online protection. F-Secure provides solutions to these threats through its offering.
Risk (DVC/UVC, OO)	Security of vendors and partners	Security vulnerabilities from suppliers and partners, relying on external vendors, especially vendors who are one step removed in the supply chain, adds layers of vulnerability.
Risk (OO)	AI increases risk of security breach	Effective AI experimentation and roll-out dependent on high quality data sources and may also increases risk of a security breach.
Risk (OO)	Cyber security	Cyber security attacks negatively impact reputation and business
Information-related impacts for consumers and/or end-users		
Access to (quality) information (Awareness and education)		
Actual positive impact (DVC, OO)	Create awareness about cybercrimes	Increase consumers awareness about cybersecurity and cybercrime through marketing campaigns and events.

Table 45. Consumers and end-users list of IROs.

Interaction with strategy and business model

F-Secure has identified an actual positive impact in protecting consumers' digital moments, which continues to guide company strategy, decision-making and execution during 2025 and for the next strategy period (2026-2028):

1. **Product and Technology Investments:** Provide relevant, engaging and effective protection against modern threats through innovation, threat research, and consumer needs analysis. Our portfolio and protection roadmaps focus on scam protection and leveraging AI capabilities for both effective protection and engaging user experience.
2. **Growth Opportunities:** The evolving threat landscape, including the rise of scams and cybercriminals using AI, presents significant growth opportunities for F-Secure and our Service Provider partners. We leverage AI as an opportunity to innovate new protection capabilities, improve customer experience, and increase internal efficiencies.
3. **Channel Sales Model**: Develop our channel sales capabilities further and continue to build a portfolio that is "fit to channel" to reach large customer bases through our partners. Increase cyber threat awareness both directly and through our 200 channel partners by offering free tools and providing educational content

We recognize risks in our channel strategy, including changes in agreement scope, potential loss of significant Service Provider partners, and requirements especially when working with Tier 1 Service Providers. These risks could impact revenue, increase costs, or hinder operations. However, investing in capabilities for our Tier 1 business enhances resilience across all partner segments.

Additionally, F-Secure acknowledges the risk of cybersecurity attacks that may negatively impact our reputation and business, as well as security risks from suppliers and partners. We handle personally identifiable information securely, never sell it to third parties, and provide regular workforce training on PII handling as part of our Code of Conduct.

Types of consumers negatively impacted by F-Secure

F-Secure provides software-based products and services designed for all consumer types and age groups. Our cybersecurity software-based products are not inherently harmful to people and do not increase risks for chronic disease. We have not identified any material negative impact related to consumers and end-users, or any consumer subsegments.

No products or services exist that may potentially negatively impact consumer rights to privacy, personal data protection, freedom of expression, and non-discrimination. F-Secure's cybersecurity offering is built to protect consumers and their rights online, including privacy and identity protection capabilities. We collect information only for the purpose of providing the security service and do not sell any such information to third parties.

We have built our products to guide onboarding and usage to minimize the need for manuals, while offering support via community articles and support channels. Our software-based products are promoted and sold through F-Secure or reputable Service Providers and are not targeted at children or financially vulnerable individuals.

Types of consumers positively impacted by F-Secure

F-Secure's purpose is to protect consumers' digital moments, and for that purpose, we have created a design system to make 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. Compliance with accessibility practices allows creation of an inclusive product experience for individuals with disabilities and the elderly while serving the general population.

Additionally, we increase global cybersecurity awareness to combat cybercrime by educating consumers how to stay safe online. Our global campaigns target diverse regions and involve collaboration with educational institutions, government bodies, NGOs, and customers, emphasizing shared responsibility for cybersecurity. This aligns with our goals of mitigating cyber threats and promoting a secure digital environment through educational content and free tools for online safety.

Impact, risk and opportunity management

S4-1 Policies

Policy	Key Contents	Scope	Responsibility	Link to IROs
Personal Data Policy	Controls and principles for protecting customer privacy Privacy organization and roles Key privacy principles and processes Privacy training and monitoring Based on EU GDPR and relevant privacy regulations	All employees, leadership, employee-like contractors and suppliers	CEO and leadership team	Evolving threat landscape Cybersecurity Protecting digital moments
Cyber Security Policy	Objectives for strategic cybersecurity activities Governance practices and focus areas Information security, privacy, and software security management Based on ISO 27001 standard Protection of customer and employee data Maintaining availability of company services	All employees and leadership, employee-like contractors, and suppliers.	CEO (accountable), Chief Information Security Officer (implementation)	Protecting digital moments Security of vendors and partners
AI Policy	Encourages innovation with AI applications Adherence to high standards in privacy, cybersecurity, intellectual property rights, and business integrity Based on Code of Conduct values: Building Trust in Society, IP Rights and Confidentiality, Protecting Human Rights	All employees and employee-like contractors.	CEO	Use of AI in security applications AI increases risk of security breach

Table 46. Consumer and end-user policies.

While our Code of Conduct is applicable for Consumers and End-Users, serving customers and partners in a business ethical manner is described in the Business Conduct section and under the "Code of Conduct training target".

The following IROs do not have policies inked to them but are managed as part of F-Secure's business operations:

- Create awareness about cybercrimes
- Channel strategy
- Consumer willingness to pay

Externally reported targets have not been set for Create awareness about cybercrimes. However, F-Secure tracks the effectiveness of consumer cybersecurity awareness activities through quantitative engagement metrics including audience reach of partner campaigns, click-through rates on threat reports and guides, web session volumes for direct-to-consumer content, media article readership, and social media following.

Human rights commitments relevant to consumers

F-Secure has embedded commitment to international human rights in its Code of Conduct, considering globally recognized principles (refer to S1-1 for details).

F-Secure's internal policies, procedures and guidelines are aligned with the Code of Conduct and these international principles. Our commitment extends to end-users through products and services designed to respect human rights and ethical standards, including data privacy protections, secure processing of personal data, and transparent communication about user rights and responsibilities.

Engagement and Reporting Mechanisms: End-users can 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 without fear of retaliation. All reports are investigated with prompt corrective actions implemented, including remedies for human rights impacts where appropriate.

Alignment with internationally recognized instruments (SFRD and Pillar)

F-Secure is certified to **ISO 27001:2022 Standard for Information Security Management** across all operations. The standard defines controls for managing information security covering people security, secure software development, security incident response, and business continuity. Sub-standards and reference controls include:

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

Compliance Record: No reported cases of non-respect of UN Guiding Principles on Business and Human Rights, ILO Declaration on Fundamental Principles and Rights at Work, or OECD Guidelines for Multinational Enterprises involving consumers and/or end-users.

Progress Monitoring: Processes for monitoring and measuring progress are described under the Metrics and Targets section where cybersecurity training completion rate, cybersecurity incidents, and ratio of externally reported product vulnerabilities to internally identified vulnerabilities are primary metrics.

S4-2 Processes for engaging about impacts

F-Secure deploys several methods of collecting and analyzing consumer perspectives. The majority of engagements are direct with dialog between F-Secure and consumers, including customer care contacts, app store feedback, and social media feedback. F-Secure requests formal feedback through a continuous product survey process. All data is analyzed, responded to (when channels allow), and reported to applicable F-Secure stakeholders for processing.

We receive feedback from channel partners regarding their end-users that is processed similarly. Engagement scope and frequency vary between partners through joint customer need surveys, generic feedback from partners' market and consumer surveys, or feedback from their customer care teams.

Stage and frequency of engagement

F-Secure closely follows customer lifecycle performance in Direct Business. The majority of consumer engagement happens after onboarding, once consumers have installed and activated protection services. Daily engagement occurs through the protection app working in the background, protecting device use and consumers' digital moments.

Consumer feedback is obtained continuously, enabling F-Secure to respond promptly to challenges through communication channels mentioned above. All consumer feedback is consolidated, analyzed, and processed monthly.

F-Secure's Chief Product Business Officer, part of the Leadership Team reporting directly to the CEO, has operational responsibility for engagement and integration of results into F-Secure's strategy, business model, and daily activities.

Assessing the effectiveness of our engagement

F-Secure follows multiple consumer-generated metrics, including the number of support cases, NPS (Net Promoter Score), CES (Customer Effort Score), and app store ratings to assess engagement effectiveness. These metrics enable close connection with consumer sentiment, even though most business originates via Service Provider partners. We measure and track app store ratings with partners in Apple App Store and Google Play. Significant changes in metrics or feedback are investigated with corrective actions taken regardless of channel.

Gaining insights into consumers, particularly vulnerable consumers

F-Secure emphasizes the ease of use of protection apps. We strive for demographic representation in testing processes to provide a multitude of cultural perspectives in feedback applied to product creation, avoiding exclusion of consumer groups.

We include compliance with the EU Accessibility Act to maintain wide product usability. No consumer group is excluded in design, with target to make protection easy to activate and use without advanced technical skills. By complying with the

European Accessibility Act and W3C accessibility recommendations, F-Secure strives for ease of use for users with various disabilities.

F-Secure uses its beta community to verify design decisions before product availability to larger audiences.

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

Channels to raise concerns

End-users can reach F-Secure through self-help (community forum and chatbot) and assisted (chat and phone) channels. F-Secure Customer Care is active on social media and app store channels to assist customers. All customer contacts are evaluated with satisfaction measures through post-ticket surveys, including open feedback options. F-Secure provides support services in-house with dedicated resources.

- Phone support multiple languages: Available during business hours for immediate assistance. English for extended business hours.
- Chat support in multiple languages, including chatbot: Available during extended business hours. English 24/7.
- Email Support: Monitored email addresses integrated to create cases to CRM system. Dedicated address for GDPR requests.
- Feedback Forms: Integrated into customer contact cases for product/service feedback.
- Community and Social Media Channels: Official accounts on major platforms for engagement and issue resolution.

These channels are managed internally by the undertaking to ensure timely and consistent responses.

F-Secure has defined support models with channel partners where end-user support services are provided by F-Secure or partners. When channel partners are the first point of contact, we provide help desk training and maintain open support channels for partner assistance. F-Secure provides technical support for partners related to offerings per agreed Service Level Agreements.

Effectiveness and trustworthiness of our support channels

F-Secure logs all customer contacts (inquiries and support requests) within a ticketing system to identify trends, track performance metrics, and make data-driven decisions about customer experience and service improvement. This tracks ticket volume, resolution time, and customer satisfaction (post-ticket survey) per contact channel.

For common issues, we have monthly internal review and verification processes through the customer experience council with action points to remediate issues and follow up on progress. When relevant, we benchmark offered service and customer care metrics, especially post-incident customer satisfaction, with other cybersecurity industry companies and technology sector associations providing insight and research data.

Trustworthiness measures:

- Engage with end-users during the customer lifecycle through the protection app and lifecycle messages informing about available contact channels
- All contact channels are publicly available on the web for anyone to find and use
- Continuously follow the utilization of each channel to maintain effectiveness
- Consumers may provide feedback under the whistleblowing policy through a publicly available whistleblowing channel without fear of retaliation

Customer trust building: All customer care contacts and issue remediation are evaluated with satisfaction surveys after support case resolution, including open feedback options. F-Secure has a complaint process triggered by low post-ticket survey scores and customer requests for contact. This process engages customers to understand perceptions and handles complaints with actions to solve issues to satisfaction, plus internal actions to improve service and build trust. Post-complaint surveys measure complaint handling effectiveness.

S4-4 Actions and resources

Actions to Address Material Impacts

Protecting Digital Moments

Our cybersecurity products and services like F-Secure Total help consumers stay safe online and build trust in digitality. We continuously improve protection capabilities in our apps, SDKs and cloud to increase security efficacy and deliver real-time protection while regularly launching new product versions with new protection capabilities against scams.

During 2025, we continued to expand our scam protection capabilities and launched a dedicated Scam Protection offering in our Direct Business in May 2025. This activity continues during our strategy period (2026–2028) and is executed across our focus regions and channels. Expected outcomes include increasing the number of consumers we protect globally, consumer and partner satisfaction, while creating value for our channel partners and shareholders.

Creating Awareness About Cyber Crimes

Increasing consumer awareness on cybercrime is critical to help consumers stay safe when online. Our dual strategy raises awareness directly with service providers and consumers while equipping our 200+ channel partners to educate their customers. We achieve consumer awareness by making free tools for consumers available, especially in our Direct Business such as identity theft checker, messaging scam analysis, and online scanners. Additionally, we regularly create relevant new content to inform of blog posts, tips and guides, especially related to scams.

For service providers and partners, our annual Cyber Threats Guide drives partner awareness measured in terms of click-through-rates and time spent on the pages, while we measure the effectiveness of our direct-to-consumer articles through sessions and time spent on our web pages. Our PR secures expert placement in major outlets and uses LinkedIn to further increase awareness as measured through reach and/or followers.

With channel partners, our annual Cybersecurity Awareness Month Campaign provides partners with ready-to-use materials to educate their end-customers about cybercrime. Furthermore, we supplement this with year-round white-labelled content and monthly F-Alert bulletins offering timely threat insights. We track the effectiveness of these activities in 2025 through audience reach (consumers reached) and page visits. Expected outcomes of these actions include increased partner satisfaction and preventing consumers from becoming victims of cybercrime. We'll continue expanding these activities throughout 2026 directly and through our partners.

Actions to avoid causing or contributing to a material negative impact on consumers and end-users

F-Secure has not identified material negative impacts on consumers and end-users. Furthermore, 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.

To ensure we don't cause or contribute to material negative impacts towards consumers, we've during 2025 reviewed the effectiveness and trustworthiness of our support channels as described in chapter "S4-3 Processes to remediate negative impacts and channels to raise concerns" in addition to tracking any reports received via our whistleblowing channel. Additionally, our product Net Promoter Score surveys conducted during 2025 serve as a further sensor to gauge, if our product would start to have material negative impact(s).

We expect to continue to assess our support channel effectiveness and trustworthiness as well as conduct product surveys during the strategy period (2026-2028). These activities did not require any material operating expenditures (Opex) and/or capital expenditures 2025, and we expect it to remain the same for the strategy period.

Actions to pursue material opportunities

Actions related to our material opportunities were executed during 2025. We continue to see them as relevant also for the current strategy period (2026-2028):

Opportunity	Actions 2025	Effectiveness Measures and expected outcomes
Evolving Threat Landscape	Re-direct resourcing and investments into research, innovation, and product creation capabilities around scam protection Support channel partners by upgrading them to latest F-Secure product versions with scam protection capabilities Support launching, promoting, and selling security directly to consumers, and via existing and new partners	Number of new scam protection capabilities launched during the year as part of Embedded or Security Suite portfolios. Outcomes directly connected to consumer satisfaction and F-Secure's revenue growth in key regions and channels
Use of AI in Security Applications	More engaging, relevant, and contextual protection experience (user experience) Improved security efficacy where AI technologies advance F-Secure's threat research capabilities and allow providing more effective protection capabilities	Enhances our consumer and channel partner offerings leading to a differentiated market position in our key regions and channels, further driving growth. Improves product NPS.

Table 47. Actions in pursuit of opportunities related to consumers and end-users.

Actions to mitigate material risks

Our most material impact is protecting consumers' digital moments through holistic, engaging cybersecurity products and services directly and through partners. This carries five inherent risks with corresponding mitigation strategies as listed in the table below. These mitigation activities were executed in 2025 in our focus geographies and channels, and we see them being relevant during the strategy period (2026-2028):

Risk	Actions 2025	Effectiveness Measures and expected outcomes
Consumer willingness to pay decline	Continuously add new relevant scam protection capabilities that increase value to consumers. Service Provider partners combine security with their own services or apps for increased value or offer as a new core/ value-added service.	Partner and product NPS tracking, service provisioning, activation and usage rates leading to subscriber base growth and ARPU increase.
Channel strategy risks	Help partners drive their topline growth, lower churn. Deliver value based on a compelling vision and roadmap to meet partners' business needs. Develop healthy sales pipeline.	Partner commitment to sales/ marketing activities, adoption of new versions of our products, NPS evolution and overall funnel development leading to revenue and ARPU increase. Service provisioning and activation tracked similar to previous risk.
Security of suppliers and partners	Security review gateways in procurement process, contractual security requirements enforcement, regular security audits of critical vendors.	% share applied globally to all suppliers and partners. Expected outcome is 100% coverage for critical suppliers.
Cyber security attacks	ISO 27001 standard implementation, proactive security monitoring, vulnerability management, regular crisis rehearsals, continuous policy monitoring and improvement	Number and criticality of security incidents and vulnerabilities in software and third-party solutions. Expected outcome is 0 critical security incidents.
AI increase risk of security breach	Security review of new AI tools, limiting AI access to sensitive information, information processing instructions and security awareness	Number and criticality of security incidents involving AI tools

Table 48. Actions to mitigate risks related to consumers and end-users.

Human rights issues connected to consumers

F-Secure has zero (0) human rights issues or incidents connected to consumers during 2025.

Resources allocated to the management of the material impacts

- **Product Management and Technology:** F-Secure's product management function is responsible for creating product vision, offering, and related product roadmaps to meet partners' and consumer customers' needs in the short and long term. Product management steers our Product Board, which prioritizes product initiatives and roadmaps for technology organization resource allocation for implementation projects (product releases). New product experimentations or initiatives may also be implemented within the Product organization. The Technology organization is also responsible for threat intelligence and research activities, providing effective protection against modern threats.

- **Marketing and Content Creation:** Marketing teams drive a content creation strategy aligned with direct business and partner channel needs and opportunities, supported by technology organization threat intelligence teams providing expert views on latest scams. Implementation of free tools is governed through the Product Board process.

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 the baseline year in all targets except ratio of reported vulnerabilities and completion rate of security awareness where the baseline year is 2024. Progress will be reported annually.

Methodologies

All NPS results are measured through a dedicated marketing survey solution. Cybersecurity training metrics are tracked through F-Secure's Learning Management System. Major cybersecurity incidents and bug bounty-related issues are tracked with a dedicated ticketing system. All systems are used globally with no need for regional data collection.

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 Targets Consumers

Target	Baseline 2023	2024	2025	2030 target
F-Secure consumer product NPS (Total)	49	49	52	55
Partner Business NPS	56	63	55	Above 55
Completion rate of internal cyber security training	Baseline is 2024	95%[1)]	94%	98% (all employees)
Number of major cyber security incidents	2 (no customer data was compromised)	1 (no customer data was compromised)	0	0 incidents involving leaked customer personal data

1) Target updated for 2024 (97%) including all employees.

Table 49. Consumer and end-user targets.

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, leveraging opportunities in the evolving threat landscape, and mitigating risks around consumer willingness to pay.

Net Promoter Score (NPS) measures 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 ranging from -100 to +100.

At F-Secure, NPS tracks progress in fulfilling our vision to become the number 1 security experience company and mission to continuously deliver brilliantly simple, frictionless security experiences. NPS reflects product quality, customer journey, sense of security, and trust-related sentiments of consumer customers.

An NPS target has been set for our main consumer product F-Secure Total, measured in our Direct Business channel. The F-Secure Total NPS target for 2027 is 50 and 55 for 2030. The 2025 outcome for product NPS is 52. We review progress monthly and report the NPS outcome annually as part of the sustainability report.

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

Partner Business NPS evolution

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

We apply NPS to measure 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 outcome in 2025 was 55. We expect our NPS score to remain above 55 in the medium and long term.

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

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

Completion rate of internal cybersecurity training

The completion rate target of F-Secure cybersecurity training measures F-Secure employees' awareness of internal security policies. This target is based on objectives defined in F-Secure Cybersecurity Policy and Personal Data Policy, measuring employee knowledge against the company's general cybersecurity objectives, security policies and guidelines.

The target is calculated based on the current employee count, and presented as a completion percentage (%). All F-Secure employees are part of the target with no geographical boundaries.

We have set a 2030 target of reaching a training completion rate of over 98%. For 2025, the training completion outcome was 94%. We review progress regularly and report the outcome annually.

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

Training data is extracted from F-Secure's learning management system, and information related to long-term absences comes from our HR systems.

Number of major cybersecurity incidents

The number of major cybersecurity incidents target is based on objectives related to information security and privacy defined in F-Secure Cybersecurity

Policy. It measures company security processes and their capability to prevent major incidents from occurring, and the impact of cybersecurity incidents on F-Secure customers.

The occurrence of major cybersecurity incidents is tracked as part of F-Secure 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. 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. In 2025 our outcome was 0.

The target measurement is not completely absolute since it is dependent on human assessment of the incident. This shortcoming is mitigated by having multiple security team members review all incidents.

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

Metrics tracked internally

Ratio of externally reported product vulnerabilities to internally identified vulnerabilities

F-Secure also tracks the effectiveness of cybersecurity-related policies and actions with alternative processes through monitoring bug bounty reports and internally identified vulnerabilities. This bug bounty-related metric is based on objectives related to software security defined in F-Secure's Cybersecurity Policy. It measures F-Secure's engagement with the cybersecurity researchers' community and the efficiency of the company's secure software development processes.

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.

The target tracks ratio of externally reported product vulnerabilities where bounty has been paid to internally identified vulnerabilities. This includes comparing externally reported medium, high and critical vulnerabilities to what has been found by F-Secure internally. 2024 is the baseline year.

The target measurement is not completely absolute as it depends on human assessment of the reported finding. This shortcoming is mitigated by having multiple developers review the reports and criticality and the suggested bounty compared to earlier paid bounties.

GROUP SUSTAINABILITY REPORT -

Governance

G1 – Business conduct

SBM-3 Material impacts, risks and opportunitites

	Material impact, risk or opportunity	Description
Business Conduct		
Corruption or bribery		
Risk (DVC)	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 (DVC/UVC ,OO)	M&A transactions	Anti-Bribery and Corruption risks increase as a result of M&A transactions due to limited understanding of the target
Corporate culture		
Actual Positive impact (OO)	Culture reinforcement	F-Secure is strengthening its culture by reviewing people and culture structures to reflect the desired culture, supporting leadership and team development, and fostering a culture of experimentation
Protection of whistleblowers		
Actual Positive impact (OO/DVC)	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.

Table 50. Business conduct-related list of IROs.

Impact, risk and opportunity management

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. Our desired culture includes values, aspired behaviors, and leadership principles. Our culture is called “Fellowship” and it includes four values: 1) Keep focus, 2) I make a difference, 3) Just do it, and 4) Dare to care.

To foster our corporate culture, we have implemented the following key actions:

- We have implemented a Leadership Academy with learning programs for current and aspiring leaders. Through the Leadership Academy, our goal is to strengthen our ‘ready-now’ leadership succession pipeline to 65% by the end of 2026. The program targets current Team Leaders and high-potential employees identified through talent calibration processes. Launched in 2023, the Leadership Academy has ongoing annual programs continuing through 2025 and beyond. The programs are funded through annual operational budgets.
- We have established a strategic forum for leaders called Leadership Lab. The expected outcome is to foster strategic alignment and execution, measured by F-Secure Objectives and Key Results achievement, enable collaborative decision-making, and create a shared understanding of organizational priorities among leadership. All F-Secure Team Leaders are invited to the sessions (approximately 90 leaders). The forum was established in a different format already in 2022 and is organized quarterly in 2025, continuing as a permanent leadership practice.
- We have strengthened active and transparent internal communications through clarifying our key internal communication channels, and strengthening the opportunities of employees to actively participate and provide feedback in monthly townhalls. We aim to increase employee understanding of strategic direction and priorities and enhance two-way dialogue. The scope includes all Fellows across F-Secure's global locations. These actions have been enhanced starting in 2024, with continuous improvement and regular communication touchpoints.
- We have supported team performance dynamics building. We expect Talent Density (i.e., the proportion of high-performers in the organization) to grow to 50% by the end of 2025 and the results will be available in March 2026. We have been focusing on teams where we have identified needs for enhancing trust and psychological safety, impact and meaning, clarity and structure, and/or accountability and dependability. We measure this in our Fellow survey with a high-performing team index covering the above-mentioned four dimensions of high-performing teams. Thus far, we’ve focused on the most crucial 10% of our teams that are identified through our Fellow survey as having gaps in high-performing team components mentioned above. This is an ongoing effort started in 2025 and continuing going forward.
- We have renewed our leadership annual clock in 2025. We aim to systematically lead performance, learning and development, as well as recognition and rewards. The annual process cycle enables linkages between these core processes in a way that performance and learning boost the growth of employees, and where high performance is recognized and rewarded. The annual leadership processes concern all Fellows and are a continued effort going forward.
- We have also continued reviewing employee lifecycle processes aligned with our culture to ensure value-aligned experiences throughout the employee journey from pre-boarding and onboarding through performance management, learning and development, and exit. Through the above-mentioned actions, voluntary attrition remained under 12%. The scope includes all Fellows across the organization. The renewal of the processes was initiated in 2024, with implementation aimed to be completed in 2026. Yet, we will continuously improve these structures and processes going forward.
- We track cultural development through regular Fellow surveys. Through the survey, we monitor cultural health, measure engagement levels, identify improvement areas, and inform action planning to address any concerns while maintaining high engagement. The main outcome is employee engagement measured by eNPS, where we aim for 50 by the end of 2030. The scope includes all Fellows biannually. The survey is a continuous action with regular survey cycles.

G1-1 Policies

Policy	Key Contents	Scope	Responsibility	Link to IROs
Code of Conduct	Outlines F-Secure's ethical principles, values, and expected behaviors. Includes anti-corruption standards and reporting procedures. Further information regarding which third-party standards and initiatives F-Secure commits to respecting through the Code of Conduct is disclosed under S1-1.	All employees and leadership. Suppliers and channel partners expected to adhere to principles.	Owned by the General Counsel, approved by the Board of Directors	Partnership business, use of agents and other intermediaries M&A transactions Whistleblower channel available Culture reinforcement
Anti-Bribery and Corruption Policy	Covers prohibited conduct, gifts, conflicts of interest, third-party due diligence, compliance requirements, and enforcement procedures. Based on the UN Convention Against Corruption.	All employees and leadership. External officers.	Owned by the General Counsel, approved by the Board of Directors	Partnership business, use of agents and other intermediaries M&A transactions
Whistleblowing Policy	Defines reporting channels, investigation procedures, and protections for whistleblowers, including confidentiality and anti-retaliation measures.	All employees and external stakeholders.	Owned by the General Counsel, approved by the Board of Directors	Whistleblower channel available

Table 51. Business conduct policies.

These policies and relevant complementary procedures and guidelines are available to employees on the F-Secure intranet and SharePoint, which are accessible to all employees. Any updates to the policies are communicated via the news section on the intranet, the monthly newsletter, and Townhall meetings. The mandatory Code of Conduct training also outlines the key elements of these policies to help employees understand their implications. The Code of Conduct and Whistleblowing Policy are also available to the public on the F-Secure website. These policies are owned by the General Counsel and approved by the Board of Directors, and other stakeholders have not been directly involved in setting these policies.

External officer in this context refers to any agent or any other party representing or acting on behalf of F-Secure who is not in an employment relationship with F-Secure.

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

F-Secure employees have multiple channels to report Code of Conduct violations: direct communication with managers, Legal, or HR; our anonymous whistleblowing channel; or writing to our CEO or Board. External stakeholders can use our public whistleblowing channel.

All reports are handled confidentially with appropriate measures taken against violations. F-Secure provides measures to protect against retaliation against its own employees who are whistleblowers in accordance with Directive (EU)2019/1937, including:

- identity protection;
- 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;
- 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 also provides protection 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, we monitor anti-corruption effectiveness through regular audits and reviews. F-Secure has procedures to investigate business conduct incidents promptly, independently, and objectively. All employees must accurately record financial transactions with proper documentation.

Policy for business conduct training

Our Code of Conduct training is mandatory for all employees, including specific modules on anti-corruption and reporting procedures. New employees complete this during onboarding, with refresher training required every two years. This training covers 100% of high-risk functions, particularly sales and procurement teams, which we've identified as most susceptible to corruption and bribery risks. The Code of Conduct training also includes information to employees about the whistleblowing channel and other mechanisms for reporting Code of Conduct violations.

G1-3 Procedures to address corruption and bribery

F-Secure encourages a culture of openness and accountability. Employees who suspect policy violations can report through multiple channels: speaking to managers, Legal, or HR; using our whistleblowing channel; or writing to the CEO or Board. We guarantee a confidential review of all reports and protect whistleblowers from retaliation.

We require an accurate recording of all financial transactions involving F-Secure expenses or asset transfers. Our expense management systems maintain proper documentation and transparency. The effectiveness of our anti-corruption efforts is monitored through regular audits and reviews that identify and address risk areas or compliance issues.

No action plans require significant capital expenditure (CapEx) or operating expenditure (OpEx), and all actions are funded through normal business operations.

Investigating and reporting incidents

When investigating suspected incidents, we ensure investigators are separate from the management chain involved in the matter. Investigation teams are determined on a case-by-case basis to ensure impartiality. Substantiated investigations involving corruption or bribery are reported to the Audit Committee, with outcomes communicated to relevant management bodies and to authorities when legally required.

Nature and scope of the training programs

F-Secure's anti-corruption training is mandatory for all employees, with particular focus on high-risk functions. The training includes realistic scenarios that test employees' ability to apply Code of Conduct principles to decision-making situations and covers appropriate reporting mechanisms. This comprehensive training ensures 100% coverage of functions at risk, particularly those in sales and procurement, as well as our executive management, including the Leadership Team.

Metrics and targets

G1-4 Targets

G1-4 Targets Business Conduct

F-Secure has established two targets related to business conduct:

Target	Baseline 2023	2024	2025	2030 target
Zero-tolerance on bribery & corruption	0 incidents	0 incidents	0 incidents	0 incidents
Code of conduct training target	*Baseline is 2024*	96%	96%	98% (Permanent and fixed-term employees)

Table 52. Business conduct targets.

G1-4 Progress towards targets

F-Secure reports zero convictions and zero fines for violations of anti-corruption and anti-bribery laws during 2025. As there have been no known breaches in anti-corruption procedures or standards, we have not needed to take remedial actions.

Zero-tolerance on bribery & corruption

Our zero-tolerance target is based on our Code of Conduct principles and Anti-Bribery and Corruption Policy. 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 F-Secure's Board of Directors. The target applies to all F-Secure operations globally and aims to maintain zero incidents of bribery or corruption. 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. The target is absolute, and it is measured in the number of incidents related to bribery or corruption. With zero incidents since our 2023 baseline, we are on track to maintain this performance through 2030.

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.

Code of Conduct training target

This target aims to ensure that 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 training includes anti-corruption components and proper reporting procedures. With 2024 as our baseline year, we've achieved 96% completion, working toward our 2030 target of 98%. The General Counsel, together with the Leadership Team, has set this target. This target acknowledges practical limitations like recent hires and employees on extended leave. We monitor performance through our Learning Academy platform and implement targeted follow-up for non-completions. The reported Code of Conduct training target includes permanent and fixed-term employees and excludes individuals for whom employee status information is unavailable.

G1-4 Incidents of corruption or bribery

G1-4 Confirmed incidents

	2024	2025
Number of convictions and amount of fines for violations of anti-corruption and anti-bribery laws	0	0

Table 53. Incidents of corruption or bribery.