

W / T H[®]
secure



WithSecure Annual Report 2024



Contents

WithSecure 2024	3
WithSecure in Brief	3
WithSecure Elements	4
WithSecure - 2024 sustainability highlights	5
WithSecure in 2024 – Becoming a European flagship of cyber security	6
Board of Directors' report and financial statements	8
Board of Directors' report	10
Sustainability Report	25
WithSecure consolidated financial statements	101
WithSecure Corporation financial statements	142
Signatures of the Board of Directors' report and Financial statements	158
Auditor's Report	159
Assurance Report on the Sustainability Report	165
Auditor's assurance report on ESEF Financial Statements	168
Corporate Governance	170
WithSecure's Corporate Governance Statement 2024	172
Internal control and risk management	177
Board of Directors	179
Global Leadership Team	183
Remuneration Report	187
Letter of the Chair of the Personnel Committee	189
Remuneration of the Executives and company performance during the last five financial years	191
Remuneration of the Board of Directors	192
Remuneration of the President and CEO	193
Information for shareholders	198
Contact information	198

WithSecure in Brief

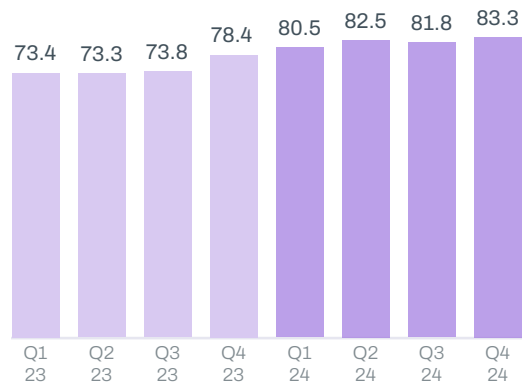
Building and sustaining digital trust, confidence and equity.

Elements Company

105.7
2024 Revenue

694
Employees

Cloud ARR *EUR million*

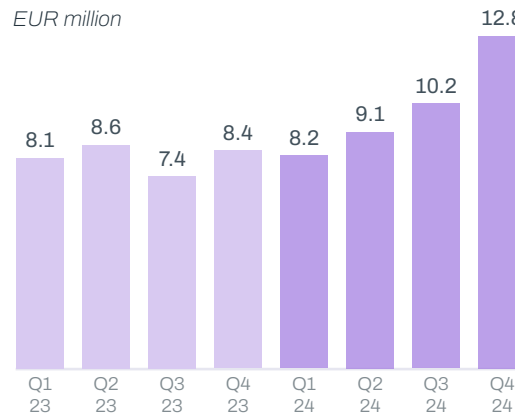


Cloud Protection for Salesforce

9.4
2024 Revenue

37
Employees

ARR *EUR million*



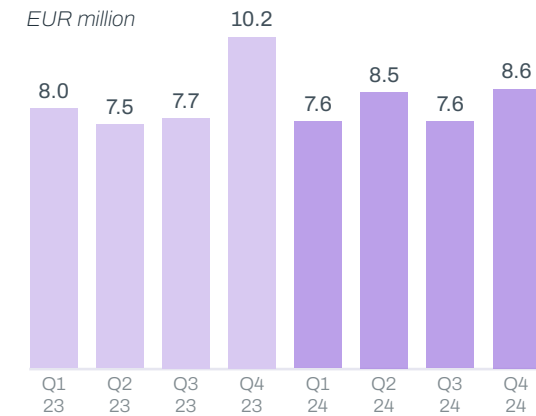
Cyber Security Consulting

to be divested in 2025

32.3
2024 Revenue

230
Employees

Revenue *EUR million*



Founded

1988

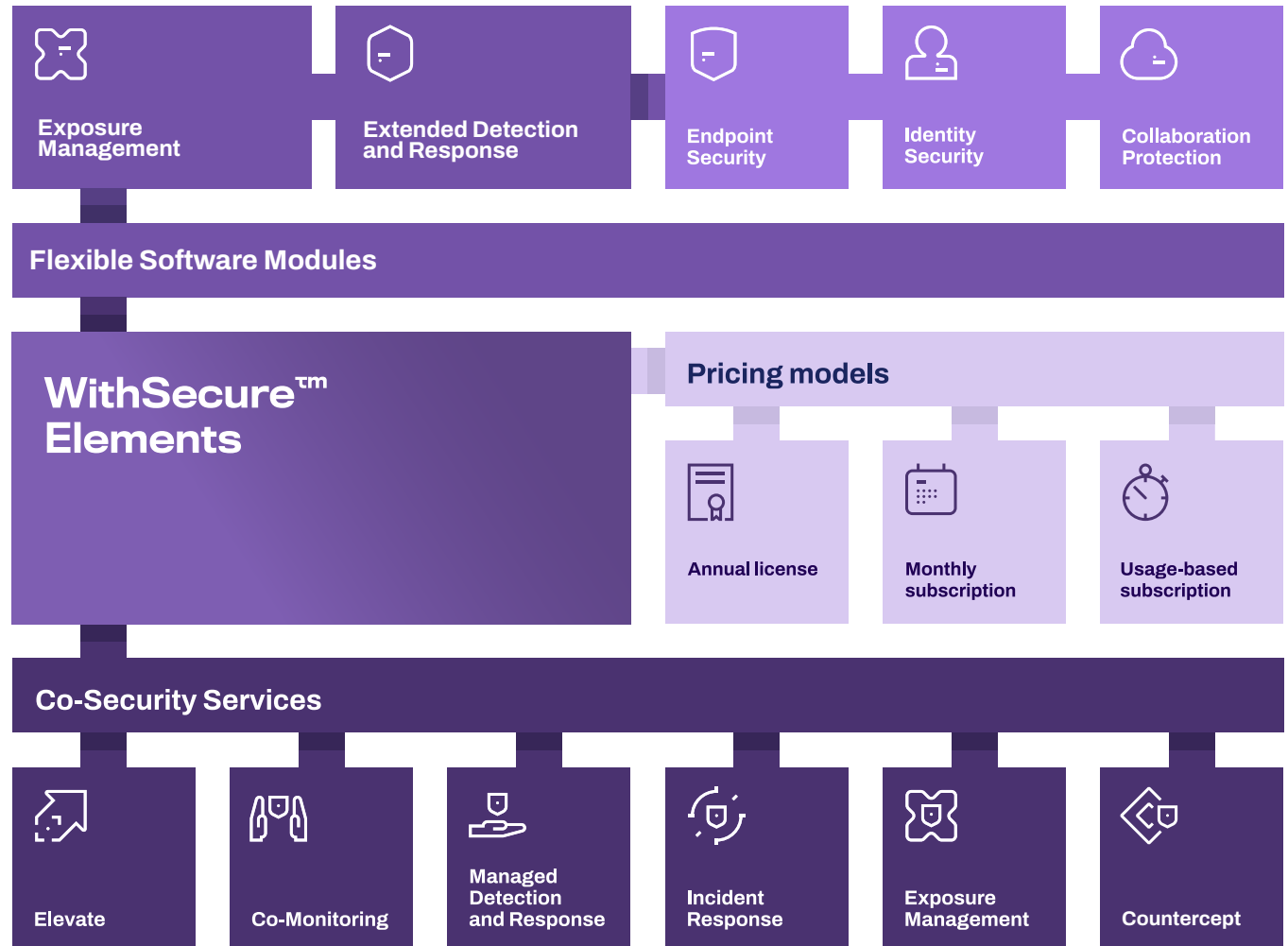
2024 Adj. EBITDA

3.1

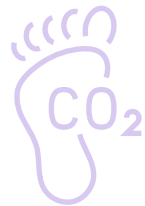
Unified Elements-based offering

One Experience.
Fully modular.
Made for Co-Security.

WithSecure Elements™ is a unified, cloud-based, intelligent and highly automated cyber security platform. It is complemented by world-class services, available to customers and partners according to their needs.



WithSecure 2024 sustainability highlights



Carbon footprint decreased to **69.2 tons of CO2** per million EUR of revenue.

100%

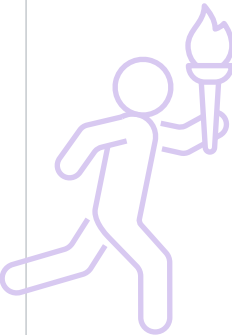
completion rate of Code of Conduct training for new employees.



NO major security incidents

according to NIS2 directive.

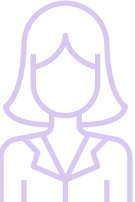
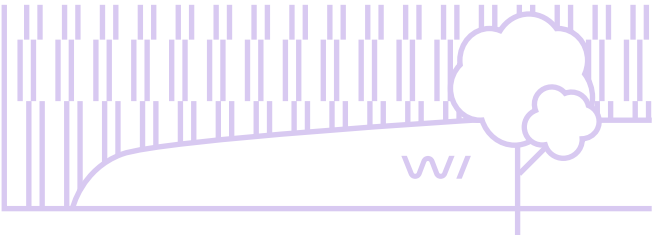
ISO 27001 and **ISAE 3000** certifications for cyber security.



WithSecure partnered with the **Finnish Olympic Committee**

to enhance cybersecurity in Finland's sports community, securing Suomisport's **850,000 accounts** used by athletes, parents, and over 4,000 clubs and societies.

Helsinki office moved to new headquarters in **Wood City**, where the building has a **LEED Platinum certification** and **A class energy rating**.



The representation of **female leaders** among line managers increased from **22% to 26%**.

WithSecure in 2024 – Becoming a European flagship of cyber security



Digital services are an integral part of society – they are expected to work seamlessly without any disruptions. Cyber security, together with the institutions offering physical security, has become a pillar of a secure society. The fast-evolving industrial-scale cybercrime means cyber security is a must for every company, regardless of their size. For the past year, WithSecure has been focusing its strategy on solving the cyber security challenges of mid-market companies. Our aim is to offer our customers a selection of software and services that provide cyber resilience and trust in digital society, efficiently and in compliance with regulation. In the changing geopolitical environment, we take pride in providing a European alternative for cyber security, and uncompromising reliability in the trust business.

With the increasing complexity of cyber security risks, an effective protection of our customers is always

a result of collaboration between WithSecure, our partners and end-customers. We are in a continuous dialogue to ensure that our products meet both the cyber security needs of the end-customers and create meaningful portfolio items for the partners who are selling them as part of their own offering.

In 2024, the economic growth in the European markets was modest and continued to be impacted by the geopolitical uncertainties. On the other hand, previously surging inflation subsided, and the unemployment rates remained at low levels. Positive development in the markets outside Europe offset some of the impacts, but WithSecure's main markets are mostly located in Europe. Despite the economic headwinds, WithSecure's revenue of Continuing operations grew by 6% in 2024, and the company was adjusted EBITDA profitable for the past financial year.

We expanded the offering by an important product in 2024: WithSecure Exposure Management was launched in May, and it became generally available in the third quarter. It provides continuous scanning of the customer's attack surface, with estimated impacts of the attack paths and recommendations for remediations generated by AI. Customer interest on Exposure Management has been high, and we expect it to be a growing product in the next few years. We also added Identity security to our product portfolio and introduced the AI assistant Luminen, which has been providing its advice to all our Elements customers since September 2024.

Elements Cloud revenue grew by 9.4% in 2024 and was EUR 83.3 million (EUR 76.1 million). Annual Recurring Revenue (ARR) growth in the same period

was 6.2%. Total Elements Company segment revenue grew by 4.5% in 2024 and was EUR 105.7 million (EUR 101.1 million).

Cloud Protection for Salesforce (CPSF) is a software product ensuring scanning of external content for potential malware, before it is loaded to Salesforce. The CPSF team's continuous, systematic efforts to improve sales execution are providing strong results. The ARR growth of the business was 52% from the previous year-end. The growth is driven by both new customers – we were glad to welcome many new international enterprise customers in the past year – and expansions to existing customers. We continue to develop the CPSF as an independent business inside WithSecure, while keeping the strategic review options open.

On 23 January 2025, WithSecure signed an agreement intending to divest the Cyber security consulting business. Consulting is reported as part of the Discontinued operations result in the 2024 financials. WithSecure consultants are offering world-class offensive security services to some of the most demanding customers in the world. We are very happy to have a new owner who will continue to develop the business as an independent company. The divestment is expected to close during the second quarter of 2025.

For the past two years, WithSecure has been focusing on profitable growth. The full company adjusted EBITDA (Continuing and Discontinued operations total) of 2024 was EUR 3.1 million (EUR -16.1 million). Full-year operative cash flow before financial items and taxes was EUR 2.1 million. We are pleased to

report the improvement in profitability, demonstrating that the cost structure has been adjusted to a level that can sustain some volatility of revenue.

WithSecure, as a company, went through many changes in 2024. We had a sudden change of CEO in April, when the previous CEO Juhani Hintikka stepped down from his position. I was first appointed as interim CEO, and on 1 July 2024 as the CEO of WithSecure. I have had the pleasure of looking at the company from a new perspective, and appreciate the diversity, capabilities and excellence of our teams and partners. In May, we arranged our third SPHERE event for customers and partners. The event was marked by launches of our new products, but also by joyful meetings and inspirational speakers – even a detective story on cyber security was published at SPHERE. In October, our Helsinki team moved to our new Wood City headquarters that provide an environmentally sustainable and inspiring environment for working.

At the closing of my first financial year as the WithSecure CEO, I would like to thank our personnel for their great work and change resilience. I also want to thank the WithSecure partners, customers, shareholders, and other stakeholders for your collaboration. We are looking forward to a great continued partnership with you in 2025.

A handwritten signature in black ink, appearing to read 'Antti Koskela', written in a cursive style.

Antti Koskela



Board of Directors' Report and Financial Statements

Contents

Board of Directors' report	10
Signatures of the Board of Directors' report and Financial statements	158
Auditor's Report	159
Assurance Report on the Sustainability Report	165
Auditor's assurance report on ESEF Financial Statements	168

Board of Directors' report

Year 2024 was marked by modest growth rates and economic uncertainty in WithSecure's main markets in Europe. Geopolitical situation remained tense and unpredictable. Increasing complexity of system landscapes, together with the rise of new technologies, are setting continuously new challenges for the cyber defenders.

After its strategy update in October 2023, WithSecure has been focusing strongly on the "mid-market playbook", ensuring a comprehensive offering of cyber security products and services that enable small- and medium-sized companies to protect themselves from the complex threats, and to ensure they are prepared for the increasing regulatory requirements such as the NIS2 directive that is currently being implemented in the EU countries.

WithSecure's Elements Company segment revenue grew by 4% from previous year and was 105.7 million. The growth is driven by the cloud-based security products and services, where the annual growth rate was 9%. Revenue from the on-premise and other legacy products declined by 12%, which is according to the company expectations.

Cloud Protection for Salesforce (CPSF), disclosed as a separate segment, is a software product ensuring scanning of external content for potential malware, before it is loaded into Salesforce. Customers are primarily enterprise-sized companies, with extensive use of Salesforce platforms. Its sales developed well in 2024, leading to a revenue growth of 14%. WithSecure continues to develop the CPSF as an independent business inside the group, in order to be prepared for future options.

On 23 January 2025, WithSecure announced that it has entered into an agreement intending to divest the Cyber security consulting business. Consulting is reported as part of the Discontinued operations result in the 2024 financials. As an exception from this rule, the segment reporting is based on the calculation principles applied during 2024, to ensure comparability.

Market overview

The global cybersecurity market is a rapidly evolving industry driven by increasing digitalization, growing cyber threats and the widespread adoption of cloud-based

technologies. In 2024, the market experienced increasing security demands across industry verticals and sectors. Factors driving market expansion were among other things rising data breaches due to identity-based attacks, ransomware, increasing regulatory requirements and increasing adoption of AI. The global geopolitical tensions are also creating increased activity and threats for private and public organizations.

Constantly evolving attack vectors require continuous innovation in organization of all sizes. Overall economic uncertainty and IT budget constraints have slowed down the adoption of the latest cyber security technologies, especially among small and medium-sized enterprises (SMEs). At the same time third-party breaches across the supply chain and a global shortage of skilled cybersecurity professionals remain as pressing issues.

Globally organizations are investing in cyber defenses to combat growing threat levels in a digitized economy. North America holds the largest market share due to significant investments in cybersecurity infrastructure whereas in Europe the increased awareness of regulatory requirements has been contributing to steady growth.

AI capabilities have been increasingly introduced to improve productivity and reduce threat detection and response times. Stolen or compromised credentials remain the most prevalent attack vector that is addressed by emerging Identity Security solutions. Cloud Security continues as a high-growth segment as companies seek to protect their modern IT environments and cloud-based services. Organizations have started to recognize the need of moving their focus from reactive to proactive security approach that is fueling the demand for emerging exposure management solutions. There is also increasing demand for securing IoT devices and operational technology against vulnerabilities and cyberattacks. Managed security services will continue to address the skills and resource shortages.

The cybersecurity market is poised for sustained growth as organizations prioritize cyber resilience and compliance. With advancements in AI, cloud-native security, and exposure management, the industry is set to address increasingly complex threats while capturing new opportunities in emerging sectors.

Financial performance and key figures

Continuing Operations

Revenue and ARR

Total revenue of Continuing operations increased by 6% to EUR 116.0 million from the previous year (EUR 109.9 million).

In 2024, WithSecure started to report its revenue split into three segments. Elements Company segment is split further to Elements Cloud products and services, On-premise products and Other revenue. Cloud Protection for Salesforce is a software product that is reported as a separate segment.

Third segment, Cyber security consulting, is reclassified to Discontinued operations, following the signing of a divestment agreement in January 2025. As a deviation from this rule, it is still presented as a segment in the segment reporting, following the previously applied calculation principles.

Elements Cloud products and services

Elements Cloud products' and services' revenue grew by 9% to EUR 83.3 million (EUR 76.1 million). The growth was driven by both new customer acquisition as well as expansion of existing customers to new products, especially Endpoint Detection and Response (EDR). Exposure Management and Identity security were launched in 2024 as new modules to the platform. Elements Cloud platform is regularly updated with new features to provide a comprehensive and up-to-date cyber security protection to the customers.

For cloud and on-premise products, WithSecure reports the Annual Recurring Revenue (ARR) on a quarterly basis to reflect the latest status of recurring revenue sales. The ARR is calculated by multiplying the monthly recurring revenue of the last month of the quarter by twelve. Monthly recurring revenue includes recognized revenue within the month excluding non-recurring revenues. In 2024, Elements Cloud ARR grew by 6% from previous year and was EUR 83.3 million (EUR 78.4million).

On-premise products

On-premise security products' revenue declined by 12% to EUR 21.4 million (EUR 24.4 million). The decline is in line with WithSecure's expectations, it is a consequence of the customers moving their data processing to cloud environments.

Cloud Protection for Salesforce (CPSF)

CPSF revenue grew by 14% to EUR 9.4 million (EUR 8.3 million). ARR grew by 52% to EUR 12.8 million (EUR 8.4 million). Revenue growth was driven by both acquisition of new customers and expansions to existing customers.

Gross margin

Gross margin of Continuing operations for 2024 increased to EUR 92.6 million (EUR 86.8 million) and was 70.2% (65.1%) of sales. Continuous work on aligning technology platforms of the MDR solutions, as well as optimizing data processing costs has resulted in improved profitability.

Operating expenses

Operating expenses, excluding items affecting comparability (IAC) as well as depreciation and amortization, declined to EUR 92.6 million (EUR 103.1 million). The development is mostly a result of cost savings and other efficiency measures taken by WithSecure in the past two years.

Items affecting comparability (IAC) were EUR -0.9 million (EUR -9.0 million). Of this, EUR -0.6 million is related to restructuring activities, EUR -0.5 million to restructuring costs related to HQ relocation, EUR -1,0 million relates to other strategy projects, EUR +0.8 million to earn-outs and EUR +0.4 million to divestments.

Profitability

Continuing Operations Adjusted EBITDA was EUR 2.0 million for 2024 (EUR -14.8 million in 2023). The improvement of profitability is partly related to the improved Gross margin. In addition, WithSecure has carried out cost savings and other efficiency measures to bring the operating expenses to a level that allows profitable growth.

Discontinued Operations result

Discontinued Operations result includes the Cyber security consulting segment result, adjusted to correspond with the scope of the divested business. In addition, the direct costs related to divestment, as well as impairment of the consulting-related goodwill are included in the Discontinued Operations results. A bridge between the segment and Discontinued Operations result is presented in the company's fourth quarter financial release.

Cash flow (Combined operations)

Cash flow from operating activities before financial items and taxes was EUR 2.1 million (EUR -19.9 million). Negative operative cash flow in 2023 was driven by operative result as well as significant restructuring related costs. Improvement of cash flow is a result of revenue growth and cost efficiency measures.

Total change in cash was EUR -9.4 million (EUR -17.9 million), after deducting the payments of lease liabilities.

Acquisitions and financial arrangements

WithSecure did not carry out acquisitions during 2024.

Changes in the group structure

WithSecure did not have any changes in its group structure during 2024.

Capital structure - Combined operations

The Group's liquid assets of EUR 27.3 million (EUR 36.6 million) consisted of cash and cash equivalents. Cash and cash equivalents include bank deposits with maturity of less than three months.

Research and development

WithSecure research and development expenditure in 2024 was EUR 35.0 million (EUR 36.3 million), representing 30% (33%) of revenue. Capitalized development expenses were EUR 1.7 million (EUR 3.0 million). WithSecure is a cyber security technology company for which the ability to innovate is imperative.

In 2024, WithSecure products have been recognized in third party technology evaluations. We believe this is for providing the best protection, advanced detection and effective response capabilities and high customer satisfaction. Gartner® yet again included WithSecure in their September 2024 Magic Quadrant™ for Endpoint Protection Platforms¹. During 2024, WithSecure achieved top marks in the scoring for Protection and Usability in AV-TEST's continuous evaluation of the Elements portfolio. We feel this is a strong statement to the value of our solution that protects our customers effectively without sacrificing its precision. For the sixth consecutive year, WithSecure participated in MITRE's ATT&CK® Enterprise evaluation. This year's evaluation was more sophisticated than before, featuring a revised methodology and challenging participants with multiple emulated threat actors. WithSecure's performance was impressive and showed a significant improvement from last year. WithSecure Elements effectively detected threat actor activity in a way that was actionable and minimized unnecessary alerts and false positives, ensuring user productivity was not disrupted.

As a leading European cybersecurity vendor, WithSecure is dedicated to continuously monitoring the evolving threat landscape and tracking malicious actors and adversaries. In 2024, WithSecure made significant strides in exposing threat actor activity through groundbreaking research on KrustyLoader and Kapeka, effectively weakening their tools and operations. The company also published reviews addressing key aspects of the threat landscape, including the trend of mass exploitation of Edge Services and Infrastructure, the state of the ransomware landscape, and the cyber threats facing the 2024 Olympic Games. Furthermore, successful collaboration with law enforcement officials in cyber security related matters has been part of WithSecure's activities, reflecting the company's unwavering dedication to making the world safer.

¹ GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner content described herein (the "Gartner Content") represents research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, Inc. ("Gartner"), and is not a representation of fact. Gartner Content speaks as of its original publication date (and not as of the date of this Annual Report), and the opinions expressed in the Gartner Content are subject to change without notice.

WithSecure also focused extensively on the topic of Large Language Models (LMM) and the challenges and opportunities that they bring to cybersecurity, resulting in several highly visible publications. WithSecure team have advised many high-profile entities and media outlets on the topic and plans to continue researching what happens at the intersection of cybersecurity and AI. The results of the research are regularly shared on the [WithSecure™ Labs](#) website.

Year 2024 brought along advancements to the WithSecure product and service offering. Building on the Elements launches of the previous year, WithSecure continued to further develop the unified capabilities of its Elements Cloud platform. WithSecure launched Elements Exposure Management, a completely new product enabling organizations to proactively identify cyber security exposures and mitigate them to reduce risk and ensure compliance. Elements Exposure Management builds on WithSecure's decades of cyber security research and expertise, incorporating new technologies and approaches such as the heuristic attack path engine that emulates how a real-world cyber attacker would attempt to breach an organization.

WithSecure further strengthened its offering in Extended Detection and Response (XDR) by launching Elements Identity Security to detect and respond to identity-based threats. For organizations with limited cyber security skills and resources, WithSecure launched WithSecure Managed Detection and Response (MDR) tailored to the needs of mid-size companies being served by local IT partners and managed service providers.

A testament to WithSecure's continued innovation was the launch of W/Lumina, WithSecure's AI assistant that utilizes advanced artificial intelligence and large language models (LLMs). W/Lumina provides users with immediate, actionable, and context-specific analysis of any security events in their organization as well as recommendations on how to resolve and proactively mitigate cyber security threats.

Organization and management

Personnel

At the end of 2024, WithSecure had 961 employees (1,087). Of this, 731 (813) are employees of the Continuing operations, and 230 (274) are employees of the Discontinued operations. Reduction of employees is partly resulting from normal attrition, partly from the restructuring at the end of 2023.

Leadership team

On 8 April 2024, Juhani Hintikka, President and CEO of WithSecure, announced that he steps down from his position in the company. The decision to step down follows the Supreme Court ruling of 5 April 2024 where Juhani Hintikka was found guilty of abuse of inside information related to a matter dating back to 2014, years before he joined WithSecure. The Board of Directors appointed Antti Koskela to act as the interim CEO of the company. As of 1 July 2024, Antti Koskela was appointed as President and CEO of WithSecure. Pilvi Tunturi was appointed as interim Chief Product Officer.

As of 1 November 2024, following the organizational updates of WithSecure, Scott Reininga's position ceased to be a part of the Global Leadership Team.

At the end of the year, the composition of the Global Leadership Team was the following: Antti Koskela (President and CEO), Christine Bejerasco (Chief Information Security Officer), Lasse Gerdt (Chief Customer Officer), Charlotte Guillou (Chief People Officer), Tom Jansson (Chief Financial Officer), Tiina Sarhimaa (Chief Legal Officer), Pilvi Tunturi (interim Chief Product Officer), and Ari Vanttinen (Chief Marketing Officer).

On 1 January 2025, following the organizational updates of WithSecure, Charlotte Guillou became Chief Culture and Performance Officer, Lasse Gerdt became Chief Revenue Officer, and Pilvi Tunturi became Chief Customer Officer. Nina Laaksonen and Artturi Lehtiö are sharing the Chief Product Officer responsibilities as interim arrangement. On 1 January 2025, Ari Vanttinen left the company and the Global Leadership Team.

Shares, Shareholders' equity, Own shares

WithSecure has one share class. The total number of company shares is currently 176,098,739. The company's registered shareholders' equity is EUR 80,000. The company held 81,890 of its own shares at the end of the financial year.

The company holds its own shares to be used in the incentive compensation plans, for making acquisitions or implementing other arrangements related to the company's business, to improve the company's financial structure or to be otherwise assigned or cancelled.

In January–December, 32,248,332 (59,951,540) of WithSecure's shares were traded on the Helsinki Stock Exchange. The highest trading price was EUR 1.25 (1.74), and the lowest price was EUR 0.70 (0.74). The volume weighted average price of WithSecure's shares in 2024 was EUR 0.95 (1.28). The share's closing price on the last trading day of the year, 31 December 2024, was EUR 0.76 (1.04). Based on that closing price, the market value of the company's shares, excluding the treasury shares held by the company, was EUR 133.2 million (182.2 million).

The company currently has share-based incentive plans covering management and key personnel of the Group, as well as a share savings plan available to all employees. Information on the programs is provided in note [16 Share-based payment transactions](#) of the Financial Statements, as well as the [Remuneration Report](#).

Risks and uncertainties

WithSecure operations are subject to risks and uncertainties that can impact the business performance, profitability, financial position, market share, reputation, share price or the achievement of its short-term and long-term objectives. These risks and uncertainties described here should not be considered as an exhaustive list.

The objective of WithSecure risk management is to identify various risks that could have an impact on the business, and to implement appropriate measures to mitigate the risks. In assessing the risks, WithSecure considers both the probability and the potential impact of each risk, as well as the resources required to manage and mitigate the risk. Ensuring business continuity in all situations is an essential part of the risk management. WithSecure risk management principles and process are described in the [Corporate Governance Statement](#). The sustainability-related risks and uncertainties have been discussed in the [Sustainability Report](#). Financial risks are discussed in more detail in the note [18 Management of financial risks](#) to the Financial statements.

Risks related to cyber security market

Market consolidation and competition

The cyber security market is scattered to many providers of software and services. The large market participants are investing heavily in the development of embedded security and winning market share. Market consolidation is considered a likely development. WithSecure must succeed in its chosen strategy as well as in finding the right acquisition targets, and in integrating the acquired companies into its operations. As one of the smaller players in the market, the company must always keep itself relevant to the customers, by ensuring both up to date technology and good quality, timely services. Additionally, WithSecure must address brand recognition among the target audience to effectively differentiate itself from competition

Geopolitical risks

Geopolitical uncertainties, such as the war in Ukraine, have significantly increased the risk of unexpected disruptions of the world economy and security stability. Likelihood of acts of terror impacting societal infrastructures has increased with this development. Any such events could also impact WithSecure's ability to run its business. The increasing activity of nation-state cyber criminals will continue to impose business interruptions also during 2025.

For corporate responsibility reasons, WithSecure is not conducting business with any Russian or Belarussian parties, even in cases where it would be permitted by the export control regulations.

WithSecure operates in different countries and is therefore exposed to country risks of each location. Changing circumstances and regulation in different operating countries is exposing WithSecure to compliance risks, such as unfavorable tax treatment or export controls.

Environmental risks

As part of the sustainability materiality analysis, WithSecure has assessed the impact of the environmental risks, especially climate change, on its business. The company is a provider of software and services, and as such not significantly impacted by the environmental risks. Business continuity planning covers scenarios

related to unavailability of resources due to natural disasters or other hazards, including potential supply chain disruptions.

Risks related to WithSecure operations and products

Attracting and retaining talent

Unavailability of skilled personnel may result in inability of providing high-quality products and services to customers. Competition for skilled personnel is increasing and there is structural undersupply of talent in the cyber security industry. WithSecure is continuously developing and adopting new ways of recruitment, building its own talent and knowledge pools, and investing in training and development of personnel to attract and retain talent.

Partners

WithSecure's cyber security products and services market model is very dependent on a functioning partner channel and network. It is critical for WithSecure to ensure it has the right partners in the regions and that the partners receive the needed support, and that WithSecure's cyber security offering is made available accordingly to the local demand. Not being able to serve the needs of the partners needs could result to negative impact on WithSecure's business performance.

Product risks

WithSecure operates in a highly competitive market. Cybercrime is growing fast and becoming more innovative and professional. Large vendors make significant investments in their development and marketing activities, while new vendors are emerging in the market, and the operating system manufacturers are increasing their focus on built-in security features. WithSecure must succeed in maintaining in-depth understanding of cyber security threat landscape, following the hacker techniques and technologies, as well as continuing to innovate in defensive technologies.

Investments in new technologies and products come with the risk of not meeting the future requirements of the market. Agile methods are applied by WithSecure to ensure that its decisions regarding future technologies are aligned with the best information and expectations of the market developments.

Cyber security incidents

Exposure to cyber security incidents threatens the confidentiality, integrity, and availability of WithSecure products and services, and their mitigation is considered as high priority in all parts of the company. WithSecure builds cyber resilience by continuously improving its capability to identify, protect, detect, and respond to relevant threats. Continuous efforts are taken to protect sensitive data of the company and its customers.

Intellectual property rights (IPR)

WithSecure protects its technologies and innovations through copyrights, patents, trademarks, and technology partnerships. While WithSecure uses all available protection mechanisms, the businesses are exposed to risks relating intellectual property claims, particularly in the US markets.

Financial risks

Inflation and interest rates

Cost inflation in the countries where WithSecure operates increases the risk for negative development of the cost structure. This is monitored very closely, and inflation will also most likely require mitigation actions to retain workforce in the company. Increasing interest rates could limit the possibilities of external funding.

Liquidity risk

As a company still improving its profitability, WithSecure must focus on accurate cash planning and prompt collections to ensure liquidity of all group companies and to avoid needs of short-term financing.

Currency fluctuations

Increasing volume of operations outside the Euro zone in different currencies exposes WithSecure to an increased risk related to currency fluctuations. To mitigate the impact of currency fluctuations on future cash flows, the group can use forward contracts.

Annual General Meeting

The Annual General Meeting (AGM) of WithSecure Corporation was held on 20 March 2024. The meeting confirmed the financial statements for the financial year 2023 and reviewed the remuneration report for governing bodies. The members of the Board and the President and CEO were discharged from liability.

The meeting approved the proposal of the Board of Directors that no dividend will be paid for the financial year 2023 due to the loss-making net result of the year. The company will focus on funding its growth and developing the business.

The AGM decided that the annual remuneration of the Board of Directors will remain unchanged: EUR 80,000 for the Chair of the Board of Directors, EUR 48,000 for the Committee Chairs, EUR 38,000 for the members of the Board of Directors, and EUR 12,667 for the member of the Board of Directors employed by the Company. Approximately 40% of the compensation will be paid in company shares.

The AGM decided that the number of Board members shall be seven. The following current Board members were re-elected: Risto Siilasmaa, Tuomas Syrjänen, Kirsi Sormunen and Ciaran Martin. Amanda Bedborough, Niilo Fredrikson and Harri Ruusinen who belongs to the personnel of WithSecure Corporation, were elected as new members of the Board of Directors.

The Board elected Risto Siilasmaa as the Chair of the Board. Tuomas Syrjänen was nominated as the Chair of the Personnel Committee and Risto Siilasmaa and Niilo Fredrikson as members of the Personnel Committee. Kirsi Sormunen was nominated as the Chair of the Audit Committee and Ciaran Martin, Amanda Bedborough and Harri Ruusinen were nominated as members of the Audit Committee.

Audit firm PricewaterhouseCoopers Oy was re-elected as Auditor of the Company. Mr. Jukka Karinen, APA, acts as the responsible auditor.

The sustainability audit firm PricewaterhouseCoopers Oy was elected as the Company's sustainability auditor. Mr. Jukka Karinen, ASA, will act as the responsible sustainability auditor.

The AGM authorised the Board of Directors to resolve upon the repurchase of a maximum of 17,609,870 of the Company's own shares in total. The maximum amount equals to approximately 10% of all the shares in the Company, in one or

several tranches with the Company's unrestricted equity. The AGM authorised the Board of Directors to resolve on the issuance of a maximum of 17,609,870 shares in total through a share issue as well as by issuing options and other special rights entitling to shares pursuant to chapter 10, section 1 of the Companies Act in one or several tranches. The maximum number of shares corresponds to 10% of all shares in the Company. The authorisation concerns both the issuance of new shares and the transfer of treasury shares held by the Company.

Full disclosure of the AGM resolutions, as well as the organizing meeting of the Board of Directors held on the same day, has been provided in the Stock Exchange release of 20 March 2024.

Outlook for 2025

Annual Recurring Revenue (ARR) for Elements Cloud products and services will grow by 10-20% from the end of 2024.

At the end of 2024, Elements Cloud ARR was EUR 83.3 million.

Elements Company segment's Adjusted EBITDA will be 3-7% of revenue.

Annual Recurring Revenue (ARR) for Cloud Protection for Salesforce (CPSF) will grow by 20-35% from the end of 2024.

At the end of 2024, CPSF ARR was EUR 12.8 million.

Cyber security consulting business will be divested in 2025. Elements company and CPSF will have their own guidance going forward. Both are recurring, subscription-based businesses, which is reflected in the new guidance.

Medium-term financial target (for Elements Company segment)

Over the next three years (2025-2027), WithSecure will become a "Rule of 30+" company. The components of the target are

- Annual revenue growth as percentage
 - Adjusted EBITDA as percentage of revenue
- WithSecure is targeting to reach a sum of the components that exceeds 30.

Sustainability reporting

WithSecure has prepared its Sustainability report in accordance with the Corporate Sustainability Reporting Directive (CSRD) and the related Finnish legislation. Full [Sustainability report](#) is attached to this report of the Board of Directors.

Board of Directors' proposal for disposal of distributable funds

WithSecure's dividend policy is to pay approximately half of its profits as dividends. Subject to circumstances, the company may deviate from this policy. On 31 December 2024, WithSecure Corporation's distributable funds totaled EUR 77.5 million of which net result for the financial year was EUR -44.0 million. No material changes have taken place in the company's financial position after the balance sheet date. WithSecure's Board of Directors proposes that no dividend will be paid for 2024. The company will focus on funding its growth and developing the business. Net loss for the year is retained in the shareholders' equity.

Events after period-end

After the end of the financial year, on 23 January 2025, WithSecure announced the sale of its Cyber security consulting business to Swedish investment firm Neqst. The transaction is executed by the sale of shares of the parent company of a to-be-established WithSecure cyber security consulting group, to which the consulting business will be transferred prior to the completion of the transaction. As a result of the agreement, total of approximately 250 employees located in Finland, UK, Sweden, Denmark, Singapore, Italy, and US are expected to transfer to the buyer. Cyber security consulting is presented as Assets and liabilities held for sale in the financial reporting of 2024, and the financial result is classified as Discontinued operations.

Key figures

Economic indicators	IFRS	Restated IFRS	IFRS	IFRS	IFRS
	2024	2023	2022	2021	2020
Revenue (MEUR) ¹	116.0	109.9	134.7	130	220.2
Revenue growth %	5.5 %	-18.4 %	3.6 %		1.3 %
EBIT (MEUR) ²	-10.1	-35.7	-42.6	-30.1	19.7
% of revenue	-8.7 %	-32.5 %	-31.6 %	-23.1 %	8.9 %
Result before taxes ²	-10.3	-35.2	-44.2	-30.4	16.5
% of revenue	-8.9 %	-32.0 %	-32.8 %	-23.4 %	7.5 %
ROE (%)	-10.7 %	-32.9 %	-32.5 %	14.3 %	16.2 %
ROI (%)	-9.3 %	-30.5 %	-30.5 %	15.6 %	18.5 %
Equity ratio (%)	56.5 %	73.3 %	79.0 %	59.5 %	52.5 %
Investments (MEUR) ³	5.9	5.2	4.8	6.6	14.3
% of revenue	5.1 %	4.7 %	3.6 %	5.1 %	6.5 %
R&D costs (MEUR)	40.1	47.3	39.1	32.1	41.9
% of revenue	34.6 %	43.0 %	29.1 %	24.7 %	19.0 %
Capitalized development (MEUR)	1.7	3.0	2.4	5.6	5.5
Gearing %	-0.9 %	-22.2 %	-39.9 %	-25.8 %	-14.1 %
Wages and salaries (MEUR) ²	56.9	73.5	93.8	87.3	103.7
Personnel on average ¹	760	845	1438	1,678	1,691
Personnel on Dec 31 ¹	731	813	1295	1,656	1,678

¹ For years 2024-2023, the figures have been restated to reflect continuing operations only according to IFRS 5.

² For years 2024-2021, the figures have been restated to reflect continuing operations only according to IFRS 5.

³ From 2021 onwards, the figure is presented without investments to leased assets.

Key ratios	IFRS	Restated IFRS	IFRS	IFRS	IFRS
	2024	2023	2022	2021	2020
Earnings per share (EUR), combined operations	-0.22	-0.23	2.45	0.07	0.08
Earnings per share (EUR), continuing operations	-0.05	-0.18	-0.22	-0.15	
Earnings per share (EUR), discontinued operations	-0.16	-0.04	2.67	0.22	
Earnings per share (EUR), diluted, combined operations	-0.22	-0.23	2.45	0.07	0.08
Earnings per share (EUR), diluted, continuing operations	-0.05	-0.18	-0.22	-0.15	
Earnings per share (EUR), diluted, discontinued operations	-0.16	-0.04	2.67	0.22	
Shareholders' equity per share	0.39	0.59	0.80	0.6	0.52
Dividend per share ¹					0.04
Dividend per earnings (%)					50.0 %
Effective dividends (%)					1.0 %
P/E ratio	-14.5	-4.5	-6.2	62.0	47.1
Share price, lowest (EUR)	0.70	0.74	1.27	3.66	2.04
Share price, highest (EUR)	1.25	1.74	5.65	5.53	4.14
Share price, average (EUR)	0.95	1.28	2.75	4.39	3.10
Share price Dec 31	0.76	1.04	1.37	4.97	3.84
Market capitalization (MEUR)	133.2	182.2	239.6	786.4	606.7
Trading volume (millions)	32.2	60.0	67.1	20.2	22.8
Trading volume (%)	18.3 %	34.0 %	38.4 %	12.7 %	14.3 %
Adjusted number of shares, average during the period,	175,986,422	175,593,924	171,295,721	158,354,073	158,082,324
Adjusted number of shares, average during the period, diluted	175,986,422	175,593,924	171,295,721	158,354,073	158,082,324
Adjusted number of shares, Dec 31	176,098,739	176,098,739	174,598,739	158,798,739	158,798,739
Adjusted number of shares, Dec 31, diluted	176,098,739	176,098,739	174,598,739	158,798,739	158,798,739

¹ Board proposal

Calculation of key ratios

Calculation of key ratios		Calculation of key ratios	
Equity ratio, %	$\frac{\text{Total equity}}{\text{Total assets - deferred revenue}} \times 100$	Effective dividends, %	$\frac{\text{Dividend per share}}{\text{Closing price of the share, end of period}} \times 100$
ROI, %	$\frac{\text{Result before taxes + financial expenses}}{\text{Total assets - non-interest bearing liabilities (average)}} \times 100$	Operating Expenses	Sales and marketing, research and development, and administration costs
ROE, %	$\frac{\text{Result for the period}}{\text{Total equity (average)}} \times 100$	EBITDA	EBIT + depreciation, amortization and impairment
Gearing, %	$\frac{\text{Interest bearing liabilities - cash and cash equivalents and liquid financial assets}}{\text{Total equity}} \times 100$	Adjusted EBITDA	EBITDA +/- items affecting comparability
Earnings per share, euro	$\frac{\text{Profit attributable to equity holders of the company}}{\text{Weighted average number of outstanding shares}}$	Adjusted EBIT	EBIT +/- items affecting comparability
Shareholders' equity per share, euro	$\frac{\text{Equity attributable to equity holders of the company}}{\text{Number of outstanding shares at the end of period}}$	Annual Recurring Revenue (ARR)	Monthly Recurring Revenue of last month of the quarter x 12
P/E ratio	$\frac{\text{Closing price of the share, end of period}}{\text{Earnings per share}}$	Monthly Recurring Revenue (MRR)	Recognized revenue within the month excluding non-recurring revenues
Dividend per earnings, %	$\frac{\text{Dividend per share}}{\text{Earnings per share}} \times 100$	Net Revenue Retention (NRR)	100 % x (MRR of last month of the quarter/MRR of same month last year for the same customers). NRR includes expansion revenue, downgrades and customer churn.

Reconciliation of alternative performance measures

Alternative performance measures are presented for continuing operations only.

EUR 1,000	Restated	
	Consolidated 2024	Consolidated 2023
Adjusted EBITDA	2.0	-14.8
Adjustments to EBITDA		
Other items	-1.0	-1.4
Divestments	1.2	1.4
Restructuring	-1.1	-8.9
Costs under TSA		-6.9
Income for costs under TSA		6.9
EBITDA	1.1	-23.8
Depreciation, amortization and impairment losses	-11.2	-11.9
EBIT	-10.1	-35.7

EUR 1,000	Restated	
	Consolidated 2024	Consolidated 2023
Adjusted EBIT	-7.0	-24.3
Adjustments to EBIT		
Other items	-1.0	-1.4
Divestments	1.2	1.4
Restructuring	-1.1	-8.9
Costs under TSA		-6.9
Income for costs under TSA		6.9
PPA amortization	-2.2	-2.4
EBIT	-10.1	-35.7

Classification of adjusted costs in operating expenses

	Operating Expenses 2024	Restructuring	Other items	Expenses for adjusted EBIT	Depreciation	PPA amortization	Operating Expenses for Adjusted EBITDA 2024
Sales and marketing	-51.8			-51.8	3.9		-47.9
Research and development	-40.1			-40.1	5.1		-35.0
Administration	-14.1	1.1	1.0	-12.0	0.0	2.2	-9.7
Operating expenses	-105.9	1.1	1.0	-103.8	9.0	2.2	-92.6

	Restated Operating Expenses 2023	Costs under TSA	Restructuring	Other items	Expenses for adjusted EBIT	Depreciation	PPA amortization	Restated Operating Expenses for Adjusted EBITDA 2023
Sales and marketing	-61.3				-61.3	4.1		-57.2
Research and development	-47.3	5.6			-41.7	5.3		-36.4
Administration	-23.7	1.4	8.9	1.4	-12.0	0.1	2.4	-9.5
Operating expenses	-132.3	6.9	8.9	1.4	-115.0	9.5	2.4	-103.1

Classification of adjusted income in other operating income

	Other operating income 2024	Divestments	Other income for adjusted EBITDA 2024
Other operating income	3.2	-1.2	2.0

	Other operating income 2023	Income for costs under TSA	Divestments	Other income for adjusted EBITDA 2023
Other operating income	9.7	-6.9	-1.4	1.4

Shares and shareholders

Shares and share ownership distribution, Dec 31, 2024

Shares	Number of shareholders	% of shareholders	Total shares	% of shares
1-100	8,692	26.10%	404,903	0.23%
101-1 000	17,101	51.35%	6,786,959	3.85%
1001-50 000	7,376	22.15%	33,767,418	19.18%
50 001-100 000	68	0.20%	4,753,134	2.70%
100 001-	68	0.20%	130,386,325	74.04%
Total	33,305	100.00%	176,098,739	100.00%

Shareholders by category, 31 Dec 2024	Total shares	% of shares
Corporations	12,270,053	6.97%
Financial and insurance institutions	32,312,365	18.35%
General government	18,080,603	10.27%
Non-profit organizations	1,000,579	0.57%
Households	102,855,949	58.41%
Other countries and international organizations	534,341	0.30%
Nominee registered	9,044,849	5.14%
Total	176,098,739	100.00%

Largest shareholders and administrative register

Owner	Shares	% of shares	% of votes
Siilasmaa Risto	60,067,188	34.11%	34.13%
Nordea Nordic Small Cap Fund	11,407,976	6.48%	6.48%
Skandinaviska Enskilda Banken AB	7,544,620	4.28%	4.29%
Ilmarinen Mutual Pension Insurance Company	6,020,000	3.42%	3.42%
Mandatum Life Insurance Company Limited	5,069,434	2.88%	2.88%
Proprius partners micro finland (non-ucits)	4,300,000	2.44%	2.44%
Varma Mutual Pension Insurance Company	3,970,660	2.25%	2.26%
The State Pension Fund	3,900,000	2.21%	2.22%
Säästöpankki Pienyhtiöt	2,651,079	1.51%	1.51%
Elo Mutual Pension Insurance Company	2,557,275	1.45%	1.45%
Nordea Finnish Stars Fund	2,482,869	1.41%	1.41%
Administrative register			
Skandinaviska Enskilda Banken AB	7,544,620	4.28%	4.29%
Citibank Europe Plc	488,409	0.28%	0.28%
Other registers	1,011,820	0.57%	0.57%
Other shareholders			
	65,033,928	36.93%	36.95%
Total	176,016,849	99.95%	100.00%
Own shares WithSecure Corporation	81,890	0.05%	
Total	176,098,739	100.00%	

Ownership of management

Board of Directors	Shares	% of shares
Risto Siilasmaa	60,067,188	34.11%
Tuomas Syrjänen	59,112	0.03%
Kirsi Sormunen	33,427	0.02%
Harri Ruusinen	27,678	0.02%
Ciaran Martin	23,665	0.01%
Niilo Fredrikson	16,972	0.01%
Amanda Bedborough	13,834	0.01%
Total	60,241,876	34.21%
Executive team		
	Shares	% of shares
Antti Koskela	90,476	0.05%
Christine Bejerasco	90,517	0.05%
Tiina Sarhimaa	77,583	0.04%
Charlotte Guillou	61,267	0.03%
Tom Jansson	61,267	0.03%
Pilvi Tunturi	37,861	0.02%
Lasse Gerdt	0	0.00%
Total	418,971	0.24%

The Board of Directors and executive team owned a total of 60,660,847 shares on December 31, 2024. This represents 34.4 percent of the Company's shares and 34.5 percent of votes.

W/



Sustainability report

General information

BP-1 General basis for preparation of sustainability report

WithSecure reports in accordance with the EU Corporate Sustainability Reporting Directive (CSRD) (2022/2464), which guide the contents of this sustainability report. This report is referred to as WithSecure's Sustainability Report (also "report"), as determined according to the Finnish Accounting Act (1336/1997). The report is compiled with reference to the European Sustainability Reporting Standards (ESRS) issued by the European Financial Reporting Advisory Group (EFRAG). The report is prepared in accordance with the Finnish Accounting Act Chapter 7.

The report has been prepared on a consolidated basis, according to the same principles as the financial statements. The accounting policies applied for the sustainability report have been applied consistently in the financial year and for comparative figures, when those are presented.

Information pertaining to the material risks, impacts and opportunities takes WithSecure's upstream and downstream value chain into account. The disclosed data points and sustainability matters have been assessed according to the conducted Double Materiality Assessment (DMA). Please see the section on "[Business model and value chain](#)" for more details about WithSecure's value chain and the section "[SBM-3 Material sustainability-related impacts, risks and opportunities](#)" for more details about the methodology and outcome of the Double Materiality Assessment.

WithSecure has not used the option to omit a specific piece of information corresponding to intellectual property, know-how or the results of innovation.

WithSecure has chosen to use the transitional provision for presenting comparative information for the report's metrics and will thus not be presenting comparative information. The exception to this is the Greenhouse Gas (GHG) emission calculations, where comparative and base year figures will be presented.

Additionally, WithSecure will omit data points on work-related ill-health cases and days lost to injuries, accidents, fatalities, and work-related ill health for the first year of the sustainability report. The company will also omit information on anticipated financial effects for the first year of the sustainability statement.

BP-2 Disclosures in relation to specific circumstances

WithSecure announced the intention to sell of the company's Consulting business in January 2025. This divestment is reflected in the financial statements, which include the accounting treatment of the business as discontinued operations. However, this divestment does not significantly impact the information presented in the sustainability report, as there is no change in the identified material impacts, risks, and opportunities. The main business model of WithSecure remains unchanged. The metrics presented in the sustainability report reflect the situation at the end of 2024, with the divestment set to be realized in 2025. An exception to this is in the section "[S1-6 Characteristics of the undertaking's employees](#)", where all employee-related figures are presented separately for continued and discontinued operations. This distinction is made as these figures impact certain personnel-related KPIs included in the financial statements.

GHG emissions are presented and accounted for in full for the entire company, including the discontinued operations, as they occurred before the divestment, and would otherwise be partially unreported. The personnel-related metrics in sections S4 and G1, such as the employee training rate metrics, are relative to the total number of employees, so changes are not material as they reflect the status of 2024. Similarly, most of the S1 metrics are either relative to the total amount of employees or contain sensitive information, making it impractical to differentiate which entity those figures belong to without infringing on the privacy of WithSecure's continued and discontinued operations' employees.

The time horizons used for the impact and financial materiality assessments align with the time horizon definitions of the ESRS. Short term is within 1 year, medium term is 1-5 years, and long term is beyond 5 years.

Unless otherwise specified, none of the metrics presented in this report are subject to external assurance beyond the audit assurance provided for this report. The comparable figures are not within the scope of this audit assurance. In case a metric is subject to external assurance, it is clearly stated. The targets presented in this report are not science-based.

The information presented in this report is mainly based on internal data and estimations derived from such data. Assessments and estimates are used in the reporting of some data points, which are updated based on newer estimates and judgements when needed. Changes are recognized in the period when the estimate is updated. The use of assessments and estimates based on indirect sources, as well as the associated possible measurement uncertainty have been disclosed and described in connection to those datapoints specifically. In the case of this report, the use of such external information is limited to the Greenhouse Gas (GHG) emission calculations. Such instances where indirect sources are used are described in greater detail in the GHG emissions calculation methodology descriptions per each emission category. They are presented in the respective sections in the report section "[E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions](#)".

Disclosures stemming from other legislation or generally accepted sustainability reporting standards and frameworks include the analysis of business activities under the Taxonomy Regulation (2020/852) of the European Union.

In addition, WithSecure's carbon footprint is calculated for the third consecutive year. The GHG data points for scopes 1-3 are reported based on the Greenhouse Gas Protocol. WithSecure's results and plans on the company's strategy's sustainability program are presented in their own section of the report.

The results of the Taxonomy analysis and the GHG calculations are presented in the "[Environmental information](#)" section of this report, under "[EU Taxonomy](#)" and "[E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions](#)" respectively.

In terms of disclosures incorporated by reference to other parts of the Annual report, there is no referencing to other parts of the Annual report.

GOV-1 – GOV-5 Sustainability governance

This section of the sustainability report provides information about WithSecure’s sustainability governance. This includes descriptions of the governance processes, controls and procedures put in place to monitor, manage and oversee sustainability matters. The information covers the administrative, management and supervisory bodies of WithSecure. This section also outlines the general duties, composition, diversity and relevant experience of the members of these bodies.

WithSecure established governance principles for its sustainability program in 2022. In 2023, the Sustainability policy was approved as the basis of the company’s sustainability work. In 2024, WithSecure has actively worked to implement the objectives of the sustainability policy in the company’s operations.

An overview of the material ESRS topics and their assessment method for the identified material impacts, risks and opportunities are detailed under the section “[SBM-3 Material sustainability-related impacts, risks and opportunities](#)”. A detailed descriptions of these impacts, risks and opportunities per each ESRS topic can be found in the beginning of the respective ESRS topic sections in this report. The accompanying table showcases the material impacts, risks and opportunities addressed by the administrative, management and supervisory bodies, or their relevant committees during the year 2024.

A brief description of WithSecure's material impacts, risks and opportunities			
E1 Climate change	Climate change mitigation	Financial opportunity	Customers moving to cloud environments in search of modern, cost-effective, secure and sustainable solutions continues to present a major business opportunity for WithSecure.
S1 Own workforce	Working conditions	Financial opportunity	Improved employee retention can impact business positively through better sales and lower costs.
		Financial risk	Shortcomings in working conditions or employee wellbeing can increase costs through leaves of absence for physical or mental reasons. In the worst case, such shortcomings can lead to security risks that could cause reputational damage.
	Equal treatment and working opportunities for all	Financial opportunity	Promoting diversity, equity and inclusion (DEI) will increase WithSecure's ability to attract talent. In the long run there will also be cost savings for retaining talent at WithSecure.

A brief description of WithSecure's material impacts, risks and opportunities			
		Financial risk	Shortcomings in training and skills management can lead to losing out on business opportunities. Additional financial risks associated with this are related to attrition, brain leakage and disengagement of employees. Especially for a company in cyber security, it is of utmost importance to keep the employees' skills up to date. The industry faces continuous challenges regarding investment to technical solutions. Missing the mark can lead to financial losses.
S4 Consumers and end-users	Information related impacts for consumers and end-users	Positive impact	WithSecure's largest impact on sustainability comes from the work on building and supporting digital society, through its customers and end-users. WithSecure's value chain enables a well-working digital society, and therefore creates widespread positive impacts. Operating in the cyber security sector means being trusted with access to the customers' data. Maintaining a good level of data privacy of the customers is of utmost importance to WithSecure.
		Financial opportunity	WithSecure's core business revolves around cyber security. An opportunity for us is that we are able to meet the many needs of our end-users. For example, there are several opportunities for being a European-based company compared to the majority of the American competitors, with the European privacy related legislation and requirements. Our business model also enables the offering of holistic and flexible services. End-user feedback received directly or through channel partners is an important source of developing products.
		Financial risk	WithSecure faces risks from security and privacy perspective, as the company can be an attractive target for malicious activities. The potential repercussions for WithSecure could be significant, as WithSecure's entire existence is built on ensuring security for its end-users. Major security or privacy incident would cause reputational damage and loss of revenue. The likelihood of such risks materializing is limited.
		Financial risk	As a European company, the high requirements in European legislation for diligent consumer and end-user privacy practices incur additional investments.
G1 Business conduct	Corporate culture	Financial risk	Corporate culture is important as the related privacy risk is heightened compared to other industries as its potential impact on reputation is significant.
	Protection of whistle blowers	Positive impact	WithSecure has established a confidential and secure whistleblowing channel, enabling anonymous reporting of any concerns of misconduct. The channel is maintained by an impartial external party. In a multi-cultural working environment, involving thousands of end-customers, this is an essential element of good governance.
	Management of relationships with suppliers including payment practices	Positive impact	WithSecure wants to conduct its business to a high ethical standard. The aim is to maintain a positive impact on its supply chain through emphasis on ethical business practices. These impacts can be quite widespread, as they extend into the entire value chain and can therefore also impact the company's suppliers and partners.
		Financial risk	Maintaining strong supplier management processes and best practices requires investments, incurring possible additional costs.

GOV-1, GOV-2 The role of, information provided to and sustainability matters addressed by the administrative, management and supervisory bodies

Board of Directors and Board Committees

WithSecure’s administrative body is the **Board of Directors** (“the board”). The Board of Directors has seven members, of which six are non-executive. The one executive member is a member elected from WithSecure’s personnel.

The Board of Director’s **Audit Committee** is the supervisory body of WithSecure. The Audit Committee is neither a decision-making nor an executive body. The Board of Directors appoints from among itself the members and the Chair of the committee. The Audit Committee has four members, of which three are non-executive. The independence of the members is determined based on their independence of the company, not independence of major shareholders.

In terms of the Board of Directors’ roles and responsibilities, WithSecure’s Board of Directors is the highest administrative body in charge of sustainability matters in the company. As sustainability is incorporated into WithSecure’s business strategy in form of the sustainability program, sustainability matters are a scheduled agenda item in Board of Directors’ meetings annually. The Board of Directors approves the high-level priorities and objectives regarding sustainability. The Sustainability report is approved by the Board of Directors, as part of the approval of the Board of Directors report.

The Board of Directors is also involved in approving the identified sustainability-related impacts, risks and opportunities and determining that their mitigation and management has been adequately integrated into the company’s sustainability program. The Global Leadership Team (GLT) members set and accept the sustainability-related targets on an operational basis. The progress in targets is presented to the Board of Directors annually. The Board has the final authority to approve these targets when they review and approve the full annual report. By having the authority for the final approval of sustainability related targets, they are also inherently involved in setting these targets.

Similarly, the most senior level accountable for WithSecure’s material sustainability-related policies is the Board of Directors. The most senior level accountable for the implementation of these policies are the GLT members of each business unit most closely associated with the respective policy. They approve the updates to the policies. From there, the implementation of the policies is further delegated to individuals, teams or functions within WithSecure.

The Audit Committee oversees this progress by reviewing and monitoring the status of the company’s strategic sustainability related targets. As the Audit committee members are also members of the Board of Directors, they are also involved in setting the sustainability related targets. In addition to overseeing these targets and sustainability reporting, the Audit Committee also reviews policies and makes recommendations to the Board of Directors, who have the authority to approve these policies.

Board of Director’s gender diversity ratio (percentage of women)	29%
Board of Director’s independent board members ratio	86%

Audit Committee’s gender diversity ratio (percentage of women)	50%
Audit Committee’s independent board members ratio	75%

Risk management and internal control processes at WithSecure seek to ensure that risks related to business operations and the related sustainability matters of the company are properly identified, evaluated, monitored and reported in compliance with the applicable regulations. The risk assessments are updated on regular intervals to be in line with current information at the time of evaluation.

WithSecure’s Board of Directors defines the principles of risk management, internal controls and business conduct, which are followed within the company. The President and Chief Executive Officer (“CEO”) of WithSecure is accountable for ensuring that the risk management principles are implemented and applied constantly and consistently across the organization.

The Audit Committee assists the Board of Directors in the supervision of WithSecure’s risk management function. The Audit Committee’s roles and responsibilities include reviewing, instructing and evaluating risk management, internal supervision systems, IT strategy and practices, financial and sustainability reporting as well as auditing of the accounts and internal auditing.

The Board of Directors and the Audit Committee are kept informed of the relevant sustainability-related issues and they are expected to maintain relevant knowledge to manage and oversee sustainability-related matters. The Board members possess a mix of diverse backgrounds, expertise and experience, which strengthens the Board’s performance and promotes creation of long-term shareholder value. The sustainability-related expertise that they either directly possess or can leverage

is gained through access to both internal and external experts and training. This ensures that the members are well-equipped to handle these responsibilities. This sustainability related expertise includes but is not limited to for example the S4 sub-topic "Information related impacts for consumers and end-users".

The Board of Directors also regularly reviews sustainability-related matters, presented by both internal and external experts. These reviews enable the Board members to stay informed and maintain their competences. In the section "[GOV-4 Statement on due diligence](#)" it is described how WithSecure's governance structure engages in sustainability efforts, including how the administrative bodies are informed about the implementation of due diligence. This description also includes the monitoring of the results and the effectiveness of policies, actions, metrics, and targets adopted that address the identified material impacts, risks, and opportunities.

The Group's CEO and Global Leadership Team

WithSecure's management body is the CEO and the **Global Leadership Team (GLT)**. The GLT supports the CEO in the daily operative management of the company. The GLT has seven members, of which all are executive members from WithSecure's personnel.

Global Leadership Team's gender diversity ratio (percentage of women, including CEO)	57%
--	-----

The Global Leadership Team (GLT) is responsible for the implementation and supervision of the strategy, including sustainability program. WithSecure's Chief Financial Officer (CFO) oversees the sustainability coordination and ensures that the sustainability program is appropriately resourced and working on the right areas, supporting the program's priorities. Each program topic has a "home team" which executes the program as part of their other work. The GLT owner of each home team is responsible for achieving their area's sustainability objectives. Any sustainability-specific topics are the CFO's responsibility. The GLT members are considered as the most senior level accountable for the implementation and supervision of the sustainability-related policies and actions.

The GLT is represented in the sustainability team that engages in the day-to-day sustainability operations. Thus, the GLT members have an active role in determining and overseeing how the identified material impacts, risks and opportunities manifest in the company's ground-level operations. GLT members who are responsible for specific sustainability areas have taken part in the double materiality assessment. They also hold responsibility for following internal analysis of how the sustainability program is implemented and any possible implications of both external and internal sustainability matters.

In regard to experience related to WithSecure's identified impacts, risks and opportunities, the GLT members exhibit relevant skills and expertise. Several members hold prior working experience and knowledge gained through additional training on matters related to the identified material impacts, risks and opportunities. This enables them to also keep the Board of Directors informed of relevant matters.

GOV-3 Integration of sustainability-related performance in incentive schemes

Sustainability-related performance – including climate-related considerations – has not been integrated into WithSecure’s incentive schemes. The incentivising metrics and methods need to be adequately functioning and serve WithSecure’s business model and operational industry. WithSecure explores potentially suitable metrics and inclusion methods of sustainability-related matters into incentive schemes.

GOV-4 Statement on due diligence

WithSecure’s Board of Directors and the President and CEO are responsible for the company’s governance. WithSecure’s corporate governance practices are based on applicable Finnish laws, the rules of Helsinki Stock Exchange (NASDAQ Helsinki Oy) and the regulations and guidelines of Finnish Financial Supervisory Authority as well as the company’s Articles of Association.

WithSecure’s sustainability due diligence process ensures that the company identifies, prevents, mitigates and accounts for how WithSecure addresses the actual and potential negative impacts the company might have both in its own operations as well as within the value chain.

Due diligence has been embedded in the governance, strategy and business model of WithSecure. This is showcased through the level of information provided to and the sustainability matters addressed by the company’s administrative, management and supervisory bodies, as is described in greater detail under the section [“GOV-1, GOV-2 The role of, information provided to and sustainability matters addressed by the administrative, management and supervisory bodies”](#). The administrative, management and supervisory bodies have also participated in the double materiality analysis through which the material impacts, risks and opportunities were determined. This ensures that they are deeply engaged with the foundation for sustainable conduct at WithSecure.

Affected stakeholders are engaged with in all key steps of the due diligence process. Their views were integrated in the double materiality analysis to identify WithSecure’s material impacts, risks and opportunities ensuring that they have had the possibility to influence and guide the company’s conduct. The stakeholders’ perspectives are also continuously taken into account in periodic policy updates. They have the possibility of informing the company of their views through

various channels, including public-facing contacts like investor relations and the whistleblowing channel. Additionally, they can use direct internal contacts available to, for instance, the suppliers and partners in WithSecure’s value chain.

As part of the due diligence process, WithSecure has taken great care in identifying and assessing the impacts, risks and opportunities related to people and the environment through the double materiality analysis. The identified material impacts and their assessment processes have been detailed in the section [“IRO-1 Description of the process to identify and assess material impacts, risks and opportunities”](#) that is under the section [“SBM-3 Material sustainability-related impacts, risks and opportunities”](#).

To mitigate the risks and to emphasize the positive impacts and opportunities identified in the double materiality analysis, WithSecure engages in various courses of action per each material topic, sub-topic and sub-sub-topic. The effectiveness of these actions is tracked through a set of metrics and targets. These actions, metrics and targets are detailed separately for each topical standard section in this report.

WithSecure’s due diligence is an ongoing process that responds to changes both in the company’s operations as well as the surrounding environment and society. The company is planning on updating its double materiality analysis during the year 2025 to ensure that the most current information and stakeholder views are taken into account.

Core elements of Due Diligence	Paragraphs in the sustainability statement
Embedding due diligence in governance, strategy and business model	Section “GOV-1, GOV-2 The role of, information provided to and sustainability matters addressed by the administrative, management and supervisory bodies”
Engaging with affected stakeholders in all key steps of the due diligence	Section “SBM-2 Interests and views of stakeholders”
Identifying and assessing adverse impacts	Section “SBM-3 Material sustainability-related impacts, risks and opportunities”
Taking actions to address those adverse impacts	Topic-specific action descriptions
Tracking the effectiveness of these efforts and communicating	Topic-specific target descriptions and related performance statuses

GOV-5 Risk management and internal controls over sustainability reporting

Risk Management

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

WithSecure's Board of Directors defines the principles of risk management and internal controls which are followed within the company. The Audit Committee assists the Board of Directors in the supervision of WithSecure's risk management function. The CEO is accountable for ensuring that the risk management principles are implemented and applied constantly and consistently across the organization.

The primary goal of WithSecure's risk management principles is to empower the organization to identify and manage risks more effectively. The potential negative impact and probability of different situations arising from WithSecure's business operations on the company, its customers, or its partners are monitored as part of the risk management process. Another objective of the risk management is to constantly monitor and pro-actively control the impact and/or probability of situations derived from WithSecure's business operations which may have a negative impact on WithSecure, its customers, or its partners. Proactive monitoring, risk simulation and stress testing also allows building strategic resilience in the company and its business operations. Risk management may also be utilized to identify opportunities for benefit.

WithSecure promotes continuous risk evaluation by the company's personnel. The relevant operational risks identified through the risk management process are regularly reviewed by the CEO and Global Leadership Team. Risk Management is an integrated part of WithSecure's governance and management, and the risk management process is aligned with the ISO-31000 standard. The Audit Committee regularly conducts a review of top operational risks and evaluates the effectiveness of the risk management system.

Internal Control

Internal Control, supported by Risk Management, is an important element of WithSecure's management system. The Board of Directors is responsible for ensuring that the operating principles for internal control have been defined, and that the company monitors the functioning of internal control.

WithSecure has defined its objectives for internal control based on the globally applied principles. Internal control consists of e.g. policies, processes, procedures as well as control and monitoring activities. Internal Control is designed to provide a high level of assurance regarding the achievement of WithSecure's objectives in following categories:

- Effectiveness, efficiency and transparency of operations on all levels in accordance with the WithSecure strategy
- Reporting, including financial and non-financial, external and internal, to the Board, management, shareholders and stakeholders being complete, reliable, relevant and timely
- Compliance with applicable laws, regulations and WithSecure policies and instructions

WithSecure's Internal Control Operating Principles define the roles, design and practices of internal control. The principles provide guidance on how internal control is implemented at different levels, systems and amongst employees and outsourced functions. Internal control over financial reporting consists of risk identification and assessment, processes and internal control points and internal control monitoring and reporting.

Sustainability Reporting

In WithSecure's sustainability reporting, the role of internal control is important to ensure transparency and accountability. The internal control catalogue and Internal Control Operating Principles include dedicated sections to ensure that WithSecure's sustainability reporting is conducted timely and accurately, following the relevant regulations. Sustainability-related matters are regularly addressed by the administrative, management and supervisory bodies.

SBM-1 Strategy, business model and value chain

As part of WithSecure's strategy, WithSecure has implemented a sustainability program, to ensure that sustainability issues are addressed in the company's strategy. The leading guideline of WithSecure's sustainability program is Maximizing Net Impact – on the planet, people and society. The objective of the program is to ensure that sustainability is embedded in all the company's decisions. WithSecure also wants to ensure transparency of the company's activities to the users of its reporting.

WithSecure offers cyber security products and services for business customers globally. The company's role of protecting the digital society and preventing damages and losses caused by cybercrime is its most important contribution to a more sustainable world. With this role, WithSecure's activities will always generate a positive impact on society. By preventing cyberattacks, WithSecure helps businesses to avoid financial losses and data breaches, which supports economic stability and trust in digital society. A well-functioning digital society is a major enabler of sustainability. Through its efforts, WithSecure helps create a secure digital society, reducing the need for materials and transportation. This supports a more sustainable world. As businesses become more data-driven and vulnerable to attacks, WithSecure's work in protecting them remains its most important contribution to sustainability.

However, WithSecure's aims to go further. The company strives to ensure its activities positively impact the planet, people and society. WithSecure wants to share the accumulated knowledge and support parties who cannot always defend themselves.

In terms of environmental impact, WithSecure's carbon footprint is not high, as is described in more detail in the section "[E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions](#)". Nevertheless, WithSecure recognizes that the company must do its part in minimizing the environmental impacts of company's products as well as its own activities.

People are also at the heart of WithSecure's sustainability endeavours. WithSecure employs highly skilled experts around the world and want to support their wellbeing and growth opportunities. The company's aim is to reach the sustainability goals with the support of the 961 employees divided between the 15 offices globally. The headcount of employees by geographical areas is described in the section "[S1-6 Characteristics of the undertaking's employees](#)". The major office locations are Helsinki (Finland), London (UK), Kuala Lumpur (Malaysia) and Poznan (Poland). The rest of the global offices are scattered across Europe, North America, Japan, and Asia Pacific. All offices respond to the requests of WithSecure's international partners, customers and other stakeholders.

WithSecure does not operate in the fossil fuel sector or with chemical production, controversial weapons, and cultivation and production of tobacco.

WithSecure's internal operations must always follow high ethical standards. None of WithSecure's products and services are banned in certain markets. For corporate responsibility reasons, WithSecure has however chosen to not conduct business with any Russian or Belarussian parties, even in cases where it would be permitted by the export control regulations.

WithSecure's sustainability related goals are followed on group level, which aligns with the financial reporting being followed based on one segment. Due to the nature of the business, revenue is reviewed at group level. There are no separate sustainability goals per individual product or service group, customer category, geographical area or stakeholder relationship.

Business model and value chain

WithSecure's business model is based on providing cyber security software and services to its customers. The company's clientele consists of other companies, mainly sales partners and their customers who then make up the end-user base of WithSecure's services.

Defining WithSecure's value chain ensured that the materiality assessment considered sustainability topics, sub-topics and sub-sub-topics broadly and throughout the value chain. All the ESRs Standard topics have been screened throughout WithSecure's value chain.

WithSecure's upstream value chain consists of equipment and materials manufacturing, where for example hardware and data transmission networks for WithSecure's suppliers is processed. The value chain continues to WithSecure's suppliers who provide WithSecure with software and cloud services, equipment and third-party services, such as marketing. Moving downstream from WithSecure's own operations, which consist of digital product design and cyber security solutions, are WithSecure's sales partners. Lastly in the downstream value chain are WithSecure's customers companies and end users, including WithSecure's customer companies and their employees.



SBM-2 Interests and views of stakeholders

WithSecure has identified six different groups of stakeholders. Three stakeholder groups – namely the employees, the partners, and the investors and financial analysts – have participated in the company’s double materiality analysis directly. This ensures that their views have been integrated in WithSecure’s material impacts, risks and opportunities related to the scope of the standard topics ESRS S1 “Own workforce” and ESRS S4 “Consumers and end-users”.

Other stakeholders’ views were gathered through different means, such as surveys and interviews. As a part of the information gathering, the stakeholder groups’ expectations for WithSecure were determined, the engagement and their possibilities of communicating with WithSecure were evaluated, and the expected outcomes as well as activities were also identified.

WithSecure’s stakeholder inclusion in the double materiality analysis process highlights the company’s commitment to actively listen to and engage with its stakeholders. To enable the understanding of the stakeholders’ expectations and concerns, an ongoing engagement is maintained. The continuous dialogue

facilitates the communication of WithSecure’s sustainability efforts and processes. This enables WithSecure to align its sustainability-related efforts with the interests and views of the company’s stakeholders.

The administrative, management and supervisory bodies of WithSecure are informed about the views and interests of affected stakeholders regarding WithSecure’s sustainability-related impacts. Most recently, the views and interests of affected stakeholders were thoroughly determined as part of the double materiality analysis. The comprehensive stakeholder interviews that were held ensured that the views and interests of the stakeholders were acknowledged. Through the identification of the material impacts, risks and opportunities, these views have been integrated into the WithSecure’s sustainability program.

The table below exemplifies WithSecure’s different stakeholder groups and their sustainability-related expectations for WithSecure. The table also outlines different engagement methods and examples of sustainability related expected outcomes and activities that WithSecure undertakes.

WithSecure stakeholder	Expectations for WithSecure	Engagement	Examples of expected outcomes and activities
Employees	<ul style="list-style-type: none"> Fair compensation Secure working environment Equity, diversity of workplace Professional development Work/life balance support 	<ul style="list-style-type: none"> Townhalls, other regular and ad hoc communications Continuous development – training opportunities, Personal Development Plan maintenance Employee surveys Employee rep Board member 	<ul style="list-style-type: none"> Increasing awareness on WIDE topics and Code of conduct Sharing knowledge of sustainability Enhancing PDP process and follow-up Equal pay (or similar) assessments
Partners / Direct customers	<ul style="list-style-type: none"> Reliable products, easy interface Fair compensation model Seamless collaboration and business support Up-to-date knowledge of cyber security world 	<ul style="list-style-type: none"> Partner Advisory Board Partner programs Regular engagement via sales teams Support in technical matters, training Assistance in ESG queries, answering 3rd party platform questions (EcoVadis, CDP) 	<ul style="list-style-type: none"> Up to date sustainability website Ability to provide CO2 footprint/eur to customers Increasing energy efficiency of products
End-customers	<ul style="list-style-type: none"> Reliable products Support in case of emergencies 	<ul style="list-style-type: none"> Feedback received and improvements to products 	<ul style="list-style-type: none"> Sharing knowledge on cyber security Up to date Incident Response services for smaller customers

WithSecure stakeholder	Expectations for WithSecure	Engagement	Examples of expected outcomes and activities
Investors and financial analysts	Consistent growth Predictability of results Transparency of communication Good governance	Regular meetings, attending group meetings and presentations Capital Market Days ESG ratings of 3rd parties	Up to date sustainability website Improvement of ESG ratings
Suppliers	Fair compensation for products/services Favourable terms & conditions Good business ethics	Supplier onboarding and verifications if necessary Cyber security scanning of IT related vendors	Develop a lean way of managing supply chain sustainability
Regulators	Compliance with regulations Transparent sustainability reporting	Participation in key legislation preparations regarding cyber security as an advisory body Following up regulation to ensure compliance	Alignment of activities on sustainability with regulation

SBM-3 Material sustainability-related impacts, risks and opportunities

As a step towards preparing for the CSRD reporting and to identify WithSecure’s material sustainability-related impacts, risks and opportunities, the company conducted a double materiality assessment (DMA) during the year 2023. The assessment was conducted against the EFRAG ESRS (European Sustainability Reporting Standards). This assessment and the related DMA assumptions have been updated during the year 2024 to reflect new insights, stakeholder feedback, and changes in the regulatory environment. An analysis of the short-term financial effects for the material ESRS topics was conducted during the year 2024, and no material impacts were identified. By regularly updating the DMA, WithSecure can better manage sustainability-related impacts, risks and opportunities, enhancing its overall sustainability performance.

The DMA includes topics where WithSecure could have a material impact (inside-out approach) and those posing financial risks or opportunities (outside-in approach). Following CSRD requirements, only material topics are included in the sustainability report. Both internal and external stakeholders participated in the assessment to identify material sustainability topics across the value chain. The effects have been quantified where applicable and supplemented with qualitative assessments where appropriate. The scope of the analysis covers all of WithSecure’s workforce. WithSecure is committed to upholding human rights and strictly prohibits the use of child labour, forced labour, or any other human rights violations, including human trafficking.

The following chapter details an overview of the DMA analysis outcome and WithSecure’s methodologies. Detailed descriptions of these impacts, risks and opportunities per each ESRS topic can be found in the beginning of the respective ESRS topic sections in this report.

WithSecure believes that the DMA presented fairly reflects the impacts, risks and opportunities WithSecure faces. As outlined in the “[GOV-1 – GOV-5 Sustainability governance](#)” section, risk management and internal control processes at WithSecure seek to ensure that risks related to the sustainability-related matters and business operations of the company are properly identified, evaluated, monitored and reported in compliance with the applicable regulations. The risk assessments are updated on regular intervals to be in line with current information at the time of evaluation. This also applies for WithSecure’s DMA assessment, which will be further developed to align with best practices and the global situation.

Through the DMA, WithSecure identified its material sustainability-related impacts, risks, and opportunities. Stakeholder views and interests were integrated into this assessment and the outcomes. The administrative and supervisory bodies oversee and determine that the operational strategy includes appropriate measures for the sustainability program. The sustainability team and specific GLT members are responsible for aligning daily operations with the sustainability program as well as managing and mitigating the identified impacts, risks, and opportunities.

Summary of WithSecure double-materiality assessment	Main impacts, risks and opportunities	Financial impact	Likelihood	Impact materiality			Impacts on
<i>ESRS standard</i>			<i>20% = Not very likely 80% = Very likely</i>	<i>Scope</i>	<i>Scale</i>	<i>Remediability</i>	
E1 Climate change	Impact possibilities on climate change are very limited for a software and services company. Customers moving to cloud environments presents a major business opportunity for WithSecure. The company's products have a material impact on protecting the digital society and enabling sustainable activities of the end-customers. In addition, managing and reporting carbon footprint of own operations will become a necessity and create some reputational benefits.	Medium-term	75-100%	Concentrated to widespread	Minimal to low	Difficult	Own operations, upstream and downstream value chains
E2 Pollution	<i>Due to nature of the business, no material IROs were identified. Impact possibilities are very limited for a software and services company.</i>						
E3 Water and marine resources	<i>Due to nature of the business, no material IROs were identified. Impact possibilities are very limited for a software and services company.</i>						
E4 Biodiversity and ecosystems	<i>Due to nature of the business, no material IROs were identified. Impact possibilities are very limited for a software and services company.</i>						
E5 Circular economy	<i>Due to nature of the business, no material IROs were identified. Impact possibilities are very limited for a software and services company.</i>						
S1 Own workforce	Employees are key to the company success. Maintaining a diverse, equal, competent and adaptable workforce is a very significant topic for WithSecure.	Short-, medium- and long-term	50-100%	Limited to concentrated	Minimal to high	Remediable	Own operations
S2 Workers in the value chain	<i>Due to nature of the business, no material IROs were identified. Impact possibilities are very limited for a software and services company.</i>						
S3 Affected communities	<i>Due to nature of the business, no material IROs were identified. Impact possibilities are very limited for a software and services company.</i>						
S4 Consumers and end-users	WithSecure has large impacts on protecting the digital society and enabling sustainable activities of its end-customers. Data privacy and data security are very significant matters for a cyber security company. Equally, risks related to these areas are of existential nature.	Short-, medium- and long-term	75-100%	Very widespread	Absolute	Very difficult	Downstream value chain
G1 Business conduct	Good governance and business ethics are a fundamentally important requirements for a company operating in "trust business".	Short- and medium-term	75-100%	Concentrated to widespread	Low to high	Difficult to very difficult	Own operations, upstream and downstream value chains

IRO-1 Description of the process to identify and assess material impacts, risks and opportunities

Background

The Double Materiality Assessment has been carried out as an iterative process with the support of third-party advisors. The initial materiality assessment was conducted in 2022. It was expanded into a double-materiality analysis in 2023 which again was complemented in 2024, to align with the updates of the regulation.

The Double Materiality Assessment topics were selected on the basis of European Sustainability Reporting Standards (ESRS), valid drafts and published standards at the time of each assessment round.

First the value chain perspective was considered. The time horizons were defined and WithSecure's upstream and downstream value chains were assessed. Stakeholders – including silent stakeholders – were engaged in this value chain assessment. Defining WithSecure's value chain ensures that the materiality assessment considered sustainability topics broadly and throughout the value chain. WithSecure's own operations were also included as part of the value chain assessment.

After scoping the value chain, the ESRS topics were evaluated holistically to assess possible material themes based on the scope of the value chain and own operation's assessments. Additionally relevant legal and regulatory landscape was considered.

The assessments, analyses and material have been screened against the CSRD requirements and the European Sustainability Reporting Standards (ESRS) to ensure all relevant topics and perspectives are considered. For the double materiality assessment, the ESRS topics were considered on a topic, sub-topic and sub-sub-topic levels where applicable.

Parameters used and scope of analysis

The same assessment methodology and assumptions were used for assessing all the ESRS topics, possible impacts, risks, and opportunities as well as their materiality, as detailed in this section. As part of double materiality assessment process, the board gathered to discuss these topics and possible material implications and features, ensuring diverse perspectives and strategic decisions that integrate sustainability into the company's governance and reinforce WithSecure's commitment to responsible business practices. As described in section "[SBM-2 Interests and views of stakeholders](#)", other stakeholders were included in the assessment process as well.

The process of assessing the materiality of the risks and opportunities is multifaceted. The pre-determined *time horizon* defines the timeframe in which the identified risk or opportunity will occur. The *likelihood* of the financial risks or opportunities is assessed. The scale goes from 25% indicating that the event is more likely not to happen, to 50% indicating there is a 50/50 chance, further on to 75% indicating that it is more likely to happen than not, with the scale ending at 100% which indicates an actual risk or opportunity. The value of the likelihood was freely determinable within this scale. The third determinant is the *magnitude* of the risk or opportunity. This is based on the magnitude of the impact it can potentially have on related revenue, related costs and group EBITDA.

The process for impact materiality assessment goes even more in depth. For impact materiality, the assessment uses 3 dimensions – *scale, scope and irremediability* – in addition to time horizon and likelihood. In addition to these, the part of the value chain where the impact is expected to materialize is indicated.

Scale determines how significant the positive or negative impact of WithSecure is on the topic. For example, in regard to work conditions, when the magnitude of the impact is small, there might be momentary stressful work and short sick leaves. High magnitude could mean long sick leaves and severe health hazards or work accidents.

Scope shows how widespread the company's impact is. When low, the impacts are limited in scope and emerge only in a few parts of the value chain, in only few divisions and locations, or affect only few stakeholders. Vice versa, for high scope the impacts emerge across the entire value chain, in all divisions or affect all

stakeholders. An example could be pollution limited to geographically a very limited area or manifesting as several polluted areas.

Irremediability indicates to what extent the negative impacts can be remedied and restored relatively easily or in short-term to their original state, or whether the impact is non-remediable resulting in fatal accidents or environmental disasters.

The process for identifying climate-related hazards at WithSecure considers one general high-emission across its own operations, upstream, and downstream value chain. Separate scenarios for low, medium and high emission scenarios were not utilized. This assessment covers short-term and medium-term horizons, evaluating the likelihood of these events among other aspects as mentioned above. WithSecure has also assessed the extent to which its assets and business operations are exposed and sensitive to transition events, ensuring awareness of potential risks. No material climate-related hazards or risks were identified.

The single high-emission scenario used provides a suitable base for the assessment of potential impacts. This approach ensures the incorporation of climate risks and opportunities, aligning with WithSecure's overall risk management strategy. The sustainability report is prepared on a consolidated basis, following the same principles as the financial statements, as stated in section "[BP-1 General basis for preparation of sustainability report](#)".

Due to the nature of WithSecure's business, the industry it operates in as well as the locations of its offices as a cybersecurity company, its business activities have been assessed to have a limited impact on pollution, water and marine resources, biodiversity and ecosystems, and circular economy. Consequently, WithSecure has not held consultations with affected communities of the company's possible material environmental impacts, as there are none. WithSecure has also conducted a screening of its locations, which are all rented offices in established big cities, and found they are not near biodiversity-sensitive areas. Similarly, due to no material negative impacts or risks being identified for any of the environmental topics, a further analysis of systemic risk impacts on WithSecure's operations or value chain was not conducted.

Outcome

WithSecure's double materiality assessment consists of impact materiality and financial materiality. Through the impact materiality assessment, WithSecure's impacts on the environment and society have been identified. The financial materiality assessment covers the sustainability-related risks and opportunities WithSecure is exposed to.

The material impacts, risks and opportunities for WithSecure fall under the following four ESRS topics; E1 Climate change, S1 Own workforce, S4 Consumers and end-users and G1 Business conduct. Seven different ESRS sub-topics were identified in WithSecure's materiality assessment process. These sub-topics are Climate change mitigation (E1), Working conditions (S1), Equal treatment and working opportunities for all (S1), Information-related impacts for consumers and/or end-users (S4), Corporate culture (G1), Protection of whistleblowers (G1) and Management of relationships with suppliers including payment practices (G1).

Climate change (E1) mitigation is important for WithSecure. The company optimizes energy use in its products, benefiting its value chain and supporting digital climate solutions. WithSecure's low-emission business model limits its climate impact, with most emissions being upstream scope 3. WithSecure's operations also have limited negative climate-related impacts and financial risks, and as such they have not been identified as material. An identified material opportunity is the continuous shift to cloud-based IT environments, which aligns with WithSecure's sustainability goals and supports digital climate solutions.

Business conduct (G1) is also assessed as material for WithSecure. WithSecure promotes ethical practices. The company focuses on corporate culture, whistleblower protection, and ethical supplier management, positively affecting its value chain. No significant financial opportunities were identified. Short-term risks include corporate culture and privacy issues, while medium-term risks involve the costs of maintaining ethical supplier practices.

More information about these and the other identified material sustainability-related impacts, risks and opportunities per each identified sustainability topic, sub-topic and sub-sub-topic have been presented under their respective sections.

Other non-material environmental impacts from WithSecure's upstream value chain and circular economy

WithSecure has assessed various environmental impacts within its upstream value chain and circular economy. The ESRS topics of "E2 Pollution", "E3 Water and Marine Resources", "E4 Biodiversity and Ecosystems", and "E5 Circular Economy" have not been identified as material topics for the company. The assessment methodology and assumptions made for assessing all of the ESRS topics, possible impacts, risks, and opportunities, and their materiality are detailed before this section under "Parameters used and scope of analysis".

Other environmental impacts, including pollution (E2), water and marine resources (E3), and biodiversity and ecosystems (E4), have been evaluated. These impacts are considered to be of low significance, narrow in scope, and have a low likelihood of occurrence for WithSecure's operations. Even though these possible impacts are not easily remediable, WithSecure can have indirect positive effects for the environment by ensuring its products are efficiently made. This in turn reduces the need for new devices. However, these positive impacts are quite small and limited, rendering the other ESRS environmental impact topics immaterial to WithSecure.

Similarly, the ESRS topic of circular economy (E5), encompassing WithSecure's sustainable value chain, recycling, and waste management, has not been identified as a material topic. The environmental impacts related to the circular economy are also considered to be of low significance, narrow in scope, and have a low likelihood of occurrence. WithSecure can have a small impact on the circular economy and resource efficiency by ensuring its products are efficiently built, improving the lifetime of users' devices, and minimizing the use of data centers. However, this impact is limited due to the company's size and product scope. Negative impacts on resource efficiency can occur if WithSecure's products require more resources and energy, and waste from operations can negatively impact the circular economy unless managed well. These negative impacts can be mitigated through proper product planning and recycling measures, thus mitigating the impacts.

IRO-2 Disclosure requirements in ESRS covered by the undertaking’s sustainability report

Content index list of the material Disclosure Requirements

The tables below describe all the ESRS disclosure requirements in ESRS 2 and the identified material topics E1, S1, S4 and G1 that have set the framework for the preparation of the sustainability report.

Cross-cutting standards – ESRS 2 “General disclosures”			
Standard section	Disclosure requirement	Section/report	Additional information
BP-1	General basis for preparation of the sustainability report	BP-1 General basis for preparation of sustainability report	
BP-2	Disclosures in relation to specific circumstances	BP-2 Disclosures in relation to specific circumstances	
GOV-1	The role of the administrative, management and supervisory bodies	GOV-1, GOV-2 The role of, information provided to and sustainability matters addressed by the administrative, management and supervisory bodies	
GOV-2	Information provided to and sustainability matters addressed by the undertaking’s administrative, management and supervisory bodies	GOV-1, GOV-2 The role of, information provided to and sustainability matters addressed by the administrative, management and supervisory bodies	
GOV-3	Integration of sustainability-related performance in incentive schemes	GOV-3 Integration of sustainability-related performance in incentive schemes	
GOV-4	Statement on sustainability due diligence	GOV-4 Statement on due diligence	
GOV-5	Risk management and internal controls over sustainability reporting	GOV-5 Risk management and internal controls over sustainability reporting	
SBM-1	Strategy, business model and value chain	SBM-1 Strategy, business model and value chain	See also Business model and value chain
SBM-2	Interests and views of stakeholders	SBM-2 Interests and views of stakeholders	

Cross-cutting standards – ESRS 2 “General disclosures”			
Standard section	Disclosure requirement	Section/report	Additional information
SBM-3	Material impacts, risks and opportunities and their interaction with strategy and business model	SBM-3 Material sustainability-related impacts, risks and opportunities	Also detailed per each ESRS topic in respective sections.
IRO-1	Description of the process to identify and assess material impacts, risks and opportunities	IRO-1 Description of the process to identify and assess material impacts, risks and opportunities	
IRO-2	Disclosure requirements in ESRS covered by the undertaking’s sustainability statement	IRO-2 Disclosure requirements in ESRS covered by the undertaking’s sustainability report	Detailed per each ESRS topic.

Environmental standards – ESRS E1 “Climate change”			
Standard section	Disclosure requirement	Section/report	Additional information
ESRS 2, GOV-3	Integration of sustainability-related performance in incentive schemes	GOV-3 Integration of sustainability-related performance in incentive schemes	
E1-1	Transition plan for climate change mitigation	E1-1 Transition plan for climate change mitigation	
ESRS 2, SBM-3	Material impacts, risks and opportunities, and their interaction with strategy and business model	SBM-3 Material impacts, risks and opportunities related to climate change	

Environmental standards – ESRS E1 “Climate change”			
Standard section	Disclosure requirement	Section/report	Additional information
ESRS 2, IRO-1	Description of the processes to identify and assess material climate related impacts, risks and opportunities	SBM-3 Material impacts, risks and opportunities related to climate change	See also IRO-1 Description of the process to identify and assess material impacts, risks and opportunities
E1-2	Policies related to climate change mitigation and adaptation	E1-2 Policies related to climate change mitigation and adaptation	
E1-3	Actions and resources in relation to climate change policies	E1-3 Actions and resources in relation to climate change policies	
E1-4	Targets related to climate change mitigation and adaptation	E1-4 Targets related to climate change mitigation and adaptation	
E1-5	Energy consumption and mix		Not material
E1-6	Gross Scopes 1, 2, 3 and total GHG emissions	E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions	
E1-7	GHG removals and GHG mitigation projects financed through carbon credits		Not material
E1-8	Internal carbon pricing		Not material
E1-9	Anticipated financial effects from material physical and transition risks and potential climate-related opportunities		Phase-in used

Social standards – ESRS S1 “Own workforce”			
Standard section	Disclosure requirement	Section/report	Additional information
ESRS 2, SBM-2	Interests and views of stakeholders	S1-3 Processes to remediate negative impacts and channels for own workforce to raise concerns	
ESRS 2, SBM-3	Material impacts, risks and opportunities and their interaction with strategy and business model	SBM-3 Material impacts, risks and opportunities related to own workforce	
S1-1	Policies related to own workforce	S1-1 Policies related to own workforce	
S1-2	Processes for engaging with own workers and workers’ representatives about impacts	S1-2 Processes for engaging with own workforce and workers’ representatives about impacts	
S1-3	Processes to remediate negative impacts and channels for own workers to raise concerns	S1-3 Processes to remediate negative impacts and channels for own workforce to raise concerns	
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	S1-4 Taking action on material impacts on own workforce, and approaches to managing material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions	
S1-5	Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	S1-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	
S1-6	Characteristics of the undertaking’s employees	S1-6 Characteristics of the undertaking’s employees	
S1-7	Characteristics of non-employee workers in the undertaking’s own workforce	S1-7 Characteristics of non-employees in the undertaking’s own workforce	
S1-8	Collective bargaining coverage and social dialogue	S1-8 Collective bargaining coverage and social dialogue	
S1-9	Diversity metrics	S1-9 Diversity metrics	
S1-10	Adequate wages	S1-10 Adequate wages	

Social standards – ESRS S1 “Own workforce”			
Standard section	Disclosure requirement	Section/report	Additional information
S1-11	Social protection	S1-11 Social protection	
S1-12	Persons with disabilities	S1-12 Persons with disabilities	
S1-13	Training and skills development metrics	S1-13 Training and skills development metrics	
S1-14	Health and safety metrics	S1-14 Health and safety metrics	
S1-15	Work-life balance metrics	S1-15 Work-life balance metrics	
S1-16	Compensation metrics (pay gap and total compensation)	S1-16 Compensation metrics (pay gap and total compensation)	
S1-17	Incidents, complaints and severe human rights impacts	S1-17 Incidents, complaints and severe human rights impacts	

Social standards – ESRS S4 “Consumers and end-users”			
Standard section	Disclosure requirement	Section/report	Additional information
ESRS 2, SBM-2	Interests and views of stakeholders	S4-1 Policies related to consumers and end-users	
ESRS 2, SBM-3	Material impacts, risks and opportunities and their interaction with strategy and business model	SBM-3 Material impacts, risks and opportunities related to consumers and end-users	
S4-1	Policies related to 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	S4-2 Processes for engaging with consumers and end-users about impacts	
S4-3	Processes to remediate negative impacts and channels for consumers and end-users to raise concerns	S4-3 Processes to remediate negative impacts and channels for consumers and end-users to raise concerns	
S4-4	Taking action on material impacts on consumers and end-users, and approaches to managing material risks and pursuing material opportunities related to consumers and end-users, and effectiveness of those actions	S4-4 Taking action on material impacts on consumers and end-users, and approaches to managing material risks and pursuing material opportunities related to consumers and end-users, and effectiveness of those actions	

Social standards – ESRS S4 “Consumers and end-users”			
Standard section	Disclosure requirement	Section/report	Additional information
S4-5	Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	S4-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	

Governance standards – ESRS G1 “Business conduct”			
Standard section	Disclosure requirement	Section/report	Additional information
ESRS 2, GOV-1	The role of the administrative, supervisory and management bodies	GOV-1, GOV-2 The role of, information provided to and sustainability matters addressed by the administrative, management and supervisory bodies	
ESRS 2, IRO-1	Description of the processes to identify and assess material impacts, risks and opportunities	SBM-3 Material impacts, risks and opportunities related to business conduct	
G1-1	Business conduct policies and corporate culture	G1-1 Business conduct policies and corporate culture	
G1-2	Management of relationships with suppliers	G1-2 Management of relationships with suppliers	
G1-3	Prevention and detection of corruption and bribery		Not material
G1-4	Incidents of corruption or bribery		Not material
G1-5	Political influence and lobbying activities		Not material
G1-6	Payment practices	G1-6 Payment practices	

List of datapoints in cross-cutting and topical standards that derive from other EU legislation

The table below describes all the datapoints that derive from other EU legislation as listed in ESRS 2 appendix B. It is indicated where the datapoint can be found in the

report and which data points have not been included due to them being assessed as “not material”.

Disclosure requirement	Data point	Sustainability statements / Appendix	SFDR	Pillar 3	Benchmark Regulation	EU Climate Law	Section note
ESRS 2 GOV-1	21 d	Board's gender diversity	x		x		GOV-1, GOV-2 The role of, information provided to and sustainability matters addressed by the administrative, management and supervisory bodies
ESRS 2 GOV-1	21 e	Percentage of board members who are independent			x		GOV-1, GOV-2 The role of, information provided to and sustainability matters addressed by the administrative, management and supervisory bodies
ESRS 2 GOV-4	30	Statement on due diligence	x				GOV-4 Statement on due diligence
ESRS 2 SBM-1	40 d i	Involvement in activities related to fossil fuel activities	x	x	x		SBM-1 Strategy, business model and value chain
ESRS 2 SBM-1	40 d ii	Involvement in activities related to chemical production	x		x		SBM-1 Strategy, business model and value chain
ESRS 2 SBM-1	40 d iii	Involvement in activities related to controversial weapons	x		x		SBM-1 Strategy, business model and value chain
ESRS 2 SBM-1	40 d iv	Involvement in activities related to cultivation and production of tobacco			x		SBM-1 Strategy, business model and value chain
ESRS E1-1	14	Transition plan to reach climate neutrality by 2050				x	E1-1 Transition plan for climate change mitigation
ESRS E1-1	16 g	Undertakings excluded from Paris-aligned Benchmarks		x	x		E1-1 Transition plan for climate change mitigation
ESRS E1-4	34	GHG emission reduction targets	x	x	x		E1-4 Targets related to climate change mitigation and adaptation
ESRS E1-5	38	Energy consumption from fossil sources disaggregated by sources (only high climate impact sectors)	x				Not Material
ESRS E1-5	37	Energy consumption and mix	x				Not Material
ESRS E1-5	40-43	Energy intensity associated with activities in high climate impact sectors	x				Not Material
ESRS E1-6	44	Gross Scope 1, 2, 3 and Total GHG emissions	x	x	x		E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions
ESRS E1-6	53-55	Gross GHG emissions intensity	x	x	x		E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions
ESRS E1-7	56	GHG removals and carbon credits				x	Not Material
ESRS E1-9	66	Exposure of the benchmark portfolio to climate-related physical risks			x		Phase-in used

Disclosure requirement	Data point	Sustainability statements / Appendix	SFDR	Pillar 3	Benchmark Regulation	EU Climate Law	Section note
ESRS E1-9	66 a, 66 c	Disaggregation of monetary amounts by acute and chronic physical risk; Location of significant assets at material physical risk		x			Phase-in used
ESRS E1-9	67 c	Breakdown of the carrying value of its real estate assets by energy-efficiency classes		x			Phase-in used
ESRS E1-9	69	Degree of exposure of the portfolio to climate-related opportunities			x		Phase-in used
ESRS E2-4	28	Amount of each pollutant listed in Annex II of the E-PRTR Regulation emitted to air, water and soil	x				Not Material
ESRS E3-1	9	Water and marine resources	x				Not Material
ESRS E3-1	13	Dedicated policy	x				Not Material
ESRS E3-1	14	Sustainable oceans and seas	x				Not Material
ESRS E3-4	28 c	Total water recycled and reused	x				Not Material
ESRS E3-4	29	Total water consumption in m3 per net revenue on own operations	x				Not Material
ESRS 2 IRO 1– E4	16 a i		x				Not Material
ESRS 2 IRO 1– E4	16 b		x				Not Material
ESRS 2 IRO 1– E4	16 c		x				Not Material
ESRS E4-2	24 b	Sustainable land / agriculture practices or policies	x				Not Material
ESRS E4-2	24 c	Sustainable oceans / seas practices or policies	x				Not Material
ESRS E4-2	24 d	Policies to address deforestation					Not Material
ESRS E5-5	37 d	Non-recycled waste	x				Not Material
ESRS E5-5	39	Hazardous waste and radioactive waste	x				Not Material
ESRS 2 SBM-3 – S1	14 f	Risk of incidents of forced labour	x				S1-1 Policies related to own workforce
ESRS 2 SBM-3 – S1	14 g	Risk of incidents of child labour	x				S1-1 Policies related to own workforce
ESRS S1-1	20	Human rights policy commitments	x				S1-1 Policies related to own workforce
ESRS S1-1	21	Due diligence policies on issues addressed by the fundamental International Labor Organisation Conventions 1 to 8			x		S1-1 Policies related to own workforce

Disclosure requirement	Data point	Sustainability statements / Appendix	SFDR	Pillar 3	Benchmark Regulation	EU Climate Law	Section note
ESRS S1-1	22	Processes and measures for preventing trafficking in human beings	x				S1-1 Policies related to own workforce
ESRS S1-1	23	Workplace accident prevention policy or management system	x				S1-1 Policies related to own workforce
ESRS S1-3	32 c	Grievance/complaints handling mechanisms	x				S1-3 Processes to remediate negative impacts and channels for own workforce to raise concerns
ESRS S1-14	88 b, 88 c	Number of fatalities and number and rate of work-related accidents	x		x		S1-14 Health and safety metrics
ESRS S1-14	88 e	Number of days lost to injuries, accidents, fatalities or illness	x				S1-14 Health and safety metrics
ESRS S1-16	97 a	Unadjusted gender pay gap	x		x		S1-16 Compensation metrics (pay gap and total compensation)
ESRS S1-16	97 b	Excessive CEO pay ratio	x				S1-16 Compensation metrics (pay gap and total compensation)
ESRS S1-17	103 a	Incidents of discrimination	x				S1-17 Incidents, complaints and severe human rights impacts
ESRS S1-17	104 a	Non-respect of UNGPs on Business and Human Rights and OECD	x		x		S1-17 Incidents, complaints and severe human rights impacts
ESRS 2 SBM-3 – S2	11 b	Significant risk of child labour or forced labour in the value chain	x				Not Material
ESRS S2-1	17	Human rights policy commitments	x				Not Material
ESRS S2-1	18	Policies related to value chain workers	x				Not Material
ESRS S2-1	19	Non-respect of UNGPs on Business and Human Rights principles and OECD guidelines	x		x		Not Material
ESRS S2-1	19	Due diligence policies on issues addressed by the fundamental International Labor Organisation Conventions 1 to 8			x		Not Material
ESRS S2-4	36	Human rights issues and incidents connected to its upstream and downstream value chain	x				Not Material
ESRS S3-1	16	Human rights policy commitments	x				Not Material
ESRS S3-1	17	Non-respect of UNGPs on Business and Human Rights, ILO principles or and OECD guidelines	x		x		Not Material
ESRS S3-4	36	Human rights issues and incidents	x				Not Material
ESRS S4-1	16	Policies related to consumers and end-users	x				S4-1 Policies related to consumers and end-users
ESRS S4-1	17	Non-respect of UNGPs on Business and Human Rights and OECD guidelines	x		x		S4-1 Policies related to consumers and end-users

Disclosure requirement	Data point	Sustainability statements / Appendix	SFDR	Pillar 3	Benchmark Regulation	EU Climate Law	Section note
ESRS S4-4	35	Human rights issues and incidents	x				S4-4 Taking action on material impacts on consumers and end-users, and approaches to managing material risks and pursuing material opportunities related to consumers and end-users, and effectiveness o
ESRS G1-1	10 b	United Nations Convention against Corruption	x				G1-1 Business conduct policies and corporate culture
ESRS G1-1	10 d	Protection of whistleblowers	x				G1-1 Business conduct policies and corporate culture
ESRS G1-4	24 a	Fines for violation of anti-corruption and anti-bribery laws	x		x		Not Material
ESRS G1-4	24 b	Standards of anti- corruption and anti- bribery	x				Not Material

Environmental information

EU Taxonomy

General

WithSecure has performed an analysis of the EU Taxonomy Regulation (2020/852), Commission Delegated Regulation (2021/2139) on Taxonomy screening criteria (Climate Delegated Act), Commission Delegated Regulation (2021/2178) on Taxonomy disclosures (Disclosures Delegated Act) and other related guidance from the European Commission, on reporting the activities that qualify as contributing substantially to climate change mitigation or climate change adaptation, i.e., being taxonomy aligned. This review included the EU Commission Delegated Regulation (2022/1214) (Complementary Climate Delegated Act), the EU Commission Delegated Regulation (2023/2486) (Environmental Delegated Act), and the EU Commission Delegated Regulation (2023/2485) (Amendments to the Climate Delegated Act).

In 2023, a delegated act for economic activities was published by the EU, and four new objectives were added. These objectives are; pollution prevention and control, sustainable use and protection of water and marine resources, protection and restoration of biodiversity and ecosystems, and transition to a circular economy. Modifications to the climate-related delegated act were approved, leading to updates in the environmental objectives for climate change mitigation and adaptation, and changes in the assessment criteria. From 2024 onwards, in addition to reporting the taxonomy eligibility of these activities, companies must also report the taxonomy alignment of their activities.

In short, the EU taxonomy is a classification system that defines which economic activities are environmentally sustainable. WithSecure has applied components from the delegated acts into the analysis to ensure taxonomy eligibility and alignment. This included analysing WithSecure's operations in relation to various components of the delegated acts, including economic activities that contribute to non-climate environmental objectives, as well as nuclear and gas energy related activities. WithSecure has not identified any taxonomy-eligible economic activities, and therefore has not identified any activities for which taxonomy alignment could be determined.

The EU Taxonomy develops constantly and WithSecure closely follows the new information of taxonomy reporting requirements. WithSecure has not identified any significant changes impacting WithSecure's analysis of EU taxonomy. The

analysis has been performed in collaboration between the WithSecure product team, financial controlling and sustainability team.

Cyber security software, while supporting a wide range of activities in becoming digital and therefore reducing the need of physical materials and transportations of goods and people, as well as reducing the incremental cost of cybercrime to the society, is not an activity addressed by the current climate change mitigation and climate change adaptation taxonomy, hence it is not taxonomy eligible.

According to the European Commission, the purpose of the current Taxonomy Climate Delegated Act is to include the sectors producing the largest emissions. As a company operating in a low-emission sector, WithSecure business activities are not listed in the current EU Taxonomy, and therefore they are not considered to be taxonomy eligible.

WithSecure will closely follow the further developments of the taxonomy reporting requirements and complete 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 WithSecure and trigger a need of re-assessing both eligibility and alignment.

Taxonomy-eligible 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. A more in-depth description of the turnover can be found in section "[1 Segment information](#)" of the financial statements.

Based on the analysis of the current economic activities listed in taxonomy, WithSecure business activities fall under Activity 8.2 Computer programming, consultancy and related activities (NACE J62) of the Commission Delegated Regulation (2021/2139). Within the Taxonomy, Activity 8.2 is not defined as enabling. According to the definition of turnover in Annex I of the Commission Delegated Regulation (2021/2178), cannot be defined as eligible or aligned.

Additionally, Activity 8.2 is categorized as an 'adapted' activity within the Taxonomy. This means it cannot be considered eligible unless the reporting entity can demonstrate that a climate risk and vulnerability assessment has been conducted and an expenditure plan has been established to implement adaptation solutions that mitigate the most significant physical climate risks, as outlined in Appendix A to Annex II of the Delegated Regulation (2021/2139).

WithSecure's primary activities do not directly contribute to the environmental objectives outlined in the Annex I of the Commission Delegated Regulation (2021/2178). WithSecure's services focus on protecting digital infrastructure and data, which, while crucial to businesses, does not exactly align with the specific environmental criteria set out in the Taxonomy. As a result, WithSecure reports 0% of its revenue as taxonomy eligible. Consequently, no technical screening criteria apply, and the revenue cannot be considered taxonomy aligned.

Taxonomy-eligible operating expenses

The Operating expenses (7.78MEUR) included in the taxonomy assessment are defined as direct non-capitalised costs that relate to research and development, building renovation measures, short-term lease, maintenance and repair, and any other direct expenditures relating to the day-to-day servicing of assets of property, plant and equipment by the undertaking or third party to whom activities are outsourced that are necessary to ensure the continued and effective functioning of such assets (2021/2178).

According to the Delegated Regulation (2021/2178), the operating expenses to be considered as eligible must be any of the following:

- (a) related to assets or processes associated with Taxonomy-aligned economic activities, including training and other human resources adaptation needs, and direct non-capitalised costs that represent research and development;
- (b) part of the CapEx plan to expand Taxonomy-aligned economic activities or allow Taxonomy-eligible economic activities to become Taxonomy-aligned within a predefined timeframe;
- (c) related to the purchase of output from Taxonomy-aligned economic activities and to individual measures enabling the target activities to become low-carbon or to lead to greenhouse gas reductions as well as individual building renovation

measures as identified in the delegated acts adopted pursuant to Article 10(3), Article 11(3), Article 12(2), Article 13(2), Article 14(2) or Article 15(2) of Regulation (EU) 2020/852 and provided that such measures are implemented and operational within 18 months.

WithSecure's OpEx has been assessed using these three approaches. WithSecure has conducted calculations in terms of assets including operating expenses related to rental of premises (including depreciations for leased premises accounted for under IFRS 16 standard), maintenance of premises as well as other expenses related to the functioning of the leased and owned property, plant and equipment. These were not identified as taxonomy-eligible. Additionally, the CapEx plan does not currently include expansions of Taxonomy-aligned activities or transitions of eligible activities to become aligned within a set timeframe. WithSecure utilizes third-party cloud platforms of Amazon Web Services (AWS) and Microsoft Azure for majority of its operations. Cloud hosting costs are not included in the Operating expense subject to taxonomy assessment. Taxonomy eligibility of WithSecure operating expense is therefore 0%.

Taxonomy-eligible capital expenses

The Capital expenses included in the taxonomy assessment are defined as additions to tangible and intangible assets during the financial year considered before depreciation, amortisation and any re-measurements, including those resulting from revaluations and impairments, for the relevant financial year and excluding fair value changes (2021/2178). A more in-depth description of the capital expenses can be found in section "[Statement of cash flows January 1 – December 31, 2024](#)" of the financial statements.

WithSecure capital expenses (5.93MEUR) include capitalizations of long-term IT projects and development expenditure on new products or product versions with significant new features, according to IAS 38 accounting standard.

According to the Delegated Regulation (2021/2178), the capital expenses to be considered as eligible must be any of the following:

- (a) related to assets or processes associated with Taxonomy-aligned economic activities, including training and other human resources adaptation needs, and direct non-capitalised costs that represent research and development;

(b) part of the CapEx plan to expand Taxonomy-aligned economic activities or allow Taxonomy-eligible economic activities to become Taxonomy-aligned within a predefined timeframe

(c) related to the purchase of output from Taxonomy-aligned economic activities and to individual measures enabling the target activities to become low-carbon or to lead to greenhouse gas reductions as well as individual building renovation measures as identified in the delegated acts adopted pursuant to Article 10(3), Article 11(3), Article 12(2), Article 13(2), Article 14(2) or Article 15(2) of Regulation (EU) 2020/852 and provided that such measures are implemented and operational within 18 months.

WithSecure's CapEx has been assessed using these three approaches. Accordingly, WithSecure's research work relates to developing the current activities that are considered as non-eligible for taxonomy reporting (see paragraph Taxonomy-eligible turnover above). WithSecure's CapEx plan does not currently include expansions of Taxonomy-aligned activities or transitions of eligible activities to become aligned within a set timeframe. A minor part of capital expenses relates to capitalization of employee laptops and other hardware, as well as office renovation expenses, however these are not taxonomy eligible, as they are not measures aimed at reducing GHG emissions. Taxonomy eligibility of WithSecure capital expense is therefore 0%.

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

Proportion of turnover from products or services associated with Taxonomy-aligned economic activities – disclosure covering year 2024

Financial year 2024	Year		Substantial Contribution Criteria							DNSH criteria ('Does Not Significantly Harm')(h)							Proportion of Taxonomy aligned (A.1.) or eligible (A.2.) turnover, year 2023 (18)	Category enabling activity (19)	Category transitional activity (20)			
	Economic Activities (1)	Code (a) (2)	Turnover (3)	Proportion of Turnover, year N (4)	Climate Change Mitigation (5)	Climate Change Adaptation (6)	Water (7)	Pollution (8)	Circular Economy (9)	Biodiversity (10)	Climate Change Mitigation (11)	Climate Change Adaptation (12)	Water (13)	Pollution (14)	Circular Economy (15)	Biodiversity (16)				Minimum Safeguards (17)		
Text		Currency	%	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	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%	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL	N	N	N	N	N	N	N	N	0%				
Of which Enabling		0	0%	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL	N	N	N	N	N	N	N	N	0%	E			
Of which Transitional		0	0%	N/EL						N	N	N	N	N	N	N	N	0%		T		
A.2 Taxonomy-Eligible but not environmentally sustainable activities (not Taxonomy-aligned activities) (g)																						
				EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)												
Turnover of Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities) (A.2)		0	0%	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL								0%				
A. Turnover of Taxonomy eligible activities (A.1+A.2)		0	0%	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL													
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES																						
Turnover of Taxonomy-non-eligible activities		147.4	100%																			
TOTAL		147.4	100%																			



Proportion of OpEx from products or services associated with Taxonomy-aligned economic activities – disclosure covering year 2024

Financial year 2024	Year		Substantial Contribution Criteria							DNSH criteria ('Does Not Significantly Harm')(h)							Proportion of Taxonomy aligned (A.1.) or eligible (A.2.) OpEx, year 2023 (18)	Category enabling activity (19)	Category transitional activity (20)		
	Economic Activities (1)	Code (a) (2)	OpEx (3)	Proportion of OpEx, year N (4)	Climate Change Mitigation (5)	Climate Change Adaptation (6)	Water (7)	Pollution (8)	Circular Economy (9)	Biodiversity (10)	Climate Change Mitigation (11)	Climate Change Adaptation (12)	Water (13)	Pollution (14)	Circular Economy (15)	Biodiversity (16)				Minimum Safeguards (17)	
Text		Currency	%	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	Y; N; N/EL (b) (c)	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%	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL	N	N	N	N	N	N	N	N	0%			
Of which Enabling		0	0%	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL	N	N	N	N	N	N	N	N	0%	E		
Of which Transitional		0	0%	N/EL						N	N	N	N	N	N	N	N	0%		T	
A.2 Taxonomy-Eligible but not environmentally sustainable activities (not Taxonomy-aligned activities) (g)																					
				EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)	EL; N/EL (f)												
OpEx of Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities) (A.2)		0	0%	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL								0%				
A. OpEx of Taxonomy eligible activities (A.1+A.2)		0	0%	N/EL	N/EL	N/EL	N/EL	N/EL	N/EL												
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES																					
OpEx of Taxonomy-non-eligible activities		7.78	100%																		
TOTAL		7.78	100%																		

ESRS E1 - Climate change

SBM-3 Material impacts, risks and opportunities related to climate change

E1 Climate change

Material impacts	Material risks and opportunities	Stakeholder view
Climate change mitigation		
 <p>The direct impact possibilities on climate change are considered to be limited in scope, due to the nature of the business and emissions structure. See more in section "GHG emissions".</p>	 <p>Customers moving to cloud environments in search of modern, cost-effective, secure and sustainable solutions continues to present a major business opportunity for WithSecure.</p>	<p>Slightly relevant. Cloud transition has been a part of the WithSecure's business plan for years and it is expected to yield growth of revenue. The importance of cyber security is widely recognized by all stakeholders. Software and service companies' work on their own carbon emissions is not seen as a very relevant area or concern, due to the limited magnitude of the emissions.</p>

 — Positive impact / Financial opportunity
  — Negative impact / Financial risk
  — No material impact, risk or opportunity identified

WithSecure has identified the material impacts, risks and opportunities related to climate change based on the double materiality assessment introduced in its own section. Climate change and specifically climate change mitigation has been identified as a material topic for the company.

The impact possibilities on climate change are considered limited in scope, due to the nature of the business and emissions structure of WithSecure. WithSecure's business model is not emission intensive, as is with most companies operating in the software sector. Most of the emissions WithSecure's operations generate are scope 3 emissions in the upstream value chain. The direct emissions from both scope 1 and 2 are relatively limited.

Simultaneously, the possible climate-related risks WithSecure could face are low in magnitude, likelihood or both. WithSecure has not identified itself to be vulnerable to any material climate-related physical or transition risks, rendering the need for

climate change adaptation actions redundant. Consequently, no assets have been recognised to be exposed or vulnerable to climate-related risks.

WithSecure has identified the ongoing shift of customers to cloud-based IT environments as a significant, continuing opportunity. This financial opportunity aligns with WithSecure's broader sustainability program. By providing cybersecurity software and services, WithSecure can indirectly support digital climate solutions for mitigation and adaptation, fostering trust and security in the digital world. This opportunity is assessed to materialize in the medium term.

WithSecure aims to advance its management of climate change related impacts, risks and opportunities during the coming years. The plan is to update the double materiality analysis and re-evaluate the material impacts, risks and opportunities. WithSecure will explore next steps and possible related science-based targets that could be suitable and reasonable for WithSecure's business model and impacts.

Topic	Policy	Action	Metric	Target	Status	
					2022	2024
The identified material topic	The policies related to handling/ mitigating that topic	The actions related to handling/ mitigating that policy	The metrics used to measure the action	The target related to the identified metric	Where WithSecure is in terms of the target + comparison to base year figures	
ESRS E1 "Climate change"						
Climate change mitigation	Sustainability policy	WithSecure commits to reducing its carbon footprint	Tons of CO2 emissions per million EUR revenue	Carbon footprint reduced to 75 tons of CO2 per million EUR of revenue (<i>location-based</i>)	118 tCO2eq / MEUR	69 tCO2eq / MEUR
			Business flight emissions	Business flight emissions maintained at base year level	1084 tCO2eq	891 tCO2eq

E1-1 Transition plan for climate change mitigation

Due to WithSecure’s limited impact on climate change, the company does not currently have a transition plan in place for climate change mitigation. For the same reason, WithSecure has not conducted a resilience analysis in the identification process of the material impacts, risks and opportunities. One general scenario was implemented. Separate scenarios for low, medium or high emission scenarios were not utilized. The climate change related targets are not analysed in relation to limiting global warming to 1.5°C in line with the Paris Agreement. WithSecure is not excluded from the EU Paris-aligned benchmarks. As WithSecure progresses in its sustainability journey, it will aim to enhance the monitoring and assessment of the company’s activities. The intention is to enhance the company’s adherence to the provisions of the Delegated Act (EU) 2021/2139, supporting efforts in climate change mitigation.

E1-2 Policies related to climate change mitigation and adaptation

WithSecure has a Sustainability policy which addresses climate change mitigation. The policy is publicly available on WithSecure’s website. Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis. Thus, the stakeholders have been involved and their views have been included in the policy. The most senior level

accountable for the implementation of this policy are the GLT members of each business unit most closely associated with the respective policy.

Sustainability policy

The purpose of WithSecure’s Sustainability Policy is to define the objectives for sustainability-related matters at WithSecure, demonstrate the company’s commitment to operating sustainably and establish an effective sustainability governance. The policy serves as a framework for continually improving WithSecure’s performance and integrating sustainable practices into the company’s daily operations.

The policy outlines WithSecure’s commitment to maximizing the company’s net impact on the planet, people, and society. WithSecure aims to embed sustainability into all the company’s decision-making processes and ensure transparency of WithSecure’s activities to the company’s stakeholders.

The sustainability policy applies to WithSecure’s own operations and all persons working for WithSecure, anywhere WithSecure operates globally.

The policy is publicly available on WithSecure’s website.

E1-3 Actions and resources in relation to climate change policies

WithSecure does its share in reducing the amount of waste and emissions produced by the company's operations, whenever it is reasonably possible. WithSecure has committed to reducing its carbon footprint as the company's main action to mitigate the climate change related negative impacts and risks, while emphasizing the possibilities for positive actions and supporting positive impacts as well as opportunities.

WithSecure's carbon footprint analysis includes the company's own operations and as well as both upstream and downstream activities. The scope of WithSecure's carbon footprint reduction actions is the company's own operations and upstream activities, as no material emissions were identified in the downstream activities. A more detailed description of the different material GHG emissions are described in the section "[E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions](#)". The carbon footprint reduction is an ongoing process. No significant expenditures are allocated for this action.

The Sustainability Policy provides the framework and guidelines for the actions WithSecure takes to reduce its carbon footprint. These actions are designed to address the specific areas where the company can make the most significant impact. The carbon footprint reduction is completed through a variety of different measures. These measures involve for example the company's offices, employee commuting and business travel. These are some of WithSecure's main avenues for reducing the company's carbon footprint.

- **Offices**

WithSecure has 15 offices globally, the major locations being Helsinki (Finland), London (UK), Kuala Lumpur (Malaysia) and Poznan (Poland). WithSecure offices are leased premises, and therefore the company does not have full control of the decisions taken by landlords on the energy efficiency of the buildings. However, WithSecure strongly encourage the company's landlords to take all available measures to optimize heating, cooling, lighting, and waste management at the company's office premises. WithSecure strives to minimize the company's ecological footprint by providing sustainable offices that enhance WithSecure's employees' wellbeing. To facilitate this, WithSecure has "Sustainable Workplace Guidelines" for all the 15 offices across the globe. WithSecure believes that by building for the future and implementing these guidelines it can make a positive difference for the planet and its people.

During the year 2024, the Helsinki office moved to new headquarters in Wood City, where the building has a LEED Platinum certification and A class energy

rating. The exact impact of this relocation has not been evaluated beyond the calculation of total scope 2 emissions of all offices.

- **Commuting**

Green commuting of the employees is supported through various measures. In three of WithSecure's locations, the company offers a bicycle benefit for the employees to encourage cycling to work. In three locations, WithSecure provides commuting allowances to support the use of public transportation.

- **Business travel**

WithSecure Travel Policy continues to provide a unified and simplified travel process to ensure safe, efficient and environmentally friendly business travel. It aims to reduce the environmental impact of traveling, aligned with the company sustainability targets. Employees are encouraged to use digital meeting tools when collaborating with internal and external stakeholders, and to travel only when needed, using environmentally friendly options and combining travel when possible. Due to the nature of WithSecure's business and the company's multi-location teams, the company will always require some travelling.

E1-4 Targets related to climate change mitigation and adaptation

WithSecure's actions for climate mitigation are measured through an intensity metric following the tons of CO₂ emissions per million EUR revenue emitted in WithSecure's operations and value chain. The methodology for the CO₂ emission calculations have been detailed in the section "[E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions](#)". The business flight emissions are followed as a separate metric from the total CO₂ emissions. Their calculation methodology is also detailed in that section.

The footprint reduction target is a total amount of tons of CO₂ per million EUR of revenue, making the target relative to revenue. The measured unit is the amount of CO₂ emissions in WithSecure's own operations and value chain. These total emissions include the emission from flights. This intensity target will allow the company growth but without a similar increase to the carbon footprint. The business flight related target is relative to the base year level. The scope for business flight emissions are people working for WithSecure. In addition to these informal targets, WithSecure is exploring the implementation of possible science-based targets suitable for WithSecure's business model and impacts.

The baseline value for the total carbon footprint is 75 tons of CO₂ emissions per million EUR of revenue. The baseline year for CO₂ emissions including the

business flights is 2022. WithSecure's GHG reduction initiatives impact upstream value chain. These targets are measured continuously, at least annually. The targets are not science-based.

Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis. Thus, the stakeholders have been involved and their views have been included in the setting and choosing of the targets.

Performance in the year 2024 is in line with the targets as the overall CO₂ emissions have decreased. Compared to the baseline emissions, the 2024 emissions have decreased by -36% for location-based emissions and -38% for market-based emissions. Compared to the year 2023 there is also a clear decrease in total emissions of -14% for both the location- and market-based emissions.

WithSecure reached the goal of reducing the company's carbon footprint to below 75 tons of CO₂ per million EUR of revenue. This GHG intensity figure for the year 2024 is 69.2 tCO₂eq / MEUR. In terms of the business flight emissions, those have also decreased from the 1,084 tCO₂eq baseline level to 891 tCO₂eq for the year 2024. Thus, both targets have been reached.

The mentioned methods have contributed to the carbon footprint reduction during the year 2024. In terms of business travel (flights), WithSecure has encouraged virtual meetings and limited non-essential travel, reducing travel-related emissions, resulting in the carbon footprint being -33% lower. Employee commuting has been addressed by promoting remote work options, supporting the use of public transportation, and encouraging the employees to cycle to work, decreasing the carbon footprint by -10%. These measures reflect WithSecure's sustainability policy to support sustainable commuting practices. These actions collectively contribute to the overall reduction in emissions, although no specific decarbonisation levers have been used.

The CO₂ and business travel emission outcomes have been described in more detail in the section "[E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions](#)".

E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions

Baseline

WithSecure's carbon footprint consists primarily of indirect emissions. Most of WithSecure's emissions were identified as Scope 3 (indirect, others) emissions. WithSecure's upstream leased assets were identified as Scope 2 (indirect, purchased electricity, steam, heating, and cooling) emissions in 2024, and the company did not identify any Scope 1 emissions (from own offices, vehicles, and fugitive emissions).

WithSecure's CO₂ emissions baseline is 2022, with adjustments made in 2023 to include heating estimates for Scope 2 emissions and additional spend-based emissions for Scope 3, specifically in Category 1 – Goods and services. The baseline emissions are 15,935 tons of CO₂e for location-based emissions and 15,883 tons of CO₂e for market-based emissions.

There was a slight adjustment to Scope 2 emissions for 2023, as the square meterage of the Helsinki, Poznan and Stockholm offices was determined more precisely. Additionally, the emissions allocation per area in use for WithSecure in the old Helsinki office building, which was shared with other tenants, was refined. Furthermore, district heating for the Oulu offices was added to the calculations separately. This increased the scope 2 emissions from 564 tons of CO₂e to 850 tons of CO₂e. There was also a minor correction to the Scope 3 emissions for 2023, decreasing the total scope 3 emissions from 11,080 tons of CO₂e to 11,068 tons of CO₂e, due to cloud computing originally being accounted for twice.

Calculation methodologies

The calculations are conducted based on the Greenhouse Gas (GHG) Protocol. The GHG calculation methodology follows the financial control consolidation method. There have been no changes to the GHG protocol consolidation methodology or significant changes to the organisational structure that would impact the GHG emissions calculation.

WithSecure's GHG emissions are calculated in the following manner: the total annual CO₂ emissions are determined based on actual emissions from January to November, with December emissions included as a forecast. For primarily the

year end months, the scope 2 emissions have been estimated using forecasts and historical data due to insufficient reliable data from the local service partners. The calculation principles for the comparable figures are the same. Biomass or biogenic emissions are not separately calculated or taken into account for any of the emissions. WithSecure's GHG figures are not externally assured beyond the audit assurance of this report. The comparable figures are not within the scope of the audit assurance.

Scope 2 – Purchased electricity, heating, and cooling

The calculation followed the GHG protocol, consisting of both the location-based and market-based emissions. The methods included the electricity consumption by location and the appropriate emission factor.

The emission factor represents the GHG intensity of the electricity consumption in the location. For the location-based emission factor, the CO₂ emissions of electricity generation have been calculated using appropriate CO₂ residual mix emission factors for the office locations sourced from [AIB](#) for European locations and for non-European locations from local authorities' websites, including [DEFRA](#), [SEDA](#), [EMA](#), [Climate Transparency](#), and [EPA](#).

The market-based emissions have been estimated using the emission factors published on the websites of the companies that provide electricity to WithSecure's office locations. This includes the Helsinki offices' electricity emissions from the base year 2022 onwards and for the London office for the year 2024. In other locations where no specific emission factor is provided by the local electricity providers, the same residual mix factor used for the location-based calculation was applied. There are no contractual obligations or other agreements related to WithSecure's Scope 2 emissions.

The average consumption of WithSecure's offices per square meter was used to estimate the consumption in locations where electricity consumption data was not available. The office electricity consumption corresponds with WithSecure's proportion of each office, when WithSecure shares office space with external parties. Heating consumption was included in the energy consumption of the offices which are located in countries where district heating is common. These countries are Finland, Sweden, Denmark and Poland. Statistical data was used to estimate the heating consumption, and the consumption was calculated in cubic meters. Cooling of the offices is included in the electricity consumption.

Scope 3

Category 1 – Goods and services

The category 1 emissions are based on the actual usage related footprint, as collected directly from the service providers, such as the suppliers of cloud computing services. In the absence of such activity-based data for other purchases, WithSecure has used the GHG Protocol's spend-based method to calculate the emissions from goods and services. The emission factor (sourced from [Exiobase3](#)) has been applied for the collected economic value of goods and services purchased. The spend-based method is based on estimated averages, and therefore includes significant uncertainty regarding data accuracy. However, WithSecure's purpose is to include the full inventory of emissions in the footprint calculation.

Category 5 – Waste emissions

WithSecure used GHG Protocol's average-data method in the calculations. First, the average annual waste produced per employee was determined and then the amount of waste was calculated by estimated treatment method. Landfill and combustion were the treatment methods included in the calculations. The applicable emission factor by country (sourced from [DEFRA](#)) was used for each waste amount by waste treatment type.

Category 6 – Business travel (flights)

Applicable emission factors (sourced from [DEFRA](#)) were used based on the flight type, distance, and cabin class. The data was collected from internal travel data and third-party data provided by travel agencies. The category only includes the flights booked for the year 2024. The same cut-off method has been consistently applied on the previous year. Other business travel expenses, such as train tickets and hotel expenses, are included in Category 1. In 2022, WithSecure used the applicable emission factors from [DEFRA](#) and [EPA-US](#). For 2023 and 2024, all flights were calculated using [DEFRA](#) emission factors.

Category 7 – Employee commuting

GHG Protocol's distance-based method was used in the calculations per employee. WithSecure determined the travel method (car, train, bus, cycling, and walking) and used the applicable emission factor (sourced from [DEFRA](#)) in the calculations.

The average distance to work, estimated office days per week and the estimated split of travel method per country were determined. The calculations included the bicycle, car, and public transportation benefits, as well as estimates of travel mode per country.

Year 2024

The total location-based emissions for 2024 were 10,205 tons of CO₂e, corresponding to the annual emissions of 2,219 typical petrol passenger cars. The total market-based emissions for 2024 were 9,908 tons of CO₂e, corresponding to the annual emissions of 2,154 typical petrol passenger cars. The GHG intensity based on net revenue for 2024 is 69.2 .

For 2024 scope 2 location-based emissions were 928 tons of CO₂e (9% of total location-based GHG emissions), while the market-based emissions were 630 tons of CO₂e (6% of total market-based GHG emissions). Scope 2 emissions include the energy consumption of WithSecure's offices. Heating emissions have been estimated for offices in Finland, Sweden, Denmark and Poland. In these countries district heating has a significant share of the total heat market. Cooling of the offices is included in the electricity consumption.

Scope 3 emissions were 9,278 tons of CO₂e (91% of total location-based GHG emissions, 94% of total market-based GHG emissions). Four categories were identified as Scope 3 indirect emissions. These categories are Category 1 – Goods and services, Category 5 – waste emissions, Category 6 – business travel (flights), and Category 7 – employee commuting. The content, calculation methods and reporting boundaries used for each category are briefly explained per each category.

WithSecure's carbon footprint currently excludes emissions from third-party devices running WithSecure software (Category 11 – Use of sold products). An estimate for customer device energy use is not included due to the significant variances related to the assumptions. For example, variations in device types, usage patterns, and energy efficiency make it challenging to provide an accurate estimate. Based on the current analysis and assumptions, emissions from this category are not considered significant due to the variability in device energy consumption and their relatively small share of total emissions. However, as part of WithSecure's sustainability initiatives, the company has started collecting real-life endpoint energy-usage data. When reliable, validated measurements are available, WithSecure will consider adding Category 11 to the company's carbon footprint.

WithSecure has also excluded the following categories from the CO₂ calculations as these categories are not applicable for WithSecure's business model and operations, or WithSecure has no significant emissions that fall within these categories;

- Category 2 – Capital Goods
- Category 3 – Fuel- and energy-related activities
- Category 4 – Upstream transportation and distribution
- Category 8 – Upstream leased assets
- Category 9 – Downstream transportation and distribution
- Category 10 – Processing of sold products
- Category 12 – End-of-life treatment of sold products
- Category 13 – Downstream leased assets
- Category 14 – Franchises
- Category 15 – Investments

Metrics that include value chain and other data estimated using indirect sources are limited to the GHG emissions calculations. These indirect sources include sector-average data and other figures from recognized and reliable databases.

WithSecure has identified that the quantitative metrics related to Greenhouse Gas emission Scope 3 calculations are subject to measurement uncertainty due to the availability and quality of data from the company's upstream and downstream value chains as well as the publicly available databases. WithSecure is dependent on the parties providing the requested information from the upstream and downstream value chains ensuring that the value chain data fulfils the information needs communicated to them. To detect and mitigate any major data discrepancies, WithSecure conducts internal comparison and analysis of the data from the value chain and updates used database sources regularly.

	Retrospective				
	2022 (Base year)	2023 (Compa- rative)	2024	Δ% (2023 vs 2024)	
Scope 1 GHG emissions					
Gross Scope 1 GHG emissions (tCO ₂ eq)	0	0	0	0%	
Scope 2 GHG emissions					
Gross location-based Scope 2 GHG emissions (tCO ₂ eq)	310	850	928	9%	
Gross market-based Scope 2 GHG emissions (tCO ₂ eq)	259	438	630	44%	
Significant scope 3 GHG emissions					
Total Gross indirect (Scope 3) GHG emissions (tCO ₂ eq)	15,624	11,068	9,278	-16%	
1	Purchased goods and services	13,955	9,212	7,915	-14%
Sub-category: Cloud computing and data centre services		26	12	28	130%
5	Waste generated in operations	20	18	16	-8%
6	Business traveling	1,084	1,330	891	-33%
7	Employee commuting	565	509	456	-10%
Total GHG emissions					
Total GHG emissions (location-based) (tCO ₂ eq)		15,935	11,918	10,205	-14%
Total GHG emissions (market-based) (tCO ₂ eq)		15,883	11,506	9,908	-14%

GHG intensity per net revenue	2023 (Compa- rative)	2024	Δ% (2023 vs 2024)
Total GHG emissions (location-based) per net revenue (tCO ₂ eq/MEUR)	83.5	69.2	-17%
Total GHG emissions (market-based) per net revenue (tCO ₂ eq/MEUR)	80.6	67.2	-17%

Scope 2 – Purchased electricity, heating, and cooling

The emissions for energy consumption of WithSecure's offices were calculated for all of the company's offices. 6% - 9% of WithSecure's carbon footprint stems from energy consumption, depending on whether location- or market-based total emissions are used.

Scope 3

Category 1 – Goods and services

Goods and Services is the largest emission category for WithSecure, as 78% - 80% of the company's total emissions were from Goods and services, depending on whether location- or market-based total emissions are used. Cloud data processing emissions are 0.27% - 0.28% of WithSecure's total emissions.

Category 5 – Waste emissions

0.16% of WithSecure's total emissions consist of waste emissions.

Category 6 – Business travel (flights)

Business travel (flights) amount to 9% of WithSecure's total emissions. WithSecure used GHG Protocol's distance-based method to calculate the emissions from flights.

Category 7 – Employee commuting







4% - 5% of WithSecure's carbon footprint stem from the employee commuting category.


Social information

ESRS S1 - Own workforce

SBM-3 Material impacts, risks and opportunities related to own workforce

S1 Own workforce

Material impacts	Material risks and opportunities	Stakeholder view
Working conditions		Relevant. Competent workforce is the most important expectation for a software and service company. Unmanaged attrition can cause competence gaps. This issue, however, is universal and not WithSecure specific.
 <p>The potential impacts on working conditions are considered as relatively limited, since majority of the employees are knowledge workers.</p>	 <p>Improved employee retention can impact business positively through better sales and lower costs.</p>	
	 <p>Shortcomings in working conditions or employee wellbeing can increase costs through leaves of absence for physical or mental reasons. In the worst case, such shortcomings can lead to security risks that could cause reputational damage.</p>	
Equal treatment and working opportunities for all		
 <p>The potential impacts on equal treatment and working opportunities are considered as relatively limited, since majority of the employees are knowledge workers.</p>	 <p>Promoting diversity, equity and inclusion (DEI) will increase WithSecure's ability to attract talent. In the long run there will also be cost savings for retaining talent at WithSecure.</p>	
	 <p>Shortcomings in training and skills management can lead to losing out on business opportunities. Additional financial risks associated with this are related to attrition, brain leakage and disengagement of employees. Especially for a company in cyber security, it is of utmost importance to keep the employees' skills up to date. The industry faces continuous challenges regarding investment to technical solutions. Missing the mark can lead to financial losses.</p>	

 — Positive impact / Financial opportunity
  — Negative impact / Financial risk
  — No material impact, risk or opportunity identified

WithSecure has identified the material impacts, risks and opportunities related to own workforce based on the double materiality assessment introduced on its own section "[SBM-3 Material sustainability-related impacts, risks and opportunities](#)". The ESRS sub-topics of "Working conditions" and "Equal treatment and working

opportunities for all" were identified as material topics for WithSecure. Although no material impacts were found for these topics, the company did identify significant financial risks and opportunities associated with them.

Topic	Policy	Action	Metric	Target	2024 Status
The identified material topic	The policies related to handling/ mitigating that topic	The actions related to handling/ mitigating that policy	The metrics used to measure the action	The target related to the identified metric	Where WithSecure is in terms of the target
ESRS S1 "Own workforce"					
Working conditions		New investments in learning and development initiatives	Total hours spent on learning	Increase the total hours spent on learning from the previous year.	6.3 hours
		Support line managers in having individual development discussions	Individualized development goals	90% of employees to have personal development goals defined and documented	81.6 %
Equal treatment and working opportunities for all	Code of conduct WIDE strategy (well-being, inclusion, diversity, and equity) Harassment Prevention Policy & Procedure Grievance policy Whistleblowing policy Rewarding philosophy Learning philosophy	Driving diversity and promoting gender balance in leadership	Gender balance among line managers	Increase the representation of female leaders among the line managers	25.9 %
			Diversity among senior leaders	Maintain the number of different nationalities and the representation of female leaders among senior leaders at the base year level	Other than male senior leaders 35.6 % Number of nationalities 9
		Gender pay gap analysis to be conducted with the regular 2025 salary review process	Gender pay gap	Reduce the unexplainable gender pay gap to no more than 5% by the end of 2027	13.9 %*

* This figure includes pay gaps that can be explained by differences in location or job levels

S1-1 Policies related to own workforce

The policies outlined below are adopted to effectively manage WithSecure's material impacts on its own workforce, as well as the associated material risks and opportunities. These frameworks are designed to address critical areas such as employee well-being, professional development, diversity, equity, and inclusion, and workplace safety, ensuring a supportive and thriving environment for everyone. By proactively mitigating risks like skill gaps, disengagement, or workplace inequities,

and seizing opportunities to enhance talent retention and leadership capabilities, WithSecure ensures that its workforce remains a resilient and integral driver of the company's long-term success. The most senior level accountable for the implementation of these policies are the GLT members of each business unit most closely associated with the respective policy.

Code of Conduct (incl. Human Rights Policy)

Please see section "[G1-1 Business conduct policies and corporate culture](#)".

Whistleblowing policy

Please see section "[G1-1 Business conduct policies and corporate culture](#)".

WIDE strategy

The WIDE strategy (Wellbeing, Inclusion, Diversity, and Equity) aims to create a supportive, inclusive, and equitable workplace. It prioritizes employee wellbeing, fosters belonging, celebrates diversity, and ensures fair access to opportunities. Progress is monitored through regular employee feedback surveys.

The strategy applies organization-wide, and the accountability rests with Chief Culture and Performance Officer. The strategy is shared through internal communications and trainings to promote awareness.

Harassment Prevention Policy & Procedure

The harassment prevention policy underscores WithSecure's commitment to a workplace free from harassment and discrimination. It aims to foster a respectful, safe, and inclusive environment for all employees, regardless of position or location. The policy outlines the company's zero-tolerance stance on harassment, serving as a key resource for awareness and prevention.

This policy applies globally to all WithSecure employees, without exclusions, ensuring consistent standards across locations. Accountability for implementation rests with Chief Culture and Performance Officer.

Grievance policy

The Grievance Policy ensures employees have a clear and fair process for resolving employment-related concerns promptly and equitably. It promotes consistent and transparent handling of grievances, fostering trust and fairness in the workplace.

This policy applies to all workers ensuring broad accessibility and fairness. Local legislation and requirements are taken into consideration, and the policy is tailored and detailed in local HR handbooks. It is communicated through internal channels to ensure employees understand the process and their rights.

Rewarding philosophy

The Rewarding Philosophy Policy outlines WithSecure's commitment to fair, transparent, and competitive compensation practices. Its objectives are to reward good performance, promote equity, enhance employee engagement, and align compensation with market benchmarks. The policy mitigates risks such as employee turnover and disengagement, while fostering opportunities to attract and retain top talent. Monitoring is conducted through structured processes like the Global Salary Review and performance-based incentive evaluations.

The policy applies to all employees globally, ensuring consistency across countries, business lines, and functions. There are no significant exclusions, as it is tailored to address local market conditions and practices. Accountability for implementation lies with the Chief Culture and Performance Officer, ensuring alignment with organizational goals.

The policy aligns with relevant external market benchmarks and standards to maintain competitiveness and fairness. Key stakeholder interests, such as employee feedback and market data, are central to its design. The policy is made accessible to all employees through the company intranet, ensuring transparency and understanding across the organization.

Learning philosophy

The Learning Philosophy Policy highlights WithSecure's commitment to fostering personal and professional growth through equal access to diverse learning opportunities. Guided by the 70-20-10 model, it emphasizes learning through real-world experiences, collaboration, and structured programs, helping employees develop skills, stay competitive, and align personal goals with organizational priorities. Risks such as skill gaps and disengagement are mitigated, while opportunities for innovation and talent retention are enhanced. Progress is supported through performance and development planning, regular check-ins, and access to robust learning resources. The policy applies to all employees globally, ensuring inclusivity across geographies and roles. Accountability for the policy lies with the Chief Culture and Performance Officer, ensuring its alignment with organizational values. It is accessible through the company intranet, providing clear guidance on personal development processes and available learning resources.

WithSecure has not identified any specific groups within its workforce as being at particular risk of vulnerability. The company's policies and commitments are designed to ensure equity, inclusion, and well-being for all employees, fostering an environment where every individual is supported and treated fairly, regardless of their role, background, or circumstance. These principles underpin WithSecure's dedication to creating a safe, inclusive, and empowering workplace.

WithSecure's Code of Conduct outlines the ethical principles that guide the company's operations, emphasizing integrity, transparency, and accountability. It sets clear expectations for employee behaviour, promoting a workplace culture of respect, fairness, and compliance with all applicable laws and regulations. These principles ensure that working conditions are conducive to retaining talent, fostering their well-being, and promoting equal treatment and opportunities for all. An in-depth description of the Code of Conduct is included in the section "[G1-1 Business conduct policies and corporate culture](#)".

Respecting the human rights is a fundamental aspect of WithSecure's business model. The Code of Conduct integrates the United Nations Guiding Principles on Business and Human Rights (UNGPs), which serve as a foundational framework for the company's policies. While not explicitly outlined in the Code of Conduct, WithSecure upholds internationally recognised human rights standards, including the ILO Declaration on Fundamental Principles and Rights at Work and the OECD Guidelines for Multinational Enterprises. WithSecure ensures compliance

with labour laws, fair wages, non-discrimination, and the provision of safe working environments.

WithSecure does not tolerate any use of child labour, any form of forced labour or any other human rights violations including human trafficking. WithSecure supports the fundamental human rights to good working conditions, and reasonable balance between working hours and leisure time for everyone. To support these commitments, the company has implemented policies such as anti-harassment and anti-discrimination policies, local health and safety policies, and a remote work policy, as well as strategies and guidances like the Well-being, Inclusion, Diversity, and Equity (WIDE) strategy, and rewarding and learning philosophies to ensure compliance and promote a positive workplace culture.

WithSecure has implemented employee feedback systems and grievance mechanisms to identify and mitigate human rights risks. These mechanisms, discussed further under "[S1-3 Processes to remediate negative impacts and channels for own workforce to raise concerns](#)," allow employees to report issues confidentially and ensure timely, fair resolution.

WithSecure is committed to preventing discrimination in all its forms, including but not limited to race, gender, age, disability, sexual orientation, religion, and ethnicity, and the company promotes equal access to career development, fair treatment, and protection from harassment. The company's harassment prevention policy includes clear reporting procedures. Employees can raise concerns with their line manager, HR, or Legal representatives, ensuring that incidents are promptly addressed. Disciplinary action is taken where necessary, and WithSecure complies with local laws and regulations requiring additional procedures to prevent discrimination.

To foster a safe and healthy working environment, WithSecure has begun developing a new global comprehensive health and safety policy, which includes a workplace accident prevention policy and management system. This system, set to be implemented in 2025, is designed to minimize risks, reduce workplace accidents, and ensure a safe environment by identifying, managing, and mitigating hazards that could lead to injuries, illnesses, or fatalities. These initiatives, along with remote work policies, collectively support the physical and mental well-being of employees worldwide.

S1-2 Processes for engaging with own workforce and workers' representatives about impacts

WithSecure actively engages with its employees across all levels of the organization to ensure their voices are heard and integrated into decision-making processes.

The company maintains open communication channels that encourage feedback and provide opportunities for meaningful participation in decision-making processes related to workplace conditions and organizational goals.

WithSecure has established regular touchpoints through various platforms:

- **Electing an employee to the Board of Directors:** Each year, WithSecure employees can apply to become a representative on WithSecure's Board of Directors. This employee will have the chance to directly convey feedback from the employees to the Board. Additionally, the elected representative will be invited to HR Board meetings, where issues affecting Finnish employees are discussed on a monthly basis.
- **Formal employee surveys:** These surveys allow WithSecure to gather feedback on critical employee engagement-related matters such as diversity and inclusion, career development opportunities and overall wellbeing. In 2024, WithSecure conducted these surveys two times. The survey results are discussed in various decision-making forums where also actions are planned: in the global leadership team, function and unit specific leadership teams and local management teams. There's a line manager guidance available to support discussing the results and plan actions also at the team level. The Objectives and Key Results framework is a transparent tool for documenting development priorities and actions.
- **Employee Resource Groups (ERGs):** WithSecure's ERGs provide a space for employees from diverse backgrounds to share their experiences, collaborate on initiatives, and propose improvements related to our workplace culture and policies. In 2024, there were two active groups, one group focusing on wellbeing, inclusion, diversity, and equity (WIDE) related matters and one sub-group focusing specifically on mental health.
- **Feedback channels:** In addition to formal surveys, WithSecure's quarterly held company-wide and monthly held function and unit specific townhalls provide regular opportunities to ask questions and express any concerns, suggestions, or ideas. There are also regular monthly meetings for line managers to address any concerns, ask questions, and provide feedback. These meetings are recorded and accessible afterwards.

Additionally, as part of WithSecure's ongoing commitment to fostering a sustainable and inclusive work environment, ensuring excellent working conditions, and

retaining top talent, the company has initiated the development of a company-specific collective agreement in Finland in 2024. This agreement will reflect WithSecure's dedication to fair labour practices and ensures that the company's employees are treated with respect, fairness, and transparency.

By engaging in open dialogue with employee representatives, WithSecure has tailored the agreement to meet the specific needs of the company's workforce while aligning with technology industry standards. This initiative not only guarantees fair salary settlement but also promotes work-life balance, learning and development, and clearer working conditions.

Through this collaborative approach, WithSecure aims to foster a culture of mutual trust, ensure compliance with labour regulations, and contribute to the long-term sustainability of the workforce. The agreement marks a significant milestone in WithSecure's commitment to create a trusted workplace for employees and in the company's goal of being a preferred employer in the technology sector.

Operational responsibility for ensuring workforce engagement and incorporating the results into WithSecure's approach lies with the Chief Culture and Performance Officer, who holds the most senior role in this area. This individual leads the Operational Excellence function, driving initiatives to maintain meaningful engagement with the workforce and ensuring that feedback informs strategic decisions and policies effectively.

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

WithSecure is committed to fostering a supportive and transparent environment for its workforce, ensuring that negative impacts on employees are addressed in a timely and effective manner. WithSecure recognizes the importance of providing clear processes to remediate any adverse impacts the company's business may have on its employees and offering accessible channels for employees to raise concerns.

WithSecure's general approach to remediation involves investigating and addressing instances where the company has caused or contributed to material negative impacts on its workforce. The process includes conducting formal investigation to understand the underlying causes and the extent of the issue. This includes engaging with affected employees, gathering relevant information,

and consulting with relevant stakeholders to develop an appropriate course of action. To ensure the effectiveness of remedies and to evaluate satisfaction with the outcomes, WithSecure employs a feedback loop with the affected individuals.

WithSecure provides two channels for its workforce to raise concerns confidentially and without fear of retaliation. These include line manager and HR access, and whistleblower. Employees are first encouraged to engage directly with their line managers or HR representatives to discuss concerns and needs. A dedicated whistleblowing mechanism, managed by a third party, has been established to allow employees to report any unethical, unlawful, or harmful practices anonymously and without fear of retaliation. More information about the whistleblowing channel and whistleblowing policy can be found in the section "[Protection of whistle blowers](#)" under the section "[G1-1 Business conduct policies and corporate culture](#)".

In addition to the whistleblowing channel, WithSecure is in the process of developing a new grievance mechanism that will cater specifically to a broader range of employee concerns. This mechanism will provide employees with a structured and transparent avenue for raising concerns and ensuring that they are addressed promptly. The new channel will also help the company to track and monitor issues raised and addressed in a more systematic way. This channel is planned to be opened during 2025.

The available channels are designed to be easily accessible to all employees across the workforce.

S1-4 Taking action on material impacts on own workforce, and approaches to managing material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions

The company has implemented comprehensive initiatives to retain talent, to improve their well-being, promote diversity, equity, and inclusion (DEI), and provide equal opportunities for continuous learning and leadership development. These efforts include creating equal opportunities for continuous learning and leadership development, alongside strategic investments to build an inclusive and equitable workplace.

These initiatives cover a wide range of activities, including training programs, leadership development, and wellbeing and DEI initiatives. They extend across all

of WithSecure's locations globally, ensuring that employees in every region benefit from these initiatives. This global implementation ensures a consistent approach to training, leadership development, and DEI, while also allowing for regional adaptations to meet specific local needs and contexts. The scope of these efforts is WithSecure's own operations.

New investments in learning and development initiatives

WithSecure aims to increase the total hours spent on learning compared to the previous year, demonstrating its commitment to fostering continuous growth, providing meaningful development opportunities, and retaining talent.

In 2024, WithSecure introduced the LinkedIn Learning platform to all employees, reinforcing the company's commitment to continuous growth and development. This platform provides curated content aligned with strategic capabilities, supporting employees in developing skills critical to business success. Regular monitoring of course participation ensures that the platform is actively leveraged. WithSecure plans to intensify its use in 2025.

Leadership development remains as another core focus in this area. The values-based leadership program continues to be a cornerstone, supplemented by an expanding leadership development portfolio.

The effectiveness of these initiatives is assessed through employee engagement surveys. These efforts encompass the entire workforce and are integrated into general operations, with no significant additional expenditures allocated to their implementation.

Support line managers in having individual development discussions

WithSecure aims for 90% of employees to have defined and documented personal development goals, promoting tailored growth opportunities. Line managers are supported through resources and training to conduct meaningful individual development discussions. The formal bi-annual discussions ensure equal access to growth opportunities while addressing employees' unique needs.

The effectiveness of this action is assessed by gathering employee feedback on development discussions conducted as part of the personal development plan process. This effort encompasses the entire workforce and is integrated

into general operations, with no significant additional expenditures allocated to its implementation.

Driving diversity and promoting gender balance in leadership

The focus is on enhancing the representation of female leaders among line managers and maintaining gender balance and nationality diversity within senior leadership roles. To achieve these targets, WithSecure has enhanced its WIDE strategy through a newly developed DEI dashboard, enabling data-driven management discussions to promote diversity across all levels. Additionally, a dedicated taskforce organizes initiatives throughout the year to strengthen DEI awareness and action.

The effectiveness of this initiative is measured through quarterly monitoring to ensure progress and alignment with the targets. It applies to the entire workforce and is embedded within general operations, requiring no significant additional expenditures.

Gender pay gap analysis to be conducted with the regular 2025 salary review process

WithSecure has established a goal to reduce the gender pay gap to a maximum of 5% by the end of 2027. To achieve this, the company will conduct a comprehensive gender pay gap analysis during the regular 2025 salary review process. This analysis will take into account geographical differences and job grading structures to ensure a nuanced and equitable approach. The initiative applies to the entire workforce and is integrated into general operations, requiring no significant additional expenditures.

WithSecure remains committed to systematically driving positive outcomes through these efforts, proactively addressing potential risks and mitigating any negative impacts to ensure sustainable progress.

S1-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities

The effectiveness of these learning and development initiatives is assessed through employee engagement surveys and by tracking the utilization rates of mental health

and learning resources. Feedback gathered through surveys and other channels is used to identify and implement timely, targeted actions throughout the year. More details about how WithSecure engages directly with its own workforce or workers' representatives in tracking the undertaking's performance and in identifying any lessons or improvements as a result of this performance can be found from the section "[S1-2 Processes for engaging with own workforce and workers' representatives about impacts](#)".

The new Diversity and Inclusion dashboard will offer insights into representation metrics, enabling ongoing progress monitoring and the identification of further actionable opportunities. It will also help the company identify any possible gaps and biases in hiring and promotions, mitigating risks of inequity.

In 2025, WithSecure is committed to continuing improving employee retention by prioritizing enhanced working conditions and promoting equal treatment and opportunities for all. The WIDE taskforce continues to serve as a key driver of well-being and DEI initiatives. An example future action is a series of well-being webinars planned for the year to support all members of WithSecure's workforce.

Additionally, recognizing the critical role of skills development in maintaining a competitive edge, WithSecure remains dedicated to addressing skill gaps and nurturing leadership potential across the organization. In 2025, the company plans to launch a SaaS Academy as a key initiative to support its ongoing transformation. The academy focuses on reskilling and upskilling employees, ensuring that the company's workforce has the necessary capabilities aligned with WithSecure's strategy.

The targets related to these measures are increasing the total hours employees spent on learning from the previous year. Additionally, it is followed that 90% of employees have personal development goals defined and documented.

WithSecure has also established clear, outcome-oriented, and time-bound targets to reduce negative impacts, advance positive impacts, and manage material risks and opportunities within its workforce. These targets reflect the company's commitment to fostering a learning culture, promoting diversity, and ensuring equal opportunities for all employees.

The baseline values for these targets are the 2024 reportable figures. No scenarios were used to define the targets. These targets are not science-based.

Gender Balance Among Line Managers: By the end of 2027, WithSecure aims to increase the representation of women among line managers across the company. This target reflects the company's commitment to gender equity in leadership roles and ensures that decision-making processes are enriched by diverse perspectives.

Diversity Among Senior Leaders: WithSecure is committed to maintaining diversity among senior leaders, with a particular focus on maintaining both the number of nationalities represented and the proportion of female leaders within this group. This target emphasizes the importance of cultural and gender diversity in driving innovation and broadening the leadership perspective.

Gender Pay Gap: The company is committed to reducing the gender pay gap to a maximum of 5% by the end of 2027, focusing specifically on eliminating any unjustifiable differences in pay. This target underscores WithSecure's dedication to equitable compensation practices.

The process for setting these targets involved members of company's senior leaders, and the WIDE taskforce was consulted during the identification and validation of these targets. Insights from employee feedback channels were used to ensure that the targets reflect the workforce's priorities and expectations.

WithSecure's performance against these targets is tracked through quarterly reporting, and the company regularly evaluates progress to identify areas for improvement. Lessons learned from the company's performance are incorporated into future goal setting to ensure continuous progress.

These initiatives reflect WithSecure's commitment to advancing positive impacts on the company's workforce, reducing any negative impacts, and managing material workforce-related risks and opportunities in alignment with WithSecure's broader sustainability program.

S1-6 Characteristics of the undertaking's employees

The data represents employee characteristics as of the end of the reporting period, measured by headcount regardless of employees' full-time or part-time designation.

During the reporting period, a total of 270 employees left the company, resulting in a turnover rate of 26.5 %. The turnover rate is calculated by dividing the total number of employees who left during the reporting period by the average number

of employees employed during that same period. Our voluntary employee turnover rate is 16.2 %. The higher total turnover rate is a result of the operating model change and related reorganization in late 2023.

The disclosed total employee figures correspond to those in the most representative workforce-related section of WithSecure's financial statements for the reporting period, ensuring alignment between sustainability and financial disclosures.

Employees by contract type, broken down by gender (headcount)

	Continued operations					Discontinued operations				
	Female	Male	Other	Not disclosed	Total	Female	Male	Other	Not disclosed	Total
Number of employees	200	526	3	1	731	62	167	1	1	230
Number of permanent employees	196	522	3	1	723	61	167	1	1	229
Number of temporary employees	4	4	0	0	8	1	0	0	0	1
Number of non-guaranteed hours employees	2	0	0	0	2	0	2	0	0	2
Number of full-time employees	193	519	2	1	715	60	160	1	1	222
Number of part-time employees	7	7	1	0	15	2	7	0	0	9
Number of contractors					120					38
Number of employees under 30 years old	23	63	0	0	86	10	48	1	0	59

Employee head count in countries where the undertaking has at least 50 employees representing at least 10% of its total number of employees.

Country	Number of employees (head count) on 31.12.2024	Continued operations	Discontinued operations
Finland	441	384	57
United Kingdom	164	75	89
Poland	86	86	0
Malaysia	84	84	0

S1-7 Characteristics of non-employees in the undertaking's own workforce

WithSecure classifies non-employee workers into three groups based on their roles and contracts.

- Contingent workers are self-employed individuals operating through their own companies, providing services under tailored agreements aligned with WithSecure's standards.
- Consultants through frame agreements are professionals employed by larger firms with group-level agreements, offering resources and expertise while adhering to WithSecure's policies.
- Non-information workers (no IT access) are workers under group-level agreements who perform operational roles without needing IT tools, governed by security-focused contracts.

At the end of the reporting period, WithSecure's workforce included 158 non-employees, reported in headcount. This figure is based on the total number of non-employees at that time. When tracked and monitored monthly during the year 2024, the number of non-employees ranged from a minimum of 104 to a maximum of 160, based on the status at the end of each month.

S1-8 Collective bargaining coverage and social dialogue

WithSecure is committed to ensuring that the terms and conditions of employment for its workforce are shaped by fair and inclusive processes, fostering a positive work environment and sustainable business practices.

42.6 % of WithSecure’s total employees were covered by collective bargaining agreements during the reporting period. This percentage is due to the collective bargaining agreement in place for employees in Finland, where coverage is 92.7 %. Employees in other locations are not covered by collective bargaining agreements. WithSecure supports its employees’ rights to organize and engage in collective bargaining, where applicable under local laws and practices.

WithSecure aligns with internationally recognized labour standards and is dedicated to maintaining open dialogue with employee representatives to address workplace matters collaboratively. However, the company does not collect information on whether its employees are members of any labour unions to respect their privacy and uphold principles of non-discrimination and neutrality regarding union membership.

WithSecure does not have any agreements in place for employee representation through a European Works Council (EWC), a Societas Europaea (SE) Works Council, or a Societas Cooperativa Europaea (SCE) Works Council.

Like described under the section S1-1, WithSecure is strengthening collective bargaining coverage and social dialogue to foster a sustainable and inclusive work environment. In 2024, in Finland, WithSecure began developing a company-specific collective agreement, ensuring fair labour practices and treating employees with respect and transparency. By collaborating with employee representatives, the company has tailored the agreement to address workforce needs and industry standards, covering areas such as salary, work-life balance, and career development. This initiative supports mutual trust, regulatory compliance, and long-term workforce sustainability, reinforcing WithSecure’s commitment to being a trusted, preferred employer in the technology sector.

Collective bargaining coverage and social dialogue

Coverage Rate	Collective Bargaining Coverage		Social Dialogue
	Collective Bargaining Coverage - Employees (EEA)	Collective Bargaining Coverage - Employees (Non-EEA)	Social Dialogue - Workplace Representation (EEA Only)
0 - 19%			
20 - 39%			

Coverage Rate	Collective Bargaining Coverage		Social Dialogue
	Collective Bargaining Coverage - Employees (EEA)	Collective Bargaining Coverage - Employees (Non-EEA)	Social Dialogue - Workplace Representation (EEA Only)
40 - 59%	Finland		
60 - 79%			
80 - 100%			

S1-9 Diversity metrics

WithSecure is committed to fostering a diverse and inclusive workforce.

Senior leaders at WithSecure includes the CEO and the two organizational layers directly below the CEO, along with leaders holding specific job grades. At this level, 45 individuals are represented, with 33.3 % women and 64.4 % men. These figures are calculated based on the total number of individuals in top management and their respective gender distribution.

Regarding the overall workforce distribution, 15.1 % of employees are under 30 years old, 70.0 % are between 30 and 50 years old, and 14.9 % are over 50 years old. These percentages are derived from the total number of employees and their age groups.

S1-10 Adequate wages

All WithSecure employees are paid an adequate wage, aligned with applicable benchmarks. The company conducts annual salary reviews, utilizing relevant external global benchmarks to assess and implement any necessary adjustments. This process ensures that wages remain adequate for all employees, in line with market standards, and are consistently adjusted to reflect changing economic conditions, ensuring fairness across the entire workforce.

S1-11 Social protection

WithSecure ensures that all its employees are covered by social protection against the loss of income due to sickness, unemployment, employment injury and acquired disability, and parental leave. This coverage is provided either through public social protection programs or through benefits offered by the company.

- **Sickness:** All employees are covered and have access to healthcare and support in case of illness.
- **Unemployment:** In the event of unemployment, WithSecure is committed to providing support for reemployment, including partnerships with external organizations during company restructuring.
- **Employment Injury and Acquired Disability:** Employees are covered by insurance and appropriate social programs that ensure income security in the event of injury or disability incurred during employment.
- **Parental Leave:** WithSecure provides paid parental leave to all employees to support them during family-related events.
- **Retirement:** All employees are covered for income security in retirement, either through public pension programs or employer-sponsored private benefit plans, depending on the country.

WithSecure is committed to ensuring comprehensive social protection for its employees, fostering financial security and well-being during critical life events. By providing coverage through public programs or company-offered benefits, WithSecure upholds its responsibility to support employees across all regions.

S1-12 Persons with disabilities

WithSecure does not collect information on employees' disabilities, reflecting its commitment to inclusivity and non-discrimination. This approach is consistent with the General Data Protection Regulation (GDPR), which emphasizes safeguarding personal data and protecting privacy.

By refraining from collecting sensitive information such as disability data, WithSecure minimizes potential privacy risks and ensures compliance with GDPR's principles of data minimization and purpose limitation. Instead, the company fosters an inclusive work environment through proactive initiatives and policies that support diversity and equal opportunity.

S1-13 Training and skills development metrics

WithSecure provides equal opportunities for everyone to learn, grow, and succeed, with a strong focus on increasing employee engagement and retaining top talent. This commitment is crucial for attracting and retaining talent, as well as maintaining high competence levels within the organization. WithSecure believes that continuous learning and professional development are vital for both individual and organizational success.

WithSecure's learning philosophy is grounded in the 70-20-10 model, a widely recognized framework for effective skill acquisition. By integrating this approach, the company empowers its employees to learn dynamically, fostering an environment where real-world application and collaboration are prioritized alongside structured learning.

In 2024, WithSecure has placed a strong emphasis on upskilling activities that align with the company's strategic capabilities. These focus areas include leadership development, artificial intelligence, Software-as-a-Service, customer success management, and partnership management. By honing these essential skills, WithSecure is preparing its workforce for the evolving demands of the industry and ensuring that the company's employees are equipped to navigate the complexities of today's business landscape.

To further enhance learning opportunities, WithSecure has introduced LinkedIn Learning as a valuable resource accessible to all employees. Also, non-employees who have access to company resources are provided an access to this learning platform. LinkedIn Learning offers a vast array of courses across various topics, enabling WithSecure's workforce to pursue their interests and develop new skills at their own pace. With thousands of learning modules available, the company's employees can customize their learning journeys, fostering a culture of self-directed growth and continuous improvement.

WithSecure also remains committed to the company's values-based leadership program that is designed to cultivate leaders who not only excel in their roles but also embody the values and principles that define WithSecure. By focusing on values-driven leadership, WithSecure creates a cohesive and motivated leaders that inspire and guide the company's people toward shared goals.

Supporting career development is another critical aspect and WithSecure recognizes that line managers play a vital role in this process, which is why the

company has trained them to conduct meaningful development talks with their team members. These discussions empower employees to set personal development goals and create tailored plans that align with their aspirations. By fostering open communication and providing guidance, WithSecure ensures that its employees feel supported in their career growth and are equipped to reach their full potential.

During the reporting period, WithSecure followed the company management's plans by conducting both a performance review and a career development review for each employee. 75.9 % of employees participated in the annual performance review conducted during the first quarter of the year. This participation rate, when broken down by gender, was 74.8 % for women and 76.5 % for men. 78.8 % of employees participated in the annual career development review conducted during the third quarter of the year. This participation rate, when broken down by gender, was 72.9 % for women and 81.4 % for men. The participation rates are calculated based on the completion of the review task by employees' line managers in the performance management tool, using the employee headcount at the end of the reporting period.

To further support employee development, the average number of training hours per employee was 6.3 , with women averaging 6.4 hours and men averaging 6.3 hours. These figures include a combination of training hours logged through virtual and in-person courses recorded in the learning management system, as well as hours spent on the other available learning platform. Additionally, WithSecure encourages ongoing learning by providing opportunities for both individuals and teams to engage in external training programs. Notably, the hours dedicated to these external training opportunities are not included in the reported averages.

A key metric tracked by WithSecure to assess the effectiveness of its development programs is employees' perception of having opportunities to learn and grow within the company. In the most recent employee engagement survey, 73% of respondents agreed or strongly agreed that they had sufficient opportunities for learning and growth.

Training and skills development metrics

Data point	Female	Male	Other	Not disclosed	Total
Average Hours of Training per Employee	6.4	6.3	7.4	8.6	6.3
Percentage of Employees Participating in Regular Performance and Career Development Reviews (Leading Performance)	74.8 %	76.5 %	50.0 %	50.0 %	75.9 %
Percentage of Employees Participating in Regular Performance and Career Development Reviews (Personal Development Plans)	72.9 %	81.4 %	50.0 %	0.0 %	78.8 %

S1-14 Health and safety metrics

WithSecure is deeply committed to the health, safety, and wellbeing of its workforce, recognizing that the company's success is intrinsically linked to the wellbeing of its employees. The company adheres rigorously to all local regulations and requirements in every country where it operates, ensuring that its health and safety management system is comprehensive, robust, and effective. Currently, all workers are covered by local health and safety practices. This commitment will be formalized through a new global health and safety policy, which will be published in early 2025. The policy ensures that 100% of employees are covered by the health and safety management system that is regularly reviewed and updated to ensure its effectiveness and ensure continuous improvement. Local policies will align with applicable local laws and legislation. It reflects WithSecure's proactive approach to fostering a safe, supportive, and inclusive workplace, going beyond mere compliance with legal standards.

WithSecure's WIDE strategy includes not only physical health and safety measures but also mental health support programs to ensure the holistic wellbeing of employees. These programs include self-care tips, access to community support networks, and resources to address mental health challenges, making it a core part of the company's health and safety framework.

During the reporting period, three workplace accidents were reported. The information was gathered from employees responsible for recording workplace accidents within their respective regions. All reported incidents were thoroughly reviewed and investigated internally, with necessary procedures implemented to ensure compliance with safety regulations. This process supports accurate documentation and comprehensive analysis of workplace safety.

In accordance with the ESRS standard, WithSecure has exercised its option to omit data on cases of work-related ill health and the number of days lost to injuries, accidents, fatalities, and work-related ill health during the first year of preparing its sustainability report.

Table: Health and safety incidents

	Employees	Non-employees
Number of recordable work-related accidents	2	1
Number of cases of recordable work-related ill health	N/A *	N/A *
Number of fatalities as a result of work-related injuries and work-related ill health	0	0
Number of days lost to work-related injuries and fatalities from work-related accidents, work-related ill health and fatalities from ill health	N/A *	N/A *

* WithSecure has chosen to use the transitional provision related to omitting the data points on number of cases of work-related ill-health and on number of days lost to injuries, accidents, fatalities and work-related ill health for the first year of preparation of its sustainability report.

S1-15 Work-life balance metrics

WithSecure is committed to supporting its employees' work-life balance, ensuring that everyone in the workforce has access to family-related leave and benefits that help accommodate family needs. The company offers a range of family-related leave entitlements, including parental leave, paid compassionate leave, and flexible working arrangements, which are essential components of WithSecure's approach to creating a supportive and inclusive work environment.

Entitlement to Family-Related Leave

100% of WithSecure employees are entitled to take family-related leave, including parental leave, paid compassionate leave in the event of the death of a close family member, and flexible working arrangements. The percentage of entitled employees who took family-related leave is calculated based on records in the HR system, which is used to document all absences.

WithSecure provides flexible working arrangements that allow employees to manage family-related matters, such as flexible hours and remote work options. The company also has a remote work policy and a remote work abroad policy to further support employees in balancing work and personal commitments.

Utilization of Family-Related Leave

WithSecure ensures that all employees are entitled to take family-related leave and is committed to fostering a workplace where everyone feels equally supported in utilizing these benefits. Utilization rates are monitored through the HR system, which records the number of employees taking family-related leave and the types of leave utilized.

Work-life balance metrics

Indicator	Female	Male	Other	Not disclosed	Total
percentage of employees entitled to take family-related leave	100	100	100	100	100
percentage of entitled employees that took family-related leave	15	10	0	0	11

S1-16 Compensation metrics (pay gap and total compensation)

WithSecure is committed to promoting equal pay and reducing pay disparities across its workforce. To provide further transparency and ensure alignment with its principles of fairness and equity, the company will start monitoring key remuneration metrics, including the gender pay gap and the ratio between the highest paid individual and the median remuneration of its employees during 2025. WithSecure takes a proactive approach to managing compensation and ensuring fairness

across its workforce. The company uses global benchmarks and industry standards to assess and adjust compensation regularly.

Gender Pay Gap

The gender pay gap at WithSecure is calculated as the percentage difference between the average pay levels of female and male employees, expressed relative to the average pay level of male employees. To ensure comparability, the annual salaries of employees who work part-time have been adjusted to full-time equivalent figures. In addition to base pay, the analysis includes short-term incentives and sales incentives at their target levels for eligible individuals. The short-term incentive program is provided equally to all employees at certain job grades, while the sales incentive plan applies to everyone in sales roles. Long-term incentive plans are not included in this calculation. As of the most recent reporting period, the gender pay gap at WithSecure stands at 16.2 %. The company has consistently prioritized addressing potential gender pay disparities, considering factors such as geographical differences and job grading structures. WithSecure remains committed to fostering pay equity by regularly reviewing and refining its compensation practices to support fairness and inclusivity.

Total Remuneration Ratio

WithSecure also discloses the ratio of the remuneration of the highest-paid individual to the median total remuneration of all employees (excluding the highest-paid individual). This ratio for the current reporting period is 7.2. The annual total remuneration is calculated as a combination of base salary, the target-level payout for short-term incentives (STI), and the target-level payout for sales incentives, where applicable. Additionally, the monetary value of the actual long-term incentive (LTI) payouts made in 2024 is included. The calculation is based on 961 employees, representing the global workforce of WithSecure as of the end of 2024. The median remuneration is determined by averaging the total remuneration of the two employees situated at the midpoint of the remuneration distribution.

S1-17 Incidents, complaints and severe human rights impacts

WithSecure is committed to maintaining a respectful, inclusive, and safe work environment for all employees. All complaints of discrimination, harassment, or any form of workplace misconduct are taken seriously, and grievance mechanisms in

place to ensure that all employees have the opportunity to raise concerns in a safe and confidential manner.

During the reporting period, five (5) complaints were filed through these mechanisms, which were handled with due diligence and in compliance with WithSecure’s company policies. This figure is calculated based on the records maintained by the HR department and includes all complaints received through formal mechanisms. All complaints were thoroughly investigated in accordance with WithSecure’s internal grievance procedures, with appropriate actions taken to address the concerns raised. The investigation process involves a detailed review of each complaint by the HR team, interviews with relevant parties, and documentation of findings and actions taken. No incidents of discrimination, including harassment, were reported, no severe human rights violations were identified and no fines, penalties, or compensation payments were incurred during the reporting period. WithSecure remains committed to continuously monitoring, enhancing, and reinforcing its policies and procedures to foster a respectful, inclusive, and ethical work environment.

Discrimination and Human Rights Incident Metrics

Metric	Value
Number of Incidents of Discrimination	0
Number of Complaints Filed Through Channels for Workforce to Raise Concerns	5
Total Amount of Fines, Penalties, and Compensation for Damages Due to Incidents of Discrimination (Including Harassment and Complaints)	0
Number of Severe Human Rights Issues and Incidents Connected to Own Workforce	0
Total Amount of Fines, Penalties, and Compensation for Severe Human Rights Issues and Incidents Connected to Own Workforce	0

ESRS S4 - Consumers and end-users

SBM-3 Material impacts, risks and opportunities related to consumers and end-users

S4 Consumers and end-users

Material impacts	Material risks and opportunities	Stakeholder view
Information related impacts for consumers and end-users		<p>Very relevant. Protecting customer data through strong data security and privacy is an obvious expectation of the stakeholders for a cyber security company.</p>
<p> WithSecure's largest impact on sustainability comes from the work on building and supporting digital society, through its customers and end-users. WithSecure's value chain enables a well-working digital society, and therefore creates widespread positive impacts. Operating in the cyber security sector means being trusted with access to the customers' data. Maintaining a good level of data privacy of the customers is of utmost importance to WithSecure.</p>	<p> WithSecure's core business revolves around cyber security. An opportunity for us is that we are able to meet the many needs of our end-users. For example, there are several opportunities for being a European-based company compared to the majority of the American competitors, with the European privacy related legislation and requirements. Our business model also enables the offering of holistic and flexible services. End-user feedback received directly or through channel partners is an important source of developing products.</p>	
	<p> WithSecure faces risks from security and privacy perspective, as the company can be an attractive target for malicious activities. The potential repercussions for WithSecure could be significant, as WithSecure's entire existence is built on ensuring security for its end-users. Major security or privacy incident would cause reputational damage and loss of revenue. The likelihood of such risks materializing is limited.</p>	
	<p> As a European company, the high requirements in European legislation for diligent consumer and end-user privacy practices incur additional investments.</p>	

 — Positive impact / Financial opportunity
  — Negative impact / Financial risk
  — No material impact, risk or opportunity identified

WithSecure is in the business of providing software and related cyber security services. WithSecure has identified the material impacts, risks and opportunities related to business conduct based on the double materiality assessment introduced in its own section “[SBM-3 Material sustainability-related impacts, risks and opportunities](#)”. The ESRS sub-topic of “Information related impacts for consumers and end-users” and specifically the sub-sub-topic of “Privacy” was recognised as of importance.

As WithSecure provides services to other companies, the scope of interest in the S4 standard covers the end-users of WithSecure’s software and services, as WithSecure has no offering to consumers. These end-users have been identified as the employees of WithSecure’s customer companies.

WithSecure operations have a major positive impact on society through its end-users. The positive implications of WithSecure’s core business of enabling a well-working digital society and the related privacy and cyber security considerations are significant. This positive impact has been assessed to materialize in short term in the downstream value chain.

On the other hand, these same topics are also associated with both financial risks and opportunities for WithSecure. The opportunity of answering to end-user’s needs

as well as the risk of increased investment needs due to developing legislation have been assessed to materialize in the short term, while the risk of being a target for malicious activities has been assessed as a medium-term risk.

As WithSecure is in the business of cyber security, the privacy and security of the personal data related to the end-users trusted in the company’s care is of utmost importance. Mitigating significant impacts on end-users is integrated into the strategy and business model of WithSecure by constantly elevating the company’s privacy and security posture to minimize the risk of data breaches. Simultaneously, a strong cyber security posture is essential for WithSecure and thus WithSecure’s own related processes and assets have a fundamental role in elevating the internal security posture. It is also important to recognize that security is a prerequisite of privacy, one cannot fully exist without the other.

These topics are strongly linked to WithSecure’s core business. The interests, views, and rights of WithSecure’s end-users are key drivers of the company’s strategy. WithSecure’s business model is built on understanding and addressing the needs of its end-users. By prioritizing these aspects, WithSecure ensures that its products and services are aligned with the expectations and requirements of those it serves. This alignment not only enhances customer satisfaction but also strengthens the company’s market position and long-term sustainability.

Topic	Policy	Action	Metric	Target	2024 Status
The identified material topic	The policies related to handling/mitigating that topic	The actions related to handling/mitigating that policy	The metrics used to measure the action	The target related to the identified metric	Where WithSecure is in terms of the target
ESRS S4 "Consumers and end-users"					
Information related impacts for consumers and end-users	<i>Privacy:</i> Personal data policy Privacy Strategy Personal Data Breach Management processes GDPR processes	Awareness raising about privacy and cyber security, including informing employees	Mandatory employee privacy training completion rate	95% for new employees	93% for new employees
			Cyber security awareness training completion rate (annually mandatory)	90% for all employees	92% for all employees
				95% for new employees	100% for new employees
				90% for all employees	96% for all employees
	<i>Cyber security:</i> Cyber Security Principles Lifecycle Security Policy Information Security Classification Policy Acceptable Use Policy Access Control Policy Baseline Security Policy Business Continuity Management Policy	Internal controls and policies kept up to date	Number of major security incidents according to NIS2 directive	No incidents	No incidents
			Maintaining achieved certification	ISO 27001 certification achieved annually	Achieved for 2024

S4-1 Policies related to consumers and end-users

End-users are at the heart of WithSecure's privacy and security processes, due to the information-related impact WithSecure is able to exert. Due to this impact, WithSecure has a set of policies guiding the company's information related conduct. WithSecure has separate policies for cyber security and privacy related matters. The most senior level accountable for the implementation of these policies are the GLT members of each business unit most closely associated with the respective policy.

WithSecure's privacy principles together with the WithSecure Personal Data Policy make up the basic pillars of WithSecure's privacy practices. WithSecure's privacy principles are available on the company's website.

WithSecure's first and foremost privacy principle reiterates the data minimisation principle that the company only asks for personal data if it is needed to serve the customer. WithSecure also carefully partners with service providers who share the

company's commitment to privacy and security. These principles are there as a reminder of the basic privacy principles relevant for WithSecure's business and ultimately ensure compliance with relevant applicable laws and regulations and to ensure and respect data protection as a fundamental right, more specifically ensuring the right to privacy of WithSecure's end-users. WithSecure also adheres to the data protection principles set out in the GDPR. To ensure privacy by design these principles are reiterated in the WithSecure Personal Data Policy.

The policies related to privacy are designed to respect the privacy of WithSecure's end-users while allowing the use of personal data for the delivery of the company's services. For example, WithSecure does not take into use any tools or offer services without having conducted a robust privacy impact assessment, if the tool or service is used to process personal data. The WithSecure Personal Data Policy is reviewed annually at a minimum and updated when needed. As per the WithSecure Privacy Strategy the privacy processes and documentation are meant to be as simple as

possible to maximise compliance scalability, so that each individual employee can uphold the level of privacy expected from employees of a cyber security company.

WithSecure's policies related to consumers and end-users ensure that WithSecure's operations and value chain activities align with the company's commitment to sustainability, privacy, and human rights. By integrating these principles into both upstream and downstream activities, WithSecure aims to create a positive impact across its entire value chain, fostering a culture of responsibility and ethical conduct.

For upstream impacts in the value chain, WithSecure conducts supplier assessments and reviews that they abide by WithSecure's standards of business conduct. This is described in more detail in the section "[G1-2 Management of relationships with suppliers](#)". In terms of own operations, WithSecure provides comprehensive training to employees on data protection and privacy, ensuring they handle data responsibly. Downstream activities involve delivering services to end-users, maintaining privacy and security practices, and engaging with customers to address any concerns. To support both up- and downstream activities, WithSecure regularly reviews and updates its privacy and security policies to reflect the latest regulatory requirements and industry best practices.

Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis. WithSecure has considered the interests of key stakeholders, including employees, customers, suppliers, and investors, in the formulation of its policies. This was achieved through for example discussions to gather their input and ensure their concerns are included and addressed. For example, WithSecure conducted stakeholder meetings to collect feedback on privacy and security practices, which were then incorporated into the policy development processes. Thus, the stakeholders have been involved and their views have been included in the policy.

WithSecure ensures that all its employees are aware of and comply with its internal policies by including them in the mandatory onboarding process and as part of mandatory trainings. All policies are accessible to WithSecure employees for example in WithSecure's intranet and any changes to them are communicated group wide. Certain policies are also publicly available. Especially policies relevant to affected stakeholders, such as the Code of Conduct and Whistleblowing policy, are readily available on WithSecure's website. More information about these can be found in the section "[G1-1 Business conduct policies and corporate culture](#)". In terms of third parties, WithSecure ensures compliance with relevant internal policies by including them in the contractual framework as appendices to agreements. All

WithSecure policies are regularly reviewed and monitored to ensure compliance and identify areas for improvement. These measures help ensure awareness of and adherence to the policies.

In respect to human rights regarding WithSecure's policies in general, WithSecure is committed to honouring internationally recognized human rights standards as is outlined in the company's Code of Conduct. No severe human rights issues and incidents connected to WithSecure's end-users have been reported within WithSecure's own operations, where the UN Guiding Principles on Business and Human Rights, the ILO Declaration on Fundamental Principles and Rights at Work, or the OECD Guidelines for Multinational Enterprises would not have been respected.

As a software and services provider, WithSecure has limited capabilities of impacting the human rights of its end-users. This is primarily because WithSecure's products and services are designed to support business operations rather than directly interact with individuals in a way that could affect their fundamental rights.

In case of any observed discrepancies in the downstream value chain, the end-users can engage with WithSecure through various channels, including public-facing contacts and direct internal contacts. These have been detailed in the section "[S4-2 Processes for engaging with consumers and end-users about impacts](#)".

WithSecure's privacy related principles, policies and standards related to the identified material impacts, risks and opportunities are:

Personal Data Policy

WithSecure continuously assesses the impact of privacy regulations in its operations and identifies key regulatory requirements arising from them. This policy addresses the requirements by implementing relevant compliance processes and controls.

Compliance with data protection principles is ensured for example by the privacy impact assessment process.

This policy applies to all employees and contractors at WithSecure or any of its subsidiaries. The policy is reviewed annually, where stakeholder consideration and feedback can be implemented.

Privacy Strategy

This document aims to outline the main focus areas for WithSecure's privacy management activities, and specify a common ambition level and risk appetite for all WithSecure privacy activities.

The primary audience for the policy are all employees whose duties require an understanding of the company's strategic privacy ambitions.

The policy is reviewed regularly, where stakeholder consideration and feedback can be implemented.

Personal Data Breach Management Process

This process describes how suspected personal data breaches are reported, investigated and notified to the authorities and data subjects.

The policy applies to all employees at WithSecure. The policy is reviewed annually, where stakeholder consideration and feedback can be implemented.

GDPR Process

The purpose of this document is to describe WithSecure's internal process regarding the handling of data subject requests to comply with its obligations and ensure fulfilment of data subject rights as set out in the GDPR.

All employees at WithSecure need to be aware of the process. The functions/employees that need to abide by the process are Customer Care, GDPR Coordinators, system owners and Managers.

WithSecure's cyber security related principles, policies and standards related to the identified material impacts, risks and opportunities are:

Cyber Security Principles

Cyber Security Principles defines the objectives of cyber security management, roles and responsibilities, and the principles for the implementation of those objectives. The document applies to all employees and any third parties that have access to WithSecure data.

To ensure the fulfilment of WithSecure's cyber security objectives, the management of information security integrated to the mandate of WithSecure Chief Information Security Officer (CISO). The CISO reports to the CEO and the Audit Committee of the Board of Directors. Software security is led by the Chief Architect who reports to the Chief Product Officer (CPO). Privacy is led by the Data Protection Officer (DPO) who reports to the Chief Legal Officer (CLO).

Cyber Security Principles is reviewed after major changes in the company direction, strategy or organization.

Lifecycle Security Policy

Lifecycle Security Policy (LSP) ensures that privacy and security requirements are covered within all products and services throughout the states of the lifecycle: design, development, and operation.

The policy includes requirements such mandatory access control analysis, threat modelling and privacy impact analysis (In case of a system processing personal information).

This policy applies to all systems, products, and services used and sold by WithSecure. The policy is reviewed annually, where stakeholder consideration and feedback can be implemented.

Information Security Classification Policy

Information Security Classification Policy describes the requirements for processing information throughout its lifecycle. It provides rules on how to classify the information and how the information is to be accessed, stored, transferred, and destroyed per the classification. The classification has four levels: public, internal, confidential and restricted access documents.

The policy applies to all employees, temporary staff, consultants, contractors, and suppliers working for, or on behalf of the company, who have access to any company information. The policy is globally applicable and applies to any location where information assets can be found or accessed from.

All company information assets have an owner. The owner is responsible for proper classification of information. The owner and their seniority vary per information asset. The policy is reviewed annually, where stakeholder consideration and feedback can be implemented.

Acceptable Use Policy

Acceptable Use Policy defines the acceptable use of the company information and other assets. It includes information security requirements for example for remote and mobile work, removable media use, taking assets off-site, usage of external services as well as the clear desk and screen policy.

This policy applies to all employees, temporary staff, consultants, contractors, and suppliers working for, or on behalf of the Company and have access to any Company information systems and assets. This is globally applicable and applies to any location where the information systems and assets reside or are accessible from.

Personnel are responsible for keeping the devices, and the company's information systems and assets safe. The policy is reviewed annually, where stakeholder consideration and feedback can be implemented.

Access Control Policy

This policy defines rules for accessing applications, systems, equipment, networks, facilities, and information, based on business requirements. It describes how users authenticate to WithSecure systems and services, and how passwords are managed. The principles of access control are the rule of least privilege/need to know.

This policy applies to all employees designing, maintaining, and/or giving access to company applications, systems, networks or services. The policy is globally applicable. Every WithSecure employee is required to implement the Access Control Policy into their system management and operation. The principles of access control are the rule of least privilege/need to know.

The policy is reviewed annually, where stakeholder consideration and feedback can be implemented.

Baseline Security Policy

Baseline Security Policy describes the requirements for system operations. This policy defines requirements for as an example for operations security (such as vulnerability management, intrusion detection, anti-malware system, system hardening, backups), user access management (e.g. session security) and access control (e.g. limiting the access to management ports), usage of cryptography (e.g. encrypted connections), data protection (e.g. pseudonymization), Logging and monitoring.

The policy applies to all employees, temporary staff, consultants, contractors, and suppliers working for, or on behalf of the company, who and have access to any company information. The policy is globally applicable.

The policy is reviewed annually, where stakeholder consideration and feedback can be implemented.

Business Continuity Management Policy

Business Continuity Management Policy defines the principles for business continuity management at WithSecure, including roles and responsibilities and objectives. It also describes the business continuity management framework where the foundation is the company risk management, followed up with the business analysis of the main threads stemming from the risk management activity and the preparation measures as business continuity and recovery plans. The policy also sets the requirement for annual review/training/testing of the recovery plans.

The policy is intended for employees responsible for business continuity management and disaster recovery and implementation of related practices at the company. The policy is reviewed annually, where stakeholder consideration and feedback can be implemented.

S4-2 Processes for engaging with consumers and end-users about impacts

WithSecure's end-users' perspectives have been integrated into impact, risk and opportunity management holistically. The end-users of WithSecure's software and service were interviewed as part of the stakeholder interviews conducted for the double materiality analysis.

The end-users have been involved and their views have considered in identifying the material impacts, risks and opportunities related to them and in managing these aspects. An extensive analysis of the perspectives of WithSecure's partners and customers was conducted during the double materiality analysis. Stakeholder views and feedback were thoroughly investigated and integrated into WithSecure's operations. These perspectives inherently included the views of the end-users they represent.

In terms of ongoing engagement between WithSecure and end-users, there are feedback and engagement channels available that for example WithSecure's partners can use to engage in dialogue or that the software and service end-users can use to send in feedback through the support services provided. The sales function at WithSecure is particularly committed to delivering the feedback from the company's end-users and making sure that their concerns and needs are met.

The publicly available privacy policies provide access to support channels. For certain privacy and cyber security related internal policies, there is a WithSecure Trust Center-website, where the end-users can validate requests for security evidence. There is also separate contact information available for the end-users to be in contact directly with WithSecure's data protection officer. In terms of privacy specifically, WithSecure has a customer support channel for privacy and data subject related requests and a data subject access (DSAR) process which sets out the process for any data subject request made by end-users or their representatives. The whistleblowing channel is an engagement channel also available for everyone, including WithSecure's end-users.

S4-3 Processes to remediate negative impacts and channels for consumers and end-users to raise concerns

As general approach to contribute to remedy identified negative impacts for end-users in instances where they have raised concerns, WithSecure has a customer care and support channel in place. These channels enable a timely response to concerns flagged by WithSecure's end-users.

The responsibility receiving end-user feedback and engaging in dialogue is shared across various departments at WithSecure, including sales, customer service, and specific contacts for privacy and other matters. This ensures comprehensive engagement and timely delivery of key information to end-users, enabling prompt internal decision-making.

In terms of information security, monthly Information Security Management System (ISMS) meetings are held to report relevant security and privacy matters to upper management. This process ensures that appropriate and timely actions can be taken to address potential negative impacts for WithSecure's end-users.

There are several internal functions and senior roles connected to these engagements. For example, the CISO office representative presents a monthly operational review. Here the monthly privacy reports, concerns and activities are assessed. The CISO reports to the Board's Audit Committee twice a year. In these instances, the CISO gives an overview of the then current situation, including possible – if any – material incidents and risks impacting security and privacy in the company. The Data Protection Officer (DPO) reports a privacy overview (including the current state of WithSecure's privacy posture) to the Security Steering Group

once per year. This group includes the Global Leadership Team (GLT) and convenes on quarterly basis.

As part of the continued work to building the end-users' awareness and trust in WithSecure's data protection efforts and commitment to transparency, WithSecure has in place engagement methods that can be accessed by publicly available privacy policies and privacy principles. As a method to increase trust, WithSecure has a whistleblowing channel managed by a third party. This also ensures a level of protection against retaliation. More information about the whistleblowing channel and whistleblowing policy can be found in the section "[Protection of whistle blowers](#)" under the section "[G1-1 Business conduct policies and corporate culture](#)".

S4-4 Taking action on material impacts on consumers and end-users, and approaches to managing material risks and pursuing material opportunities related to consumers and end-users, and effectiveness of those actions

The main actions through which WithSecure is able to mitigate possible negative impacts and risks while simultaneously maintaining possible externalities from positive impacts and opportunities is through raising awareness internally and externally as well as keeping chosen policies and certifications up to date. One of the aims of these actions is to avoid causing or contributing to negative impacts on WithSecure's end-users through its own practices. By maintaining employee awareness and up-to-date operational practices, these impacts can be minimized. As WithSecure operates in the cyber security industry, the interest in staying on top of these matters is shared by the business while simultaneously being closely connected to the interests of WithSecure's stakeholders, including WithSecure's end-users.

WithSecure is committed to increasing privacy awareness and supporting its partners and end-users in a privacy and cyber security perspective. This includes maintaining privacy and cyber security awareness of WithSecure's workforce. The awareness raising through dedicated trainings is continuous. Mandatory trainings on Privacy and Cyber Security Awareness are a part of the onboarding process of new employees. Retaking the Cyber Security Awareness training annually is mandatory to all employees. No significant expenditures are allocated for these trainings, as they are considered to be a part of general operation.

The DPO arranges additional internal privacy trainings on an ad hoc basis with focus on specific business units or internal functions for WithSecure employees. Any WithSecure employee that manages tools, products or services that are used to process personal data, are expected to complete a privacy impact assessment training. The completion of these trainings is followed to ensure compliance.

As mentioned, keeping internal controls and policies up to date is another action WithSecure engages in to manage the identified material impacts, risks and opportunities. The scope is WithSecure's own operations. The internal controls and policies are continuously managed. They are reviewed as needed, most of them at least annually. WithSecure has in place privacy and security documentation, including internal policies and processes that are updated and reviewed on a regular basis. For identifying actions needed in the event of a suspected data breach, WithSecure has a dedicated personal data breach management process. No significant expenditures are allocated for the awareness raising or keeping chosen policies and certifications up to date, as they are considered to be a part of general operation.

S4-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities

For the Privacy training, the completion rate target is 90% for all employees and 95% for new employees. For the annually mandatory Cyber Security Awareness training the completion rate targets are similarly 90% for all employees and 95% for new employees. A full 100% is not always attainable, as due to possible issues with statistics and reporting systems as well as personnel changes and leaves of absence, an error margin of sorts has to be tolerated.

The awareness raising about Privacy and Cyber Security Awareness is measured through following the completion rate of both of these trainings. The target for these metrics showcases the degree of which the employees have been made aware of the Privacy and Cyber Security Awareness related information and expected standard of operations at WithSecure. The target is a percentage and relative to the number of employees the company has. The measured unit is number of employees who have completed these trainings.

The targets' scope are all persons working for WithSecure, anywhere WithSecure operates. The targets are measured continuously, and the rate is reviewed at

least annually. The Cyber Security Awareness training completion rate is reported internally on a monthly basis. These completion rates are available directly from the training platform. Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis. Thus, the stakeholders have been involved and their views have been included in the setting and choosing of the targets.

The baseline values for these targets are the 2024 reportable figures. Milestones and interim targets include reviewing the stated target completion rates continuously, so that they are achieved at a minimum annually, and maintaining these rates at or above the targets in subsequent years. For the Privacy training, the completion rates for 2024 were 93% for new employees and 92% for all employees. For the Cyber Security Awareness training the completion rates for 2024 were 100% for new employees and 96% for all employees. The performance is in line against the target for the cyber security training and very close to target for the privacy training. The training completion rates have stayed at appropriate levels. This indicates that WithSecure's efforts to maintain high training completion rates are quite effective, enhancing compliance and security awareness within the company. WithSecure explores methods to improve the privacy training completion rate during the year 2025.

The status of the internal controls and policies being kept up to date is measured through the number of major security incidents WithSecure has faced during the year as well as whether WithSecure has maintained achieved cyber security certifications and assurance statuses. In terms of the major security incidents, they are categorized as major according to NIS2 directive requirements.

The target showcases the degree of which the company has been able to avoid significant cyber security incidents, indicating proper cyber security management and measures. The measured unit is an absolute amount of major cyber security incidents that WithSecure has faced during the fiscal year. The target's scope is WithSecure operations. The target is measured continuously, at least annually. Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis. Thus, the stakeholders have been involved and their views have been included in the setting and choosing of the targets. The target is no major incidents. Performance is in line with the target, as there were no major security incidents during the year 2024. The incidents are categorized as major according to NIS2 directive requirements.







For the cyber security certification action, the metric is that the achieved certification is maintained. In particular, it is expected that WithSecure receives the globally recognised ISO 27001 certification that is audited annually by an external party. The target demonstrates how well WithSecure's conduct aligns with internationally recognised ISO 27001 certification, indicating compliance with a specific standard for information security management systems. The target is to maintain the ISO 27001 certification annually. The measurement unit is whether the certification is upheld or not. This target applies to selected WithSecure operations and is monitored continuously, with at least an annual review. Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis. Thus the stakeholders have been involved and their views have been included in the setting and choosing of the targets. Performance is in line with the target. The ISO 27001 certification was maintained for the year 2024.

Governance information

ESRS G1 - Business conduct

SBM-3 Material impacts, risks and opportunities related to business conduct

G1 Business conduct

Material impacts	Material risks and opportunities	Stakeholder view
Corporate culture		<p>Relevant. Stakeholder expectation is that there are no governance or ethics issues. This issue, however, is universal and not WithSecure specific.</p>
<p> The potential impacts on corporate culture are relatively limited, due to the high level of expectations for companies in the software and service sector.</p>	<p> Corporate culture is important as the related privacy risk is heightened compared to other industries as its potential impact on reputation is significant.</p>	
Protection of whistleblowers		
<p> WithSecure has established a confidential and secure whistleblowing channel, enabling anonymous reporting of any concerns of misconduct. The channel is maintained by an impartial external party. In a multi-cultural working environment, involving thousands of end-customers, this is an essential element of good governance.</p>	<p> Risks and opportunities are limited due to the safeguards taken for the protection of whistleblowers. See more in section "Whistleblowing policy"</p>	
Management of relationships with suppliers including payment practices		
<p> WithSecure wants to conduct its business to a high ethical standard. The aim is to maintain a positive impact on its supply chain through emphasis on ethical business practices. These impacts can be quite widespread, as they extend into the entire value chain and can therefore also impact the company's suppliers and partners.</p>	<p> Maintaining strong supplier management processes and best practices requires investments, incurring possible additional costs.</p>	

 — Positive impact / Financial opportunity
  — Negative impact / Financial risk
  — No material impact, risk or opportunity identified

WithSecure has identified the material impacts, risks and opportunities related to business conduct based on the double materiality assessment introduced on its own section "[SBM-3 Material impacts, risks and opportunities related to business conduct](#)". The ESRS sub-topics of "[Corporate culture](#)", "[Protection of whistleblowers](#)" and "[Management of relationships with suppliers including payment practices](#)" were identified as material topics for the company.

Impact-wise. WithSecure is able to exert a positive impact on business conduct through well-managed business practices and safeguards, such as the company's whistleblowing channel. WithSecure has a positive impact on supplier management, through the company's emphasis on ethical business practices. Both of these positive impacts are present throughout the value chain and the impacts are identified to materialize in the short term.

WithSecure has not identified any material financial opportunities related to business conduct. The company believes that the positive effects of its business conduct are primarily external, as indicated by the material positive impacts.

Here the company sees that the positive implications of the company’s business conduct are more external, as the identified material positive impacts indicate.

The possible business conduct-related financial risks the company could face are related to corporate culture and supplier management. The implications of privacy risk and its impact on WithSecure’s reputation are heightened due to the industry the company operates in. This risk has been identified to impact the company in the short term. The other material financial risk pertains to supplier management and the investments that proper and ethical supplier practices require. This second risk has been assessed to occur in the medium term.

Topic	Policy	Action	Metric	Target	2024 Status
The identified material topic	The policies related to handling/ mitigating that topic	The actions related to handling/ mitigating that policy	The metrics used to measure the action	The target related to the identified metric	Where WithSecure is in terms of the target
ESRS G1 "Business conduct"					
Corporate culture	Code of conduct	Awareness raising about ethical business practices, including informing own employees	Mandatory employee Code of Conduct training completion rate	95% for new employees	100% for new employees
	Personal Data Breach Management Process			90% for all employees	95% for all employees
	Anti-bribery policy		Mandatory employee privacy training completion rate	95% for new employees	93% for new employees
	Remuneration Policy			90% for all employees	92% for all employees
Modern Slavery Statement					
Insider Policy					
Export Control Policy					
Protection of whistleblowers	Whistleblowing policy	Awareness raising about whistleblowing channel, including informing own employees	Mandatory employee Code of Conduct training completion rate	95% for new employees 90% for all employees	100% for new employees 95% for all employees
Management of relationships with suppliers including payment practices	Corporate procurement policy	Awareness raising about ethical supplier management, including informing own employees	Periodical supplier management reviews held with strategically significant suppliers	Held at least annually	Held during the year 2024

G1-1 Business conduct policies and corporate culture

WithSecure has determined a set of policies that are applied to the company’s conduct and complied with, for mitigating the identified material risks and emphasising the identified positive impacts. These integral policies are reviewed and accepted by the administrative and supervisory bodies after the inspection and approval of individuals from the management body. If there is a specific senior level accountable for the implementation of the specific policies, this is presented in the policy description. An in-depth description of the general role and expertise of the

administrative, management and supervisory bodies is included in the [“General information”](#) section under the topic [“GOV-1 – GOV-5 Sustainability governance”](#).

Several of the policies are publicly available, to ensure that WithSecure’s stakeholders have access to the information guiding WithSecure’s business conduct practices.

Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis.

Thus, the stakeholders have been involved and their views have been included in the policy.

The most senior level accountable for the implementation of these policies are the GLT members of each business unit most closely associated with the respective policy.

WithSecure has not identified any specific functions at risk. All new WithSecure employees are subject to a vetting process conducted by a third party. The scope of the vetting will be determined by the role and rights that the role has.

To ensure ethical business conduct from as many perspectives as possible, WithSecure has procedures to investigate business conduct incidents, which follow the same methodology as the whistleblowing channel. More information about the whistleblowing channel and whistleblowing policy can be found in the section "[Protection of whistle blowers](#)".

Information about possible instances of unethical business conduct, such as instances related to corruption and bribery or whistleblowing reports of unethical conduct, are relayed to WithSecure's Board of Directors through outcome reviews once per month, or more frequently is necessary. The process follows the same structure of procedure and recommended actions as the whistleblowing instances. When there is an incident that requires a response, WithSecure has an investigation process. There is no internal investigating body, but rather when suspicious activities are flagged, WithSecure engages in audit and assurance processes with external service providers.

In terms of procedures to promptly, independently, and objectively investigate business conduct incidents, WithSecure's Audit Committee considers the need for and appropriateness of a separate Internal Audit function on a regular basis. To date, the Audit Committee has concluded that, due to the size, organizational structure and largely centrally controlled financial management of the company, a separate Internal Audit function is not necessary. In the absence of an Internal Audit function, attention is paid to periodical review of the written guidelines and policies concerning accounting, reporting, documentation, authorization, risk management, internal control and other relevant matters in all departments. Related controls are also tested annually. The guidelines and policies are coordinated by the company's finance department with active involvement by the legal department.

WithSecure also has specific mechanisms in place to prevent corruption and bribery. One of the methods is monitoring expenditure related details. The company has a comprehensive invoice and payment management processes in place, to detect any attempted wrongful usage. Proper and comprehensive invoice management is in an important role. Another method for preventing, detecting and investigating possible acts of corruption or bribery is the whistleblowing channel that is discussed later in this section of the report under "[Protection of whistle blowers](#)".

There have been no confirmed incidents of corruption or bribery, nor any related convictions or fines in 2024.

The main action for WithSecure to both remediate and mitigate the identified material risks while simultaneously promoting and emphasizing the positive impacts, is through raising awareness both internally to own employees as well as externally to stakeholders and other interested parties. This includes information related to both ethical business conduct as well as the protection of whistleblowers. The expected outcome of these actions is to create a well-informed workforce that understands and adheres to ethical business practices, thereby reducing risks and enhancing positive impacts. The awareness raising is continuous process that manifest in short, medium and long term. WithSecure maintains these actions through a selection of methods.

In terms of corporate culture and whistleblowing protection, one of the key methods for raising awareness is through the company's Code of Conduct and related mandatory training. The Code of Conduct sets the high-level aims and ethical business standards that the company complies with. It also includes a dedicated section about the whistleblowing policy and whistleblowing channel for raising awareness about the protection of whistleblowers. During the year 2024 the Code of Conduct and the related training were updated.

As privacy also appears in the material impacts risks and opportunities, WithSecure has implemented a mandatory privacy training for all employees. More information about the mandatory privacy training is presented in the S4 section "[S4-4 Taking action on material impacts on consumers and end-users, and approaches to managing material risks and pursuing material opportunities related to consumers and end-users, and effectiveness of those actions](#)".

All employees are required to complete these trainings. The Code of Conduct training is also completed by the Board of Directors. There are additional trainings for specific functions or groups related to other relevant policies, such as the export

control policy related training. The financial resources for these actions are a part of general operations, with no significant expenditures related to sustainability specified. Other resources include the time and effort of WithSecure's internal experts. The costs are absorbed within the overall operational budget and are not separately itemized for sustainability purposes.

The awareness raising about ethical business practices and whistleblowing channel are measured through following the completion rates for the mandatory Code of Conduct and Privacy trainings. The completion rates for these trainings are available directly from the training platform. The training completion rate results are aggregated to show the completion rates of new employees and all employees. The expected outcome of these trainings is comprehensive training coverage across all levels of the organization, indicating widespread awareness and understanding of the company's ethical and privacy standards and ensuring that everyone is equipped with the necessary knowledge to uphold the company's standards.

Future actions will include regular updates to training materials and continuous engagement with employees and stakeholders to ensure ongoing awareness and adherence to these principles. This includes periodic reviews of the Code of Conduct and other relevant policies, along with updates to the related training materials. These efforts aim to address the emerging regulatory and internal policy changes, which will help in maintaining high standards of compliance.

Simultaneously in terms of employee engagement, a specific action continued in future periods is that the training completion rates are regularly monitored to ensure high level of participation and adherence. Additionally, WithSecure aims to enhance internal communication strategies to keep the company's employees informed about updates and changes to the policies and training materials. These planned actions are designed to support in achieving policy objectives by ensuring that all employees are continuously informed and educated about the company's ethical standards.

Regular updates and reviews will help the company to adapt to new challenges and regulatory requirements, while targeted training sessions will address specific risks and compliance needs, while simultaneously enhancing the positive impacts WithSecure is able to attain through their business conduct. Through these actions, WithSecure aspires to promote a culture of continuous improvement and proactive risk management, supporting the achievement of its policy objectives.

Other efforts to provide remedies include ensuring thorough investigations and responses to the negative impacts. This may include protection, possible compensation and remedies to those impacted, for example through the externally managed whistleblowing process.

In terms of the value chain coverage of these actions, WithSecure engages with suppliers and partners in the upstream value chain to ensure they are aware of and adhere to its ethical standards and privacy practices. This includes providing resources such as WithSecure's policies to support compliance and mitigate risks throughout the supply chain. Many of these policies include detailed guidelines for appropriate and acceptable business conduct. For the downstream value chain, WithSecure ensures that end-users are informed about the company's ethical standards and privacy practices through clear communication and feedback channels, including a specific contact persons for privacy matters. These efforts aim to extend the positive impacts of WithSecure's policies beyond the immediate organization.

One method for WithSecure to track the effectiveness of its business conduct related policies and actions specifically in relation to the material impacts, risks and opportunities, is through monitoring the completion rates for Code of Conduct training and the Privacy training. The company uses quantitative indicators to evaluate progress. The defined targets for tracking the effectiveness are set to ensure continuous improvement and alignment with industry best practices.

The methodologies used to define these targets include analysing historical training completion data and consulting with internal stakeholders. Significant assumptions made during target setting process include the availability of training resources, employee engagement levels and the reliability of the training platforms. No specific sustainability scenarios were used to define the targets.

These targets align with national, EU, and international policy goals by promoting ethical business conduct and data privacy, which are key components of regulatory frameworks, such as the EU GDPR. The targets also consider broader context of sustainable development by ensuring that all employees are equipped with the knowledge to uphold WithSecure's ethical standards and privacy practices, thereby contributing to a more responsible and sustainable business environment.

In terms of targets, WithSecure follows that the completion rates for both of these trainings are 95% for new employees and 90% for all employees. A full 100% is not attainable always, as due to possible issues with statistics and reporting systems as

well as personnel changes and leaves of absence, an error margin of sorts has to be tolerated. The scope of these targets is WithSecure's own workforce.

The target showcases the degree of which the employees have been made aware of the Code of Conduct and WithSecure's ethical business conduct principles. The target is a percentage and relative to the number of employees the company has. The measured unit is number of employees who have completed the Code of Conduct and Privacy trainings. The target's scope are all persons working for WithSecure, in all locations WithSecure operates. The target is measured continuously, and the rate is reviewed at least annually. These completion rates are available directly from the training platform.

Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis. Thus, the stakeholders have been involved and their views have been included in the setting and choosing of the targets.

The baseline values for these targets are the 2024 reportable figures. Milestones and interim targets include reviewing the stated target completion rates continuously, so that they are achieved at a minimum annually, and maintaining these rates at or above the targets in subsequent years. For the Code of Conduct training the completion rates for 2024 were 100% for new employees and 95% for all employees. For the Privacy training the completion rates for 2024 were 93% for new employees and 92% for all employees. The performance is in line against the target for the Code of Conduct training and very close to target for the privacy training. The training completion rates have stayed at appropriate levels. This indicates that WithSecure's efforts to maintain high training completion rates are effective, contributing to a well-informed and compliant workforce, supporting in ethical business conduct. WithSecure explores methods to improve the privacy training completion rate during the year 2025.

Corporate culture

In addition to the Code of Conduct, WithSecure has various other company-wide and role-based compliance trainings, as well as guidelines and policies to support the decision-making in different situations. Of these, the following policies have been identified as important for WithSecure's corporate culture in terms of the identified material impacts, risks and opportunities.

Code of Conduct

WithSecure's Code of Conduct's aim is to foster a culture that supports ethical conduct. The foundation of all activities at WithSecure is the Code of Conduct; it guides everything done at the company. It reflects the company's business culture for ethical conduct, sets clear expectations on business conduct, and provides guidance for critical risk areas.

WithSecure's Code of Conduct covers the following areas:

- Building and sustaining digital trust, confidence and equity
- Privacy and Security
- Intellectual Property Rights and Confidentiality
- Responsible use of A.I.
- Wellbeing, Inclusion, Diversity, and Equity (WIDE)
- Protecting Human Rights
- Sustainability
- No Bribery or Corruption
- Preventing Conflicts of Interest
- Securities Markets Compliance
- Trade Compliance
- Fair Competition
- Working with Responsible Suppliers
- Whistleblowing

The Code applies universally across the workforce, including employees, contractors, and business partners, ensuring adherence to consistent high ethical standards. Training and regular updates to the Code of Conduct are mandatory to ensure that everyone understands their responsibilities and the implications of non-compliance.

The Code of Conduct is publicly available on WithSecure's website.

Personal Data Breach Management Process

Please see section "[S4-1 Policies related to consumers and end-users](#)"

Anti-Bribery Policy

For fostering ethical business practices, WithSecure has committed to actions against corruption and bribery. The company's anti-bribery policy is consistent with the UN convention against corruption.

The anti-bribery policy covers situations of WithSecure's employees not giving or accepting gifts or hospitality that would exceed a certain level considered to be identifiable as corruption. An acceptable monetary level has been established.

The Anti-bribery policy applies to all persons working for WithSecure, anywhere WithSecure operates. The policy is available internally.

Insider Policy

WithSecure has prepared an Insider Policy aligned with the Insider Guidelines of NASDAQ Helsinki. Inside information is defined as: "Information of a precise nature, which has not been made public, relating, directly or indirectly, to one or more issuers or to one or more financial instruments, and which, if it were made public, would be likely to have a significant effect on the prices of such financial instruments or on the price of related derivative financial instruments".

The policy applies to all insiders. Anyone who has inside information is considered an insider, regardless of how the information has been obtained or whether the person has been included on a specific insider list. The policy is available internally.

Modern Slavery Statement

Through the Modern Slavery Statement, WithSecure is committed to ensuring that there is no modern slavery or human trafficking in its supply chains, employment practises, or in any part of the business. This is also apparent in the Code of Conduct, which all suppliers are required to abide by, that states that WithSecure does not tolerate any use of child labour, any form of forced labour or any other human rights violations. While the policy requires suppliers to pass on compliance and contractual requirements to their sub-contractors, WithSecure does not have the means to monitor the compliance of the sub-contractors or suppliers' suppliers directly.

The guidance available to employees reflects the commitment to acting ethically in business relationships and to implementing and enforcing effective controls that ensure slavery and human trafficking is not taking place.

The statement applies to all employees, temporary staff, consultants, contractors, and suppliers working for, or on behalf of the WithSecure. The policy is globally applicable. The statement is available to employees as well as both internal and external stakeholders. It is approved by the Board of Directors of the UK entity, WithSecure Limited.

Remuneration Policy

WithSecure's Remuneration Policy describes the remuneration for the Board of Directors and CEO and the considerations of determining the policy and operation of the policy. Remuneration Policy of WithSecure complies with the recommendations of the Finnish Corporate Governance Code for listed companies, Shareholders' Rights Directive legislation and any other regulations and guidelines concerning remuneration in listed companies.

Executive remuneration is designed to support business objectives and long-term profitability, based on performance and competencies. It aims to be competitive, foster commitment, and ensure consistency across the organization. WithSecure strives to offer market-level base salaries to attract and retain talent, with incentive schemes aligning with the interests of shareholders and key employees for strong performance and long-term value creation.

Employee remuneration is regularly reviewed to ensure fair compensation based on market standards, individual competencies, and performance. The CEO's remuneration follows the same principles as other employees.

The Remuneration Policy applies to all WithSecure employees and the Board of Directors. The Policy is available to employees as well as both internal and external stakeholders, as it is a public policy available on WithSecure's website. It is approved in the General Meeting is normally held once a year as an Annual General Meeting (AGM).

Export Control Policy

As WithSecure Corporation is registered in Finland, its technology and solutions are mainly exported to customers and end users from Finland, and thus the export control regulations of the European Union are the ones that are primarily relevant for WithSecure. Additionally, in many circumstances also United States' export control regulations and sanctions apply to the activities of WithSecure, including when selling products through US-based app stores or other distribution channels connected to the United States.

The main restrictions of the applicable export control laws and regulations are dual-use items and sanctions. Dissemination of dual-use items to destinations and persons outside the European Union (known as "export"), as well as in certain cases also within the European Union, has been regulated by the European Union export control laws. Distribution across borders from operators and servers located in the United States is in turn subject to US export control laws, and software developed in the United States often remains subject to US export control laws its entire lifecycle. Regulation (EU) 2021/821 of the European Parliament and of the Council ("EU Export Control Regulation") in particular is applied in the operations of WithSecure as is of the US Export Administration Regulations, 15 C.F.R. 730 et seq. (the "EAR"). The European Union and the United States have adopted restrictive measures (sanctions) which prohibit or restrict transactions with countries, companies, groups, organizations or individuals who are involved in malign behaviour, such as armed aggression, internal repression, human rights violations, or cyber-attacks. The sanctions may include arms embargoes, travel bans, asset freezes or other economic measures such as restrictions on imports and exports, including of various kinds of software products and related services.

This policy applies to all WithSecure employees, contingent workers and subcontractors globally. Special attention should be given to the content of this policy by anyone who works in connection with sales, product management, technical product management, R&D and IT/production systems. WithSecure continuously assesses the impact of export control and sanctions regulations in its operations and identifies key regulatory requirements arising from them. This policy addresses the requirements by implementing relevant compliance processes and controls. The policy is available internally.

Protection of whistle blowers

The protection of whistleblowers was identified as the second material sub-topic, making the whistleblowing policy an integral part of WithSecure's policies related to ethical business conduct, especially due to the possible positive impact the company is able to exert to the society. The whistleblowing channel functions as the main mechanism for reporting unlawful behaviour and managing business conduct incidents. The channel is available to both internal and external stakeholders.

Comprehensive information about the whistleblowing channel is readily available on the company intranet and is included as a core element of the Code of Conduct training. While the company does not actively monitor employees' trust in the channel, it ensures robust protections for whistleblowers.

Whistleblowing Policy

WithSecure's Whistleblowing Policy is an important tool in discovering undesirable conduct, such as corrupt or illegal conduct. WithSecure strongly encourages individuals to speak up if they suspect or witness any such behaviour, activities or conduct. WithSecure will take all reports made under this policy seriously

This Policy sets out how WithSecure provides individuals with an effective, objective, confidential and secure reporting channel, Whistleblowing channel, allowing them to express their concerns or suspicions openly and safely. On the Whistleblowing Channel the individuals are also advised how to make a report, how they are informed on the follow-up actions and how they are protected. WithSecure reviews the Policy and the Whistleblowing Channel from time to time in order to ensure their accuracy and proper and reliable functioning.

The breaches to be reported through the Whistleblowing Channel include actual or potential crimes, serious omissions or misconduct, as well as other breaches of the applicable laws and regulations.

The whistleblowing policy applies to all internal and external persons. An individual's right to report on the whistleblowing channel is unlimited and cannot be, for instance, restricted or waived by any agreement, policy or form or conditions of their employment. Summaries of the whistleblowing channel reports are reported to the Chief Legal Officer by the third party managing the channel. The Whistleblowing Policy is publicly available on WithSecure's website for all interested parties to see.

Whistleblowing Channel.

The main principles of WithSecure's whistleblowing channel prioritize confidentiality, anonymity, and impartial handling of reports. Employees are encouraged to report any unethical, unlawful, or harmful activities without fear of retaliation, as the channel ensures complete anonymity for those who choose to remain unidentified. All reports are handled with strict confidentiality by an independent team, ensuring that the identity of the whistleblower is protected throughout the process. The system guarantees a fair and transparent investigation, with follow-up provided to ensure appropriate action is taken while safeguarding the whistleblower's privacy.

Stakeholders can file a report on suspected breach and its potential perpetrator anonymously through WithSecure's Whistleblowing Channel.

All reports coming through the Whistleblowing Channel are confidential, meaning that WithSecure will protect and keep the whistleblower's identity and the identity of any third party possibly mentioned in the report confidential. The reporting service is entirely independent of the organization to ensure that it is impossible to find out who is behind a report.

After the report has been initially received and handled by the third-party Service Provider, the Service Provider may further report the case to at least two (2) representatives of WithSecure which are defined in the Whistleblowing Policy. The Service Provider will make the decision whether the report is further investigated and to whom at WithSecure such report is then delivered with the objective that there cannot exist any conflict of interest between the chosen representative of WithSecure, whistleblower and the person(s) mentioned in the report or related the possible breaches mentioned in the report.

The chosen representative(s) of WithSecure will decide on the required further investigations and actions to be taken by WithSecure. All such investigations and possible follow-up actions will be performed diligently and by preserving confidentiality. In case criminal activity is revealed, WithSecure will report it to the police. The Audit Committee will also receive regular reports on the whistleblowing process, including statistics and information on a general level on the reported topics, and depending on the case, may be involved in reviewing individual cases when it is deemed necessary.

Protection against retaliation

Whistleblowers will receive protection against retaliation, i.e. negative consequences, threats and attempts of retaliation that may result from the report if the conditions in the Whistleblowing Policy are fulfilled.

In short, the protection provided to eligible whistleblowers includes:

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

In addition to protection provided to the whistleblower, WithSecure provides protection also to person(s) who are suspected of having committed the Breach. Such protection includes, for instance that such person is treated in an equal and non-discriminating manner and the consequences of the Breach are based on WithSecure's policies and the applicable laws. Such person is also granted a possibility to review and comment the alleged Breach and the relevant material. Further, such persons may be entitled to compensation due to deliberate false report.

To ensure that WithSecure's employees stay informed about the Whistleblowing Channel, a section related to it and the whistleblowing policy are included in the mandatory Code of Conduct training.

G1-2 Management of relationships with suppliers

Supplier management was identified as a topic where WithSecure has a possible positive impact while simultaneously facing a possible financial risk. WithSecure is committed to ethical supplier practices. The company holds their suppliers to the same ethical standard.

At the centre for WithSecure's supplier management are a set of minimum requirements that all suppliers need to reach, the Corporate Procurement Policy. WithSecure requires all of the company's suppliers to be registered companies that abide by local laws. As an additional measure, the companies are also required to abide by WithSecure's Code of Conduct and other case by case determinable requirements related to for example data privacy and security. In terms of third-

party standards and initiatives that WithSecure commits to, the Code of Conduct includes commitment to local laws and regulations and the Ten Principles of the Un Global Compact, which cover areas such as human rights, labour standards, environmental protection, and anti-corruption.

Corporate Procurement Policy

The Corporate Procurement Policy outlines how supplier relationships are managed and goes more in depth into the need assessments in terms of suppliers.

It sets out the principles for purchase related responsibilities and gives guidance to persons and teams who may be able to assist in specific cases. WithSecure's aim is to achieve the best value (price, quality, service) for materials, goods and services the company purchases from the market. The company also wants to maintain the ethical standards and sustainability in dealing with the suppliers.

The scope of the policy includes all procurement activities within WithSecure's own operations. This encompasses all supplier categories, regardless of the suppliers' industry or geographic location. The policy applies to all stakeholder groups involved with procurement decisions including suppliers, partners, and internal teams. There are no specific exclusions mentioned in the policy, ensuring comprehensive coverage of procurement decisions. While the policy requires suppliers to pass on compliance and contractual requirements to their sub-contractors, WithSecure does not have the means to monitor the compliance of the sub-contractors or suppliers' suppliers directly. The policy is reviewed annually where possible updates based on feedback received from stakeholders, for example through periodical supplier management reviews held with strategically significant suppliers, can be integrated.

The business owners themselves have the direct responsibility over sourcing from suppliers. Their decisions are based on the corporate procurement policy. The initial assessment by the business owners is followed by steps that need to be taken with both the financial and legal departments, before any procurement decisions can be made. For major procurement decisions there is also an internal template that needs to be filled.

The corporate procurement policy is available internally to all WithSecure employees, enabling the maintaining of high-quality management of supplier relationships. It binds all employees.

For screening suppliers against sustainability-related risks, WithSecure uses several different platforms. Other risk mitigation actions that WithSecure takes is

limiting engagement to those suppliers that pass the internal cyber security review and overall scrutiny of appropriate business conduct. In the case of WithSecure this means abstaining from engaging with suppliers that do not meet WithSecure's data privacy and information security requirements. WithSecure follows that a set number of suppliers have been subjected to an information security auditing. Financial risks related to suppliers are monitored constantly.

WithSecure has not yet implemented an official internal supplier selection criteria related to social and environmental matters, beyond the requirement that the suppliers must abide by WithSecure's Code of Conduct and all local legislative requirements. In terms of social criteria this includes compliance with labour laws and human rights standards, as well as commitment to diversity, equity and inclusion, and ethical business practices. Correspondingly the environmental criteria consists of implementation of sustainable practices, adherence to environmental regulations and use of energy-efficient and eco-friendly materials and processes. The evaluation of the suppliers meeting these requirements is at the discretion of the business owners and the supporting financial and legal departments, when conducting the supplier selection process.

During the year of 2024, WithSecure has been further developing the internal risk screening process for supplier management. WithSecure is also in the process of developing further a supplier management policy to improve identification and managing of risks related to suppliers.

For mitigating the risks and emphasizing the positive impact of WithSecure's supplier relationship management, WithSecure has concluded that an effective measure is raising awareness about ethical supplier management, especially informing the company's own employees who are in supplier-facing roles. No significant expenditures are allocated for this action, as it is considered to be a part of general operation. The expected outcome of this actions is to create a well-informed workforce that understands and adheres to ethical supplier relationship management. The awareness raising is continuous process that manifest in short, medium and long term.

The awareness raising about ethical supplier management is measured through hosting periodical supplier management reviews held with strategically significant suppliers.

In terms of the value chain coverage of this action, WithSecure engages directly with suppliers in the upstream value chain. For WithSecure's this means ensuring that

suppliers adhere to the company's ethical business conduct standards and privacy practices. Simultaneously, the periodically conducted interviews with suppliers ensure, that their views are heard and addressed. These interviews provide a platform for suppliers to voice their concerns, share feedback discuss any challenges they might be facing. By engaging in this dialogue, WithSecure can better understand the suppliers' needs and support in building a collaborative relationship. Additionally, these interviews help in identifying issues requiring remedies, allowing WithSecure to take appropriate actions, such policy revisions to address the root causes or corrective actions to rectify issues, to address grievances and mitigate risks affectively

WithSecure tracks the effectiveness of its supplier relationship management related policies and actions specifically in relation to the material impacts, risks and opportunities through monitoring the completion of periodical supplier management reviews. The company uses qualitative indicators to evaluate progress. The defined targets for tracking the effectiveness are set to ensure continuous improvement and fostering stronger, more collaborative relationships with suppliers.

In terms of targets, WithSecure follows that these reviews are held at least annually. The target showcases the significance given to ethical management of relationships with suppliers. The target is a status relative to the amount of identified strategically significant suppliers that the company has. The measured unit is that periodical supplier management interviews are held with strategically significant suppliers at least annually. The scope of the target are strategically significant suppliers. The strategically significant suppliers are defined through their significance and their impact on WithSecure's operations, both in customer facing systems and internal operations, and the risks to WithSecure's operations and the company's ability to continue business without interruptions.

Stakeholder views were thoroughly investigated in the course of determining the material impacts, risks and opportunities for the double materiality analysis. This involved engaging with various stakeholders, including suppliers. Supplier engagement is the foundation for determining these determinants. For example, as part of WithSecure's ISAE 3000 certificate verification and audit process, the company needs to have a process for the main supplier management actions in the scope of the service. WithSecure has achieved this certificate for 2024. Thus, stakeholders are inherently involved in target setting and management.

The baseline value for this target is the 2024 status. Milestones and interim targets include reviewing the stated periodical supplier engagement continuously, so that

the annual minimum engagement target is achieved and maintained in subsequent years. For the year 2024, supplier management reviews were held with strategically significant suppliers. The performance is in line against the target. This indicates that WithSecure is effectively meeting its goal for supplier engagement, ensuring timely review of the suppliers' need. It demonstrates WithSecure's commitment to maintaining strong, collaborative relationship with key suppliers and continuously improving its supplier management practices.

times. From this information the proportion of payments made within 30 days can be determined.

Percentage of payments aligned with standard payment terms by main category of suppliers	58.52%
--	--------

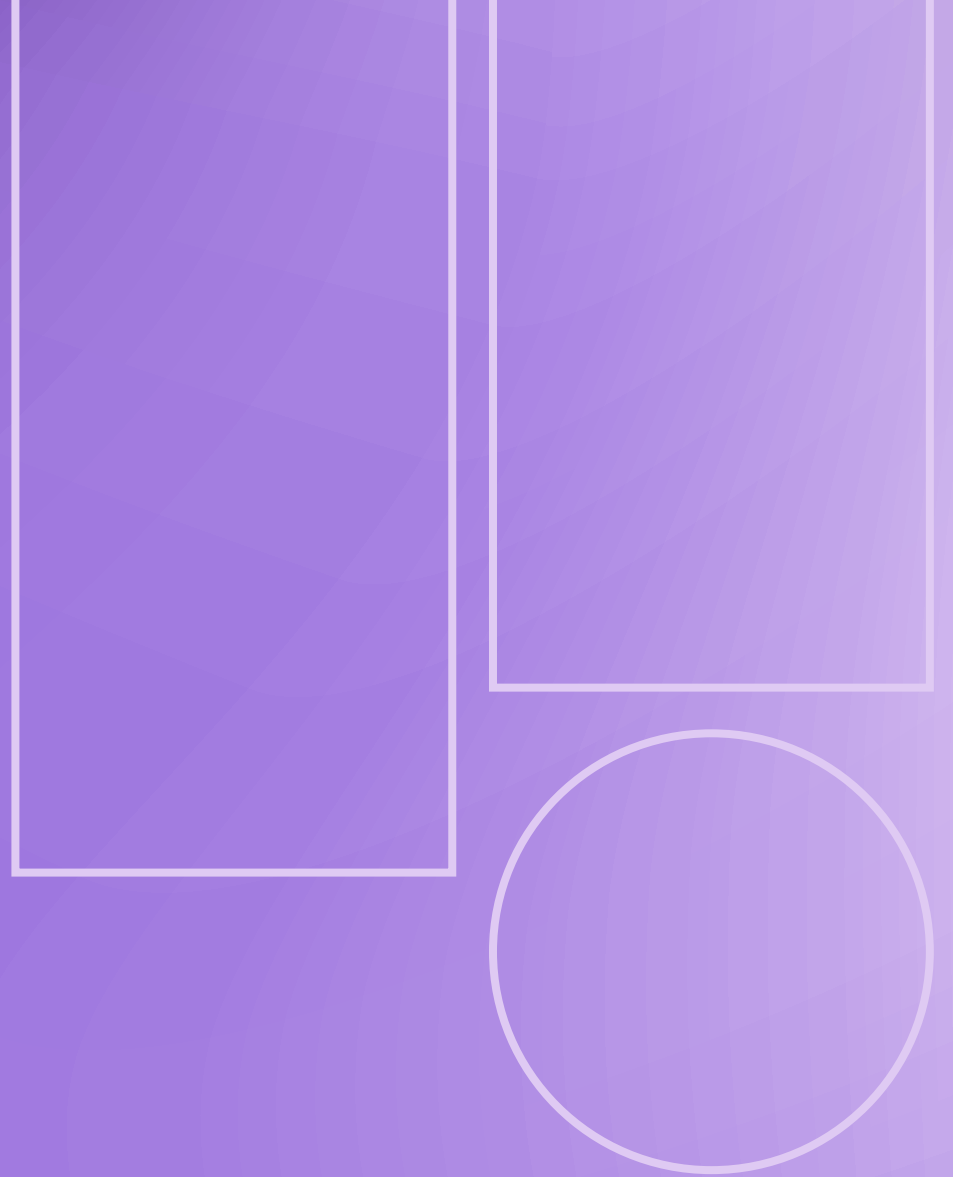
G1-6 Payment practices

WithSecure practises a Fair Payment Terms Policy which is WithSecure's Corporate Procurement Policy, to ensure transparent, fair, and sustainable payment practices that support the financial stability and growth of WithSecure's suppliers in all purchasing categories and supplier segments, particularly small and medium-sized enterprises (SMEs). Payments will be made within 30 days from the date of receipt of a valid invoice, unless otherwise agreed in writing.

Payment terms are applied consistently across different supplier categories and regions, ensuring fairness and transparency. There are no separate policies for small and medium-sized enterprises (SMEs), however some discretion is shown to small companies' payment terms on a case-by-case basis. The payment terms are a standard 30 days. The average time it takes to pay an invoice from the moment the contractual payment period begins is on average about 25 days for all invoices, and 24 days excluding intercompany invoices.

58.52% of payments adhere to the payment terms. This figure is influenced by WithSecure's set payment schedule, where invoices are paid once per week on a designated day. 70.76% of invoices are paid by or within a week from the due date. Some invoices were paid late due to various delays, such as late receipt or delays in approval process. These percentages also include intercompany invoices, which tend to be paid less frequently within payment terms, which affects the overall percentage. Additionally, WithSecure is working on improving the reporting process and the accuracy of this figure. There are no outstanding legal proceedings for late payments.

The percentage of payments aligned with standard payment terms can be derived from the invoice management data for the annual year as a whole. Representative sampling was not required, as the full data for the 2024 fiscal year can be analysed. This data includes detailed records of invoices received, their statuses and payment



WithSecure Group Consolidated Financial Statements

Statement of comprehensive income

January 1 - December 31, 2024

The income statement is presented for continuing operations only according to IFRS 5 as Consulting business is treated as discontinued operations.

EUR 1,000	Note	Restated		EUR 1,000	Note	Restated	
		Consolidated IFRS 2024	Consolidated IFRS 2023			Consolidated IFRS 2024	Consolidated IFRS 2023
REVENUE	2	116,002	109,939				
Cost of revenue	6	-23,416	-23,106	Comprehensive income for the year, continuing operations		-7,127	-30,821
GROSS MARGIN		92,585	86,832	Comprehensive income for the year, discontinued operations		-28,804	-7,891
Other operating income	3	3,249	9,735	COMPREHENSIVE INCOME FOR THE YEAR, GROUP		-35,931	-38,712
Sales and marketing	4,5,6	-51,772	-61,318	Result of the financial year is attributable to:			
Research and development	4,5,6	-40,092	-47,254	Equity holders of the parent, continuing operations		-9,175	-32,139
Administration	4,5,6	-14,054	-23,686	Equity holders of the parent, discontinued operations		-28,804	-7,891
EBIT		-10,083	-35,692	Equity holders of the parent, combined operations		-37,979	-40,030
Financial income	8	2,867	2,659	Comprehensive income for the year is attributable to:			
Financial expenses	8	-3,085	-2,147	Equity holders of the parent, continuing operations		-7,127	-30,821
PROFIT (LOSS) BEFORE TAXES		-10,301	-35,180	Equity holders of the parent, discontinued operations		-28,804	-7,891
Income tax	9	1,125	3,040	Equity holders of the parent, combined operations		-35,931	-38,712
Result for the financial year, continuing operations		-9,175	-32,139	Earnings per share:	10		
Result for the financial year, discontinued operations		-28,804	-7,891	Basic and diluted, continuing operations		-0.05	-0.18
RESULT FOR THE FINANCIAL YEAR, GROUP TOTAL		-37,979	-40,030	Basic and diluted, discontinued operations		-0.16	-0.04
Exchange difference on translation of foreign operations, continuing operations		2,049	1,319	Basic and diluted, combined operations		-0.22	-0.23

Statement of financial position December 31, 2024

ASSETS	Note	Consolidated	Consolidated
		IFRS	IFRS
EUR 1,000		2024	2023
NON-CURRENT ASSETS			
Tangible assets	4,13	23,999	13,032
Intangible assets	13	16,766	20,552
Goodwill	12	35,848	78,058
Deferred tax assets	19	12,115	10,682
Interest bearing receivables, non-current	17	4,188	6,059
Other receivables	17	1,100	1,866
Total non-current assets		94,015	130,249
CURRENT ASSETS			
Accrued income	17	1,261	5,577
Trade and other receivables	15,17	24,645	31,683
Income tax receivables	17	456	1,199
Interest bearing receivables, current	17	6,642	2,074
Other financial assets at FVTPL	17	26	26
Cash and cash equivalents	17	27,275	36,604
Total current assets		60,306	77,163
Assets held for sale	11	30,492	0
TOTAL ASSETS		184,814	207,412

SHAREHOLDERS' EQUITY AND LIABILITIES	Note	Consolidated	Consolidated
		IFRS	IFRS
EUR 1,000		2024	2023
SHAREHOLDERS' EQUITY			
	14		
Share capital		80	80
Treasury shares		-155	-155
Translation differences		1,244	-805
Reserve for invested unrestricted equity		83,638	83,638
Retained earnings		-15,575	20,222
Equity attributable to equity holders of the parent		69,233	102,980
NON-CURRENT LIABILITIES			
Interest bearing liabilities, non-current	4,17	20,653	8,370
Deferred tax liabilities	19	1,279	1,273
Other non-current liabilities		18,752	21,160
Total non-current liabilities		40,685	30,804
CURRENT LIABILITIES			
Interest bearing liabilities, current	4,17	6,042	5,366
Trade and other payables	17,21	14,320	18,034
Provisions	20	0	3,486
Income tax liabilities		407	620
Other current liabilities		43,704	46,125
Total current liabilities		64,473	73,631
Liabilities directly associated with the assets held for sale	11	10,423	0
TOTAL SHAREHOLDERS' EQUITY AND LIABILITIES		184,814	207,412

Statement of cash flows January 1 – December 31, 2024

EUR 1,000	Note	Consolidated	
		IFRS 2024	IFRS 2023
Cash flow from operations			
Result from continuing operations		-9,175	-32,139
Result from discontinued operations	11	-28,804	-7,891
Result for the financial year		-37,979	-40,030
Adjustments			
Depreciation and amortization	5	40,629	18,824
Profit / loss on sale of fixed assets	13	-134	-14
Financial income and expenses	8	370	-205
Income taxes	9	-1,823	-3,655
Other adjustments		1,015	231
Cash flow from operations before change in working capital		2,077	-24,849
Change in net working capital			
Current receivables, increase (-), decrease (+)	15	1,920	4,645
Non-interest bearing debt, increase (+), decrease (-)	21	1,787	-3,167
Provisions, increase (+), decrease (-)	20	-3,721	3,515
Cash flow from operations before financial items and taxes		2,063	-19,856
Interest expenses paid	8	-295	-314
Interest income received	8	901	1,474
Other financial income and expenses	8	-1,709	-1,985
Income taxes paid	9	-347	-2,383
Cash flow from operations		613	-23,063

EUR 1,000	Note	Consolidated	
		IFRS 2024	IFRS 2023
Cash flow from investments			
Investments in intangible and tangible assets	13	-5,929	-5,159
Divestments of businesses, net of cash	3	2,347	1,585
Investments in financial instruments	17	0	14,854
Cash flow from investments		-3,582	11,280
Cash flow from financing activities			
Repayments of lease liabilities	4	-6,443	-6,139
Cash flow from financing activities		-6,443	-6,139
Change in cash		-9,412	-17,921
Cash and cash equivalents at the beginning of the period	17	36,604	55,129
Effects of exchange rate changes		83	-604
Cash and cash equivalents at period end		27,275	36,604

Statement of changes in equity

Attributable to the equity holders of the parent.

EUR 1,000 IFRS	Note	Share capital	Treasury shares	Translation differences	Unrestricted equity reserve	Retained earnings	Total equity
Equity December 31, 2022		80	-155	-2,124	83,638	58,649	140,089
Result of the financial year, continuing operations		0	0	0	0	-32,139	-32,139
Result of the financial year, discontinued operations		0	0	0	0	-7,891	-7,891
Translation difference		0	0	1,319	0	0	1,319
Total comprehensive income for the year		0	0	1,319	0	-40,030	-38,712
Share based payments	16	0	0	0	0	1,603	1,603
Equity December 31, 2023		80	-155	-805	83,638	20,222	102,980
Equity January 1, 2024		80	-155	-805	83,638	20,222	102,980
Result of the financial year, continuing operations		0	0	0	0	-9,175	-9,175
Result of the financial year, discontinued operations	11	0	0	0	0	-28,804	-28,804
Translation difference		0	0	2,049	0	0	2,049
Total comprehensive income for the year		0	0	2,049	0	-37,979	-35,931
Share based payments		0	0	0	0	2,183	2,183
Equity December 31, 2024		80	-155	1,244	83,638	-15,575	69,233

More information in note [14 Shareholder's Equity](#)

Notes to the Financial Statements

Accounting principles for the consolidated financial statements

Basic information

WithSecure provides cyber security products and services globally for businesses.

The parent company of the Group is WithSecure Corporation, incorporated in Finland and domiciled in Helsinki. Company's registered address is Välimerenkatu 1, 00180 Helsinki. A copy of consolidated financial statements can be downloaded on www.withsecure.com or can be received from the parent company's registered address.

These financial statements were authorized for issue by the Board of Directors on 12 February 2025. According to the Finnish Companies Act, the Annual General Meeting can confirm or reject the consolidated financial statements after publication. The Annual General Meeting can also decide to change the financial statements.

Accounting principles

The consolidated financial statements of WithSecure Corporation of 2024 have been prepared in accordance with IFRS (International Financial Reporting Standards) accounting standards, applying the IAS and IFRS accounting standards as well as SIC and IFRIC interpretations that were in force and had been approved by the EU by 31 December 2024.

In accordance with the European Single Electronic Format (ESEF) reporting requirements, WithSecure has published the Board of Directors' report and the financial statements as an XHTML file. In line with the ESEF requirements, the primary statements of the consolidated financial statements have been labelled with XBRL tags, and the notes to the financial statements with XBRL block tags. XBRL tags are not audited.

Principles of consolidation

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

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

Discontinued operations

On 23 January 2025, WithSecure announced the decision to divest its cyber security consulting business. The transaction is executed by the sale of shares of the parent company of a to-be-established WithSecure cyber security consulting group, to which the consulting business will be transferred prior to the completion of the transaction. The transaction is expected to be completed during the second quarter of 2025. The completion of the transaction is subject to customary closing conditions and regulatory approvals.

WithSecure has applied the requirements of IFRS 5 Non-current Assets Held for Sale and Discontinued Operations in classifying, presenting and accounting for the consulting business in financial reporting. Result from discontinued operations is reported separately from continuing operations' income and expenses in the consolidated income statement. Comparative periods have been restated accordingly. On the balance sheet the net assets were valued at fair value less costs to sell and classified as assets held for sale on the balance sheet at 31.12.2024. Discontinued operation's financial information is presented in [note 11](#).

Transactions in foreign currency

The consolidated financial statements are presented in euros, which is WithSecure Corporation's functional currency. At each reporting date for the purpose of presenting consolidated financial statements the income statements of foreign Group companies are translated at the average exchange rates for the reporting period and the balance sheets are translated using the European Central Bank's exchange rates prevailing on the reporting date. Translation differences are recognized in shareholders' equity and the change in other comprehensive income.

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

New and amended IFRS accounting standards that are effective for 2024

During 2024 the Group has adopted the following new and amended Accounting Standards issued by the International Accounting Standards Board (IASB):

Amendments to IAS 1 Presentation of Financial Statements clarify that liabilities are classified as either current or non-current, depending on the rights that exist at the end of the reporting period. Classification is unaffected by the expectations of the entity or events after the reporting date. The amendments have no impact on the consolidated financial statements.

Other new or amended Accounting Standards already effective do not have a significant impact on the consolidated financial statements or other disclosures.

Management judgment on significant accounting principles and use of estimates

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

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

Key sources where estimation uncertainty arises at the reporting date are:

- **Impairment testing:** Recoverable amount of goodwill from acquisitions is based on estimated future cash flows which are subject to management judgment.
 - In addition to goodwill the intangible assets that are not yet ready for use are tested annually for impairment. The recoverable amount of these assets is based on estimated future cash flows from sales and/or use of the asset.
- **Deferred tax assets:** The Group has recognized deferred tax assets from tax losses and from temporary differences. The amount of deferred tax assets is based on management estimation about future profits and the recoverability of the tax losses.

Revenue recognition

From 1 January 2024 onwards, WithSecure Group has reported three segments: Elements Company, Cloud Protection for Salesforce (CPSF) and Cyber security consulting which is also reflected in the revenue reporting.

Elements Company segment includes Elements Cloud products and services, Managed services (including Countercept Managed Detection and Response, MDR), On-premise, and Other products. Elements Company revenue is presented separately for Cloud, On-premise and Other products.

Cloud Protection for Salesforce (CPSF) segment includes revenue from the CPSF product. It is a software product, ensuring scanning of external content for potential malware, before it is loaded into Salesforce. Customers are primarily enterprise-sized companies, with extensive use of Salesforce platforms.

Cyber security consulting segment includes the consulting services sold to large enterprise customers. On 23 January 2025, WithSecure signed an agreement intending to divest the Cyber security consulting business. In the Segment information note of 2024 financial statement, Cyber security consulting segment

is presented according to the calculation principles applied in the 2024 segment reporting. In other parts of the 2024 financial statements, Cyber security consulting is presented as part of the Discontinued operations. Reconciliations between the segment result and the discontinued operation's result are presented in the Segment information note.

Cloud-based Elements products and services, Managed services and CPSF are sold as recurring Software-as-a-Service (SaaS). On-premise products are sold by granting the customer access to use the intellectual property during the license period. WithSecure delivers the product and provides continuous automated updates against new threats. The software and the accompanied services are highly interdependent and therefore treated as one performance obligation for which revenue is recognized over time on a straight-line basis for the contract period. Cyber security consulting services are recognized as revenue based on the delivery of the work.

Cloud-based products and services and on-premise security products are provided either as a continuous service or for a fixed term. Continuous services are invoiced on a monthly basis and fixed term fully upfront or monthly, quarterly or annually upfront. Cyber security consulting services are invoiced as agreed with the customer. The standard payment term within the Group is 30 days.

Presentation of receivables and liabilities from contracts with customers

Receivables from contracts with customers are presented in the balance sheet as *Accrued income*. Liabilities from contracts with customers are presented in the balance sheet as *Deferred revenue* and included in *Total non-current liabilities* or *Total current liabilities* depending on the duration of the liability.

Pensions

All of WithSecure Group's pension arrangements are defined contribution plans in accordance with local statutory requirements. Contributions to defined contribution plans are recognized in the income statement in the period to which the contributions relate.

Leases

Group as lessee

Leases which meet with IFRS 16 requirements are booked to balance sheet as right-of-use asset with corresponding lease liability. Right-of-use assets and lease liabilities are initially valued at the present value of the remaining lease payments. Incremental borrowing rate is applied in discounting the remaining payments.

WithSecure's incremental borrowing rate varies between 2,45 % and 9,15 % depending on the geographical location of the leased asset, lease period and guarantees.

WithSecure's right-of-use assets comprise of rented office premises and leased cars. Short-term contracts (remaining contract period 12 months or less) and low value assets are excluded from leases and lease expense is recognized on a straight-line basis as permitted by IFRS 16.

Lease contracts for the Group's office premises are typically made for fixed periods of 3 to 10 years and they may contain extension options. Each office lease contract is negotiated individually, and the contracts may contain wide range of different terms and conditions. Some of Group's office premises are leased with on-going contracts where the ending date is not defined. The management assesses the probable duration for these contracts case-by-case and the lease liability is calculated accordingly. Changes to the estimates are accounted for at each reporting date. Estimated duration for on-going contracts vary between 3 to 5 years.

In measuring the present value of the liabilities arising from leases any service-related fees are excluded from the lease payment. The Group's lease contracts do not contain residual value guarantees or purchase options.

Group as lessor

Group acts as a lessor in sub-lease agreements signed with third parties. The sub-lease arrangements have been accounted for as finance leases. According to IFRS 16, the Group has derecognized the right-of-use assets related to the sub-lease arrangements and recognized a receivable for the net investment in the lease. Net investment in the lease is calculated as the net present value of the future payments under the sub-lease. The Group does not have operating lease arrangements.

Income taxes

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

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

Business combinations

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

The identifiable assets acquired, and the liabilities assumed are recognized at fair value at the acquisition date except for deferred tax assets or liabilities which are measured in accordance with IAS 12 Income taxes. Goodwill is measured as the excess of the transferred consideration over the net amount of the acquired identifiable assets and assumed liabilities.

Changes in fair value of the contingent consideration that do not arise within one year from the acquisition from facts and circumstances that existed at the acquisition date are recognized in profit or loss.

Goodwill

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

Intangible assets

Research and development expenditure

Research expenditure is recognized as an expense at the time it is incurred. Development expenditure on new products or product versions with significant new features are recognized as intangible assets when the Group can demonstrate:

- The technical feasibility of completing the intangible asset so that it will be available for use or sale.
- Its intention to complete and its ability to use or sell the asset.
- How the asset will generate future economic benefits.
- The availability of resources to complete the asset.
- The ability to reliably measure the expenditure during development

Amortization is recorded on a straight-line basis over the estimated useful life, which is 3–8 years for these assets.

Intangible assets acquired in business combinations

Intangible assets acquired in business combinations and recognized separately from goodwill are initially recognized at fair value on the acquisition date. Subsequent to initial recognition these assets are reported at initial value less accumulated amortization and accumulated impairment losses.

Intangible assets acquired in business combinations include technology, trademarks and customer relationships, which all have a finite useful life. Initial valuation for technology and trademarks is done based on Relief from royalty method and for customer relationships based on Excess earnings method.

The estimated useful lives for intangible assets acquired in business combinations are:

Technology	10 years
Trademark	2 years
Customer relationships	6–10 years

The estimated useful life and amortization method are assessed at each reporting date and updated if necessary.

Other intangible assets

Other intangible assets include intangible rights and software licenses, all with a finite useful life. Other intangible assets are recorded at historical cost less accumulated amortization and possible impairment. Amortization is recorded on a straight-line basis over the estimated useful life of an asset. The estimated useful lives of other intangible assets are as follows:

Intangible rights	3–8 years
Other intangible assets	5–10 years

The estimated useful life and amortization method are assessed at each reporting date and updated if necessary.

Tangible assets

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

Machinery and equipment	3–8 years
Other tangible assets	5–10 years

Other tangible assets include renovation costs of rented office space.

Gains or losses on disposal of tangible assets are shown in other operating income or expense.

The estimated useful life and amortization method are assessed at each reporting date and updated if necessary.

Impairment of assets

At each reporting date, the Group assesses whether there is any indication that an asset may be impaired. Where an indicator of impairment exists, the Group makes a formal estimate of recoverable amount. The recoverable amount of goodwill and intangible assets that are not ready for use are estimated annually for regardless of whether any indication of impairment exists.

Where the carrying amount of an asset exceeds its recoverable amount the asset is considered impaired and the carrying amount is reduced to its recoverable amount. The recoverable amount is the fair value of an asset less costs of disposal or value in use, whichever is higher. An impairment loss is recorded in the income statement.

A previously recognized impairment loss is reversed only if there has been a change in the estimates used to determine the asset's recoverable amount since the last impairment loss was recognized. The maximum reversal of an impairment loss amounts to no more than the carrying amount of the asset if no impairment loss had been recognized, net of depreciation. Impairment losses relating to goodwill cannot be reversed in future periods.

Financial instruments

Financial assets and liabilities

All financial assets and liabilities are initially recognized at fair value and subsequently classified as financial assets or liabilities at amortized cost or financial assets or liabilities at fair value through profit or loss. Financial assets and liabilities are classified according to their cash flow characteristics and the business model they are managed in.

Financial assets at amortized cost

Financial assets at amortized cost are subsequently measured using the effective interest rate method. All assets in this category are subject to a business model with the objective to collect contractual cash flows of principal and interest. This category includes trade and other receivables, corporate commercial papers, cash and cash equivalents, asset transfer receivables, and sublease receivables.

Asset transfer receivables are valued at amortized cost and held until the end of the agreement period. Sublease receivables are initially valued at the present value of the remaining lease payments and subsequently by applying a cost model, where asset cost is reduced by accumulated depreciation and impairment losses and adjusted by remeasurement of a respective lease liability. Other interest-bearing receivables are related to deferred considerations which are measured at discounted fair value on each reporting date.

Trade and other receivables are originally valued with transaction price and later with amortized cost reduced by expected credit loss. Trade and other receivables are written off from the balance sheet as the rights to associated cash flows end or become transferred to the counterpart. The increase in the credit risk for financial assets measured at amortized cost is assessed at the end of the reporting period. The credit loss allowance is estimated based on the Group's historical credit loss experience adjusted with current conditions and reasonable and supportable forecasts about the future. An expected credit loss is recognized for trade receivables according to IFRS 9. The amount of expected credit loss is updated at each reporting date to reflect changes in credit risk since initial recognition of the respective financial instrument. The Group applies the simplified approach to estimate the expected credit loss by using a provision matrix where trade receivables are grouped based on historical credit loss experience and

characteristics that depict the credit risk of receivables (e.g. geographical area and days past due).

Financial assets at fair value through profit or loss

This category includes investments in unlisted shares and deferred considerations. Fair value the unlisted shares cannot be measured reliably, the cost is considered to be a reasonable approximation of their fair value. Other interest-bearing receivables are related to deferred considerations which are measured at discounted fair value on each reporting date.

Financial liabilities at amortized cost

Financial liabilities at amortized cost are initially recognized at fair value. After initial recognition, other financial liabilities are subsequently measured at amortized cost using the effective interest method. Amortized cost is calculated by taking into account any issue costs, and any discount or premium on settlement. This category includes lease liabilities, other loans related to demerger, and trade and other payables. Financial liabilities are classified as current unless the Group has unconditional right to postpone their repayment by at least 12 months from the end date of the reporting period.

Derivative financial instruments and hedging

The Group uses derivative financial instruments such as forward currency contracts to hedge its risks associated with foreign currency fluctuations. Derivatives are valued at fair value. The fair value of forward currency contracts is calculated based on current forward exchange rates at the reporting date for contracts with similar maturity profiles. The gains and losses arising from the change of fair value are booked through the income statement as the Group does apply hedge accounting.

Provisions

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

Treasury shares

Parent company has acquired treasury shares in 2008–2011. The purchase price of the shares has been deducted from equity.

Share-based payment transactions

WithSecure provides incentives to employees in the form of equity-settled share-based instruments. Currently the Company has share-based programs.

WithSecure's share-based incentive programs are targeted to the Group's key personnel. The programs are equity-settled and valued at fair value at grant date. The expense is recognized evenly in the income statement over the vesting period with the counter-entry in retained earnings.

Some of the current programs include market-based conditions, which are taken into consideration when the fair value of equity-based instrument is determined by utilizing commonly used valuation techniques. Equity based payments that are settled net of taxes are considered in their entirety as equity-settled share-based payment transactions. The cumulative expense recognized at the grant date is based on the Group's estimate of the number of shares that will vest at the end of the vesting period times the fair value of equity-based instruments at the grant date. If a person leaves the company before vesting, the reward is forfeited. The Group revises its estimate of the non-market conditions and number of equity-based instruments that are expected to vest at the end of vesting period each reporting date. The impact of revision of original estimates is recognized in the income statement.

Presentation of expenses

Classification of the functionally presented expenses has been made by presenting direct expenses in their respective functions and by allocating other expenses to operations on the basis of average headcount in each function.

Operating result

IAS 1 Presentation of Financial Statements standard does not define the concept of Earnings before interest and taxes (EBIT). The Group has defined it as follows: EBIT is the net amount, which consists of revenue and other operating income less cost of revenue, sales and marketing, research and development, and administration.

New standards and interpretations not yet effective

Later, the Group will adopt the following new and amended standards issued by IASB:

New Accounting Standard IFRS 18 Presentation and Disclosure in Financial Statements improves the quality of financial reporting by requiring defined subtotals in the statement of profit or loss and disclosure about management-defined performance measures, as well as adding new principles for aggregation and disaggregation of information. The standard merely changes the presentation of disclosed information and increases the amount of disclosed information.

Other new or amended Accounting Standards not yet effective are not expected to have a significant impact on the consolidated financial statements or other disclosures.

1 Segment information

From 1 January 2024 onwards, WithSecure Group reports three segments: Elements Company, Cloud Protection for Salesforce (CPSF) and Cyber security consulting. The operating segments are reported in a manner consistent with the internal reporting provided to the Group Leadership Team, which has been identified as WithSecure's chief operating decision maker being responsible for allocating resources and assessing performance of the operating segments as well as deciding on strategy. The Group Leadership Team assesses the profitability of segments principally on the basis of adjusted EBITDA.

Elements Company segment includes Elements Cloud products and services, On-premise products, Managed services (including Countercept Managed Detection and Response, MDR), and Other products. Elements Company revenue is presented separately for Cloud, On-premise and Other products.

Cloud Protection for Salesforce (CPSF) segment includes revenue from the CPSF product. It is a software product, ensuring scanning of external content for potential malware, before it is loaded into Salesforce. Customers are primarily enterprise sized companies, with extensive use of Salesforce platforms.

Cyber security consulting segment includes the consulting services sold to large enterprise customers. On 23 January 2025, WithSecure signed an agreement intending to divest the Cyber security consulting business. In the Segment information note of 2024 financial statement, Cyber security consulting segment is presented according to the accounting principles applied in the 2024 segment reporting. In other parts of the 2024 financial statements, Cyber security consulting is presented as part of the Discontinued operations. Reconciliations between the segment result and the discontinued operation's result are presented in the Segment information note.

Revenue by segment	Restated	
	Consolidated	Consolidated ¹
EUR 1,000	2024	2023
Elements Company	105,661	101,143
Elements Cloud	83,277	76,132
On-premise	21,443	24,356
Other	942	656
Cloud Protection for Salesforce	9,440	8,299
Cyber security consulting	32,254	33,370
Total revenue	147,357	142,812
Discontinued operations	31,355	32,873
Total revenue, continuing operations	116,002	109,939

¹ The comparative data has been restated because, starting from January 1, 2024, WithSecure has reported three segments: Elements company, Cloud Protection for Salesforce (CPSF), and Cybersecurity Consulting.

Gross margin by segment	Restated	
	Consolidated	Consolidated
EUR 1,000	2024	2023
Elements Company	84,266	79,609
% of revenue	79.8%	78.7%
Cloud Protection for Salesforce	7,874	6,133
% of revenue	83.4%	73.9%
Cyber security consulting	13,993	14,449
% of revenue	43.4%	43.3%
Total gross margin	106,133	100,192
Discontinued operations	13,547	13,360
Total gross margin, continuing operations	92,585	86,832

Adjusted EBITDA by segment EUR 1,000	Restated	
	Consolidated 2024	Consolidated 2023
Elements Company	4,008	-10,906
% of revenue	3.8%	-10.8%
Cloud Protection for Salesforce	-958	-4,627
% of revenue	-10.1%	-55.8%
Cyber security consulting	86	-584
% of revenue	0.3%	-1.8%
Total adjusted EBITDA	3,135	-16,116
Discontinued operations	1,144	-1,308
Total adjusted EBITDA, continuing operations	1,991	-14,807
Items affecting comparability	-852	-8,951
EBITDA	1,139	-23,758
Depreciation and amortization	-11,222	-11,934
Finance Income	2,867	2,659
Finance Expense	-3,085	-2,147
Profit (loss) before taxes, continuing operations	-10,301	-35,180

Geographical information

Geographical information about revenue is presented in disclosure [2 Revenue](#).

Long-term assets EUR 1,000	Consolidated	
	2024	2023
Nordic countries	33,609	38,995
Europe excl. Nordics	39,466	1,670
North America	1,403	70,067
Rest of world	798	910
Total	75,278	111,642

2 Revenue

Principles of revenue recognition are stated in accounting principles to consolidated financial statements, section *Revenue recognition*. Disaggregation of revenue is presented for continuing operations only according to IFRS 5 as Consulting business is treated as discontinued operations. Assets and liabilities from contracts with customers (accrued income) have not been restated for continuing operations for comparative periods.

Disaggregation of revenue

Revenue from external customers EUR 1,000	Restated	
	Consolidated 2024	Consolidated 2023
Elements Company	106,562	101,640
Elements Cloud	83,271	75,985
On-premise	21,443	24,356
Other	1,849	1,299
Cloud Protection for Salesforce	9,440	8,299
Total revenue	116,002	109,939

Geographical information	Restated	
	Consolidated	Consolidated
EUR 1,000	2024	2023
Revenue from external customers		
Nordic countries	29,402	27,450
Europe excl. Nordics	58,477	55,808
North America	9,638	8,351
Rest of world	18,485	18,330
Total	116,002	109,939

Assets and liabilities from contracts with customers

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

EUR 1,000	Consolidated	
	Consolidated	Consolidated
EUR 1,000	2024	2023
Accrued income	1,261	5,577
Deferred revenue, non-current	18,478	20,772
Deferred revenue, current	49,245	46,125

Transaction price allocated to all fully or partially unsatisfied performance obligations amounted to 67,724 thousand at the end of the year. 73 % of the amount is expected to be recognized as revenue during 2024. The Group total revenue will also include new orders, renewals and contract extensions/expansions which are not known at reporting date and thus are excluded from these figures.

Increases in deferred revenue resulting from billing were EUR 46,951 thousand. Decreases in deferred revenue resulting from satisfying performance obligations were EUR 46,125 thousand.

3 Other operating income

EUR 1,000	Consolidated	
	Consolidated	Consolidated
EUR 1,000	2024	2023
Service fees charged from F-Secure under TSA	263	6,939
Capital gains from sales of operations	1,168	1,372
Government grants	267	543
Gain from sublease arrangements	860	589
Gain from sale of intangible and tangible assets	422	
Other	270	292
Total	3,249	9,735

Capital gains from sales of operations includes revision of fair value of deferred consideration from divestment of UK public sector consulting team in December 2021 and proceeds from divested business.

Government grants consist mainly from grants from Business Finland and European Union related to R&D activities. The grants are recognized as income over those periods in which the corresponding expenses arise.

4 Leases

EUR 1,000	Consolidated	
	2024	2023
Right of use assets and liabilities		
Right of use assets		
Buildings	17,670	8,182
Cars	936	997
Machinery	118	212
Total	18,724	9,391
Lease liabilities		
Buildings	21,795	9,152
Cars	1,025	1,030
Machinery	119	0
Total	22,939	10,182
Repayments of lease liabilities	6,443	6,139

EUR 1,000	Restated Consolidated	
	2024	2023
Short-term leases booked as rent expense	13	43
Low-value leases booked as rent expense	80	51

Lease related income statement effect is presented for continuing operations only according to IFRS 5 as Consulting business is treated as discontinued operations. For right of use assets and lease liabilities, comparative information is presented on a historical basis for combined operations (i.e. not restated).

Right of use assets related changes are stated in disclosure [13 Non-current assets](#).

Right of use assets related interest payments are stated in disclosure [8 Financial income and expenses](#).

Maturity of lease liabilities is stated in disclosure [17 Financial assets and liabilities](#).

5 Depreciation, amortization, and impairment

EUR 1,000	Restated	
	Consolidated 2024	Consolidated 2023
Depreciation and amortization of non-current assets		
Other intangible assets	-1,043	-1,302
Capitalized development	-4,820	-4,891
Intangible assets	-5,863	-6,193
Machinery and equipment	-797	-724
Right of use assets	-4,267	-4,796
Other tangible assets	-295	-220
Tangible assets	-5,359	-5,740
Total depreciation and amortization	-11,222	-11,934
Depreciation and amortization by function		
Sales and marketing	-3,896	-4,142
Research and development	-5,068	-5,300
Administration	-2,258	-2,492
Total depreciation and amortization	-11,222	-11,934

Depreciation and impairment is presented for continuing operations only according to IFRS 5 as Consulting business is treated as discontinued operations.

6 Personnel expenses

EUR 1,000	Restated	
	Consolidated 2024	Consolidated 2023
Personnel expenses		
Wages and salaries	-56,895	-73,519
Pension expenses - defined contribution plan	-7,754	-8,320
Share-based payments	-2,510	-3,326
Other social expenses	-4,323	-7,510
Total	-71,481	-92,675

Personnel expenses are presented for continuing operations only according to IFRS 5 as Consulting business is treated as discontinued operations.

Employee benefits of the management are stated in disclosure [23 Related party disclosures](#).

Share-based payments are stated in disclosure [16 Share-based payment transactions](#).

	Restated	
	Consolidated 2024	Consolidated 2023
Average number of personnel	760	845
Personnel by function December 31		
Consulting and delivery	56	42
Sales and marketing	252	287
Research and development	309	341
Administration	114	143
Total	731	813

7 Audit fees

EUR 1,000	Consolidated	
	2024	2023
Group auditor, PricewaterhouseCoopers		
Auditing	-288	-210
Other actions referred to in section 1, subsection 1, paragraph 2 of the Auditing Act	-29	-22
Other Services	-91	
Total	-408	-233

PricewaterhouseCoopers Oy has provided non-audit services to entities of WithSecure Group in total 120 thousand euros during the financial year 2024. These services included auditors's statements (29 thousand euros) and other services (91 thousand euros).

Other auditors EUR 1,000	Consolidated	
	2024	2023
Auditing	-79	-82
Total	-79	-82

8 Financial income and expenses

EUR 1,000	Restated Consolidated	
	2024	2023
Financial income		
Interest income from financial assets	845	1,446
Exchange gains	2,021	1,174
Other financial income	1	38
Total	2,867	2,659
Financial expenses		
Interest expense from loans and liabilities	-292	-312
Interest expense from lease liabilities	-624	-305
Exchange losses	-1,888	-1,314
Other financial expenses	-280	-216
Total	-3,085	-2,147

Financial income and expenses are presented for continuing operations only according to IFRS 5 as Consulting business is treated as discontinued operations.

9 Income tax

EUR 1,000	Consolidated	
	2024	2023
Current income tax for the year	-972	-778
Adjustments for current tax of prior periods	-198	-110
Change in deferred tax	2,295	3,928
Total	1,125	3,040

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

EUR 1,000	Consolidated	
	2024	2023
Result before taxes, continuing operations	-10,301	-35,180
Result before taxes, discontinued operations	-29,502	-8,506
Result before taxes, combined operations	-39,802	-43,686
Income tax at Finnish tax rate of 20%	7,960	8,737
Effect of overseas tax rates	733	482
Non-deductible expenses/tax-exempt revenue	-6,389	-2,201
Unrecognised tax losses	-172	-2,748
Adjustments for prior period tax	-198	-114
Other	-112	-502
Total	1,823	3,655
of which		
Continuing operations	1,125	3,040
Discontinued operations	698	615

10 Earnings per share

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

EUR 1,000	Consolidated	
	2024	2023
Net profit attributable to equity holders of the parent company		
Continuing operations	-9,175	-32,139
Discontinued operations	-28,804	-7,891
Combined operations	-37,979	-40,030
Weighted average number of ordinary shares (1 000)	175,986	175,594
Adjusted weighted average number of ordinary shares for diluted earning per share	175,986	175,594
Basic and diluted earnings per share (EUR/share), continuing operations	-0.05	-0.18
Basic and diluted earnings per share (EUR/share), discontinued operations	-0.16	-0.04
Basic and diluted earnings per share (EUR/share), combined operations	-0.22	-0.23

The weighted average number of shares takes into account the effect of change in treasury shares.

11 Discontinued operations

On 23 January 2025, WithSecure announced the decision to sell its cyber security consulting business. The transaction is executed by the sale of shares of the parent company of a to-be-established WithSecure cyber security consulting group, to which the consulting business will be transferred prior to the completion of the transaction. The transaction is expected to be completed during the second quarter of 2025. The completion of the transaction is subject to customary closing conditions and regulatory approvals.

The consulting business was presented in Group's Consulting reporting segment. At 31 December 2024, the cyber security consulting business was classified as a disposal group held for sale and the net assets were valued at fair value less costs to sell, which resulted in goodwill impairment of 13 million euro. The results of the business to be divested will be included in the discontinued operations.

Income statement	Consolidated	
EUR 1,000	2024	2023
Revenue	31,355	32,873
Cost of revenue	-17,808	-19,513
Gross margin	13,547	13,360
Sales and marketing	-9,265	-10,871
Administration	-33,632	-10,687
EBIT	-29,350	-8,199
Financial net	-152	-307
Result before taxes	-29,502	-8,506
Income taxes	698	615
Result for the financial year, discontinued operations	-28,804	-7,891
Impairment loss recognised on the remeasurement to fair value less costs to sell (included in Administration costs)	13,309	

Statement of financial position	Consolidated
EUR 1,000	2024
Assets	
Tangible assets	1,374
Goodwill	16,021
Deferred tax assets	1,335
Total non-current assets	18,730
Accrued income	5,636
Trade and other receivables	6,125
Total current assets	11,762
Total assets	30,492

Statement of financial position	Consolidated
EUR 1,000	2024
Liabilities	
Non-current interest bearing liabilities	418
Other non-current liabilities	281
Total non-current liabilities	699
Current interest bearing liabilities	436
Trade and other payables	3,695
Deferred revenue, current	5,541
Income tax liabilities	52
Total current liabilities	9,724
Total liabilities	10,423

Statement of cash flows	Consolidated	
EUR 1,000	2024	2023
Net cash flow from operating activities	1,137	-1,309
Net cash flow from investing activities	-85	-101
Net cash flow from financing activities	-210	-208

12 Goodwill

From 1 of January 2024 onwards, goodwill has been reallocated to cash-generating units (CGUs) of the new reporting structure. The carrying amount of goodwill EUR 35,848 thousand is allocated to Elements company CGU. Cyber security consulting goodwill is presented in assets held for sale.

EUR 1,000	Consolidated	
EUR 1,000	2024	2023
Elements company, goodwill 1.1.	35,032	
Cyber security consulting, goodwill 1.1.	43,026	
Cyber security consulting, impairment	-15,578	
Cyber security consulting, impairment loss recognised on the remeasurement to fair value less costs to sell	-13,309	
Cyber security consulting, goodwill classified as asset held for sale	-16,021	
Translation difference	2,698	
Goodwill	35,848	78,058

Goodwill was previously allocated as follows:

EUR 1,000	Consolidated
EUR 1,000	2023
MDR	26,844
Consulting	51,214
	78,058

Goodwill is tested for impairment annually, or more frequently if there are indications that goodwill might be impaired. The recoverable amount for each CGU is determined based on a value in use calculation which uses cash flows for the period determined for the CGU. Cash flows are based on financial budgets and forecasts approved by the Board of Directors. Forecast period used in the calculations is five years. Discount rate for Elements is 16.9 % (MDR 15.6 %) before taxes.

Cash flows beyond forecast period have been extrapolated using steady 2 % (2 %) per annum growth rate.

Revenue growth % in average during forecast period for Elements is 13 % (MDR 22%)

Profitability (EBIT -%) in average during forecast period for Elements is 9% (MDR 14%).

Sensitivity analysis

The Group has prepared a sensitivity analysis of the impairment tests to changes in the key assumptions which are revenue, profitability and discount rate. The table below shows the required change in a single assumption that the recoverable amount would fall below the carrying amounts.

EUR 1,000	2024	2023
Variable		
Revenue growth during forecast period		
Elements (MDR)	15 % decrease	33 % decrease
Profitability (EBIT-%) during forecast period		
Elements (MDR)	24 % decrease	76 % decrease
Discount rate (Post-tax WACC)		
Elements (MDR)	4.6 %-point increase	25.9 %-point increase

Sensitivity analyses assume a change in only one key variable while all other variables in the forecasts remain unchanged. In WithSecure's analyses sensitivity is tested by assuming a similar change in the tested assumption throughout the forecast period. In reality, it is highly unlikely that such change in the cash flows would occur as the management has means to react in case there is a change to the expected business performance.

Headroom for Elements remains high and the management believes that no reasonably possible change in any of the key variables would lead to the recoverable amount to fall below the carrying amount.

13 Non-current assets

Restated EUR 1,000	Intangible assets					Tangible assets						
	Other Intangible	Capitalized development	Goodwill	Advance payments & incomplete development	Total	Machinery & equip.	Right of use assets total	Right of use assets buildings	Right of use assets cars	Right of use assets machinery and equipment	Other Tangible	Total
Acquisition cost Jan 1, 2023	14,478	47,164	82,997	1,441	146,080	9,703	22,603	18,775	3,576	252	2,971	35,277
Translation difference	63	342	1,256		1,661	45	-161	-170	9		-12	-129
Impairment			-6,198		-6,198							
Additions		674		2,333	3,007	1,325	8,461	5,778	2,274	409	1,211	10,997
Disposals						-211	-5,040	-2,909	-2,131		-185	-5,436
Acquisition cost Dec 31, 2023	14,541	48,181	78,058	3,773	144,550	10,862	25,863	21,473	3,728	662	3,984	40,709
Translation difference	-84	678	2,698		3,292	472	260	260	-1		129	861
Assets held for sale	-35	-646	-16,021		-16,702	-583	-2,300	-1,882	-418		-644	-3,527
Impairment			-28,887		-28,887							
Additions		1,639		411	2,051	3,213	24,465	23,423	834	207	1,001	28,680
Disposals	-14			-335	-349	-5,906	-23,182	-22,194	-867	-121	-1,666	-30,754
Acquisition cost Dec 31, 2024	14,407	49,853	35,848	3,850	103,954	8,058	25,106	21,077	3,276	748	2,803	35,968
Acc. depreciation Jan 1, 2023	-11,269	-28,194			-39,463	-8,039	-14,491	-11,341	-2,857	-293	-2,130	-24,661
Translation difference	-45	-152			-196	-36	103	113	-9		10	77
Depreciation for the period	-1,298	-4,884			-6,182	-789	-4,842	-3,360	-1,285	-197	-403	-6,033
Depreciation of disposals						39	3,132	1,712	1,420		48	3,220
Acc. depreciation Dec 31, 2023	-12,612	-33,230			-45,842	-8,825	-16,098	-12,876	-2,731	-490	-2,475	-27,397
Translation difference	13	-301			-288	-396	-61	-61	1		-5	-461
Assets held for sale	35	646			681	304	1,477	1,231	246		372	2,154
Depreciation for the period	-1,053	-4,856			-5,906	-881	-5,470	-4,564	-605	-302	-533	-6,885

Restated EUR 1,000	Intangible assets				Tangible assets							
	Other Intangible	Capitalized development	Goodwill	Advance payments & incomplete development	Total	Machinery & equip.	Right of use assets total	Right of use assets buildings	Right of use assets cars	Right of use assets machinery and equipment	Other Tangible	Total
Depreciation of disposals	14				14	5,269	13,769	12,899	749	121	1,583	20,621
Acc. depreciation Dec 31, 2024	-13,602	-37,741			-51,340	-4,529	-6,382	-3,371	-2,340	-671	-1,058	-11,969
Book value as at Dec 31, 2023	1,929	14,951	78,058	3,773	98,708	2,037	9,391	8,598	997	172	1,509	12,938
Book value as at Dec 31, 2024	805	12,112	35,848	3,850	52,614	3,530	18,724	17,706	936	77	1,745	23,999

14 Shareholder's Equity

EUR 1,000	Total number of shares	Number of shares outstanding	Number of treasury shares	Share capital	Unrestricted equity reserve	Treasury shares
Dec 31, 2022	174,598,739	174,526,944	71,795	80	83,638	-155
Directed share issue to company itself	1,500,000		1,500,000			
Share based payments		1,345,675	-1,345,675			
Dec 31, 2023	176,098,739	175,872,619	226,120	80	83,638	-155
Share based payments		144,230	-144,230			
Dec 31, 2024	176,098,739	176,016,849	81,890	80	83,638	-155

A share has no nominal value. All issued shares are fully paid and listed on Nasdaq Helsinki.

Translation differences

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

Dividends proposed and paid

Proposed for approval at AGM for financial year 2024 is that no dividend will be paid.

For financial year 2023 company decided to not pay any dividend.

Treasury shares

Treasury shares contains shares acquired from the market and shares from the direct share issue to company itself. The cost of acquired shares is reported as a deduction in shareholders' equity. The shares have been acquired through public trading on Nasdaq Helsinki. The parent company has not acquired treasury shares during the period. During the financial year parent company's treasury shares have been used for board remuneration and incentive programs.

The total number of treasury shares was 81,890 at the end of 2024. This represents 0.05% of the Company's voting power on December 31, 2024.

15 Trade and other receivables

EUR 1,000	Consolidated	
	2024	2023
Current receivables		
Trade receivables	18,623	25,237
Other receivables	382	658
Prepaid expenses	5,640	5,788
Total	24,645	31,683

Aging of trade receivables and expected credit losses

EUR 1,000	Not fallen due	Overdue 1-30 days	Overdue 31-60 days	Overdue 61-90 days	Overdue over 90 days	Total
Average expected credit loss rate	1.5 %	1.5%	1.2%	6.0%	27.2%	
Gross trade receivables	15,253	1,764	464	505	1,584	19,571
Loss allowance	229	26	6	30	385	676
Additional provision					272	272
Total trade receivables at amortized cost Dec 31, 2024	15,025	1,738	459	475	927	18,623

EUR 1,000	Not fallen due	Overdue 1-30 days	Overdue 31-60 days	Overdue 61-90 days	Overdue over 90 days	Total
Average expected credit loss rate	1.5 %	1.5 %	1.3 %	6.3 %	26.9 %	
Gross trade receivables	19,636	3,100	766	597	3,245	27,344
Loss allowance	294	45	9	37	689	1,074
Additional provision					1,033	1,033
Total trade receivables at amortized cost Dec 31, 2023	19,342	3,055	757	560	1,523	25,237

Movements in the provision for expected credit losses

EUR 1,000	Consolidated	
	2024	2023
Book value as at Jan 1	2,194	1,571
Change for the year		
Loss allowance	-357	111
Additional provision	-63	425
Translation differences	-41	172
Receivables written off during the year	-698	-84
Book value as at Dec 31	1,035	2,194

Material items included in prepaid expenses

EUR 1,000	Consolidated	
	2024	2023
Prepaid royalty	2,003	2,015
Grant receivables	413	279
Other prepaid expenses	3,224	3,494
Total	5,640	5,788

16 Share-based payment transactions

WithSecure's current long-term incentive plans consist of Performance Share Plans, Restricted Share plans, a Performance Matching Share Plan and an Employee share savings plan.

Performance Share plans

Performance share plans consist of 3 year performance periods that the Board of Directors can decide on annually. In PSPs, participants are given an opportunity to earn WithSecure shares. The rewards are based on the company's performance against the criteria set by the Board of Directors and will be paid to the participants after the performance period, given that the participants' employment continues without termination at the time of payment.

Instrument	Performance Share Plan 2022 - 2024	Performance Share Plan 2023 - 2025	Performance Share Plan 2024 - 2026
Initial amount, pcs	5,900,000	4,600,000	6,600,000
Maximum allocation at 31.12.2024 ¹	1,436,956	3,235,000	5,980,000
Initial allocation date	12.8.2022 ²	16.12.2022	7.3.2024
Vesting date	31.3.2025	31.3.2026	31.3.2027
Performance Criteria	Absolute TSR (100%)	Absolute TSR (100%)	Revenue growth (100%)
Maximum contractual life, yrs	2.6	3.3	3.1
Remaining contractual life, yrs	0.25	1.25	2.25
Number of persons at the end of reporting year	46	81	86
Payment method	Cash & Equity	Cash & Equity	Cash & Equity
Changes during period			
1.1.2024			
Outstanding in the beginning of the period	926,810	2,020,000	
Changes during period			
Granted			3,010,000
Forfeited	208,332	402,500	130,000
Exercised			
Outstanding at the of the period	718,478	1,617,500	2,880,000

1

Excluding leavers from the allocated participants, as well as voided shares from the original plan pools

² For PSP 2022-2024 the shares were converted into WithSecure shares

Restricted share plan

Restricted Share Plans consist of 3-year restriction periods that the Board of Directors can decide on annually. WithSecure currently has three active Restricted Share Plans that are presented in the table below. There are no financial or other performance criteria in the Restricted Share Plans, only the employment pre-condition. The rewards will be paid to the participants, given that the employment continues without termination at the time of payment.

Instrument	Restricted Share Plan 2022 - 2024	Restricted Share Plan 2023 - 2025	Restricted Share Plan 2024 - 2026
Initial amount, pcs			
Initial allocation date	1,400,000 ¹	1,100,000	500,000
Maximum allocation at 31.12.2024 ²	104,444	325,000	395,000
Vesting date	17.3.2022	16.12.2022	7.3.2022
Maximum contractual life, yrs	31.3.2025	31.3.2026	31.3.2027
Remaining contractual life, yrs	3.0	3.3	3.1
Number of persons at the end of reporting year	6	18	9
Payment method	Cash & Equity	Cash & Equity	Cash & Equity
Changes during period			
1.1.2024			
Outstanding in the beginning of the period	134,444	400,000	
Changes during period			
Granted		330,000	395,000
Forfeited	30,000	60,000	
Exercised			
Outstanding at the of the period 31.12.2024	104,444	325,000	395,000

¹ For RSP 2022-2024 the shares were converted into WithSecure shares

² Excluding leavers from the allocated participants, as well as voided shares from the original plan pools

Performance Matching Share Plan

Performance Matching Share Plan for President and CEO, leadership team members and other key leaders of WithSecure consists of one 4-year performance period, which started on 1 September 2022 and ends on 30 November 2026. In the plan, the participants are given an opportunity to invest in WithSecure and earn WithSecure shares through a matching reward. The prerequisite for participation in the plan is a personal investment in WithSecure within the guidelines approved by the Board of Directors.

The company will match the participants' own investment based on WithSecure's market capitalization value. The performance-based matching is defined as 2.5 times the number of invested shares at target level and 5 times at the maximum level. The performance criterion used in the PMSP is the company's market value in absolute value. In addition, the participants will receive a guaranteed matching of 0.5 times the initial investment, given that their employment continues without termination at the time of payment.

Performance Matching Share Plan replaced Share-based incentive program's earning period 2022-2024 for participants. According to IFRS 2 modification accounting has been applied. In the modification, the fair value of the original reward and the fair value of the new reward was calculated to the modification date September 9, 2022. Expense from the original reward is booked as cost for the original earning period and the incremental expense from the modification is booked as cost for the performance period of the new reward.

Instrument	Performance matching share plan 2022-2026
Initial amount, pcs	7,900,000
Maximum allocation ¹	3,538,684
Initial allocation date	1.9.2022
Vesting date	30.11.2026
Performance Criteria	WithSecure market capitalization
Maximum contractual life, yrs	4.25
Remaining contractual life, yrs	1.9
Number of persons at the end of reporting year	16
Payment method	Cash & Equity
Changes during period	
1.1.2024	
Outstanding at the beginning of the period	1,317,334
Changes during period	
Granted	
Forfeited	673,937
Exercised	
Outstanding at the end of the period	643,397

¹ Excluding leavers from the allocated participants, as well as voided shares from the original plan pools

Employee Share Savings Plan

WithSecure currently has 2 ongoing Employee Share Savings Plans. Each plan consists of a 12-month savings period that is followed by a 2-year restriction period. The Board of Directors can decide on a new plan annually. In the plan, the participants are given an opportunity to invest in WithSecure through monthly savings and earn WithSecure shares through a matching reward. The participants have an opportunity to save 2–5% of their gross base salary. The savings will be used to purchase WithSecure shares from the market on a quarterly basis.

After the restriction period, the participants will receive one guaranteed matching share for every two shares saved within the Plan, given that their employment continues without termination at the time of the reward payment. There are no other restrictions regarding the shares after the matching rewards have been paid to the participants

Instrument	Employee Share Savings Plan 2022-2025	Employee Share Savings Plan 2024-2026
Initial amount, pcs	1,300,000 ¹	1,000,000 ¹
Initial allocation date	1.10.2022	1.1.2024
Vesting date	30.9.2025	31.12.2026
Maximum contractual life, yrs	3.00	3.00
Remaining contractual life, yrs	0.75	2.00
Number of persons at the end of reporting year	223	94
Changes during period		
1.1.2024		
Outstanding in the beginning of the period	261,311	
Changes during period		
Granted		91,609
Forfeited	58,768	6,620
Exercised		
Expired		
31.12.2024 Outstanding at the end of the period	202,543	84,989

¹ The final number of matching shares depends on the employees' participation and savings rate in the plan, and the fulfilment of the prerequisites for receiving matching shares, as well as the number of shares acquired from the market with savings.

Impacts of share-based payment transactions on financial statements

EUR 1,000	Consolidated	
	2024	2023
Booked as expense during the period	2,510	3,326

17 Financial assets and liabilities

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

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

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

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

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

EUR 1,000	Note	Fair value hierarchy	Consolidated	
			2024	2023
Financial assets at fair value through profit or loss				
Current				
Investments in unlisted shares		Level 3	26	26
Financial assets at amortized cost				
Non-current				
Interest bearing receivables ¹		Level 3	4,188	6,059
Current				
Interest bearing receivables ¹		Level 3	6,642	2,074
Trade receivables	15	Level 2	18,623	25,237
Cash and cash equivalents			27,275	36,604
Total			56,754	70,000

¹ Interest bearing receivables include receivables related to premises subleased to third parties, receivables related to deferred consideration and receivables related to asset transfers in Group subsidiaries in relation to demerger.

EUR 1,000	Note	Fair value hierarchy	Consolidated	
			2024	2023
Financial liabilities at amortized cost				
Non-current				
Interest bearing liabilities				
Other loans		Level 3		3,554
Current				
Interest bearing liabilities				
Other loans		Level 3	3,757	
Trade and other payables			3,506	3,376
Total			7,262	6,931

The carrying amount of all financial assets and liabilities, carried at amortized cost is considered to provide a reasonable approximation of their fair value.

In September 2023, the company signed a committed EUR 20 million revolving credit facility (RCF) with OP Corporate Bank. The facility will mature in three years from its signing. The new facility is subject to conventional covenants related to ratio of net debt to EBITDA and equity ratio. The facility remains unused at the end of the year.

Contractual maturities of financial liabilities							Total contractual	
	Less than 1 year	1 to 2 years	2 to 3 years	3 to 4 years	4 to 5 years	Over 5 years	cash flows	Carrying amount
Lease liabilities	2,270	3,817	3,223	2,359	1,963	9,307	22,939	22,939
Trade and other payables	3,506						3,506	3,506
Other loans	3,757						3,757	3,757
Total financial liabilities	9,532	3,817	3,223	2,359	1,963	9,307	30,201	30,202

Other loans are liabilities related to asset transfers in Group subsidiaries in relation to demerger.

Lease liabilities consists mainly of buildings (EUR 22.0 million). Cars are totalling to EUR 1.0 million and the maturity for them is mainly less than 2 years.

18 Management of financial risks

General

The goal of risk management is to identify risks that may hinder the Group from achieving its business objectives. The Group may be exposed to a variety of financial risks: market risk (including currency risk, interest rate risk and commodity risk), credit risk and liquidity risk. The responsibility for the Group's risk management lies with the CEO, the management and ultimately with the Board of Directors. The operative management of the treasury activities are centralized into Group Treasury. The Treasury Policy, which has been approved by the Board of Directors, defines the principles for measuring and managing liquidity risk, interest rate risk, currency risks and counter-party risk of the Group.

Credit risk

Credit risk is managed on Group level in line with the Group Credit policy. Credit risk derives from financial investments, derivative contracts and customer-related assets, such as accounts receivable. The Group trades only with recognized, creditworthy third parties and requires a credit review to be performed for any new customers. Advance payments or short payment terms can be used to reduce credit risk, especially with significant contracts. Receivable balances are monitored and collected on an ongoing basis. The maximum exposure to credit risk at the reporting date is the carrying value of trade receivables. There are no significant concentrations of credit risk within the Group due to its diversified customer portfolio operating in different regions. See note [15 Trade and other receivables](#)

Liquidity risk

Liquidity risk arises if the Group's existing liquidity reserves, net cash flows and available additional financing are not sufficient to cover commitments falling due within next 12 months. Group manages its liquidity risk by centralizing the management of cash and liquid assets and thereby optimizing the use of liquid funds for operational and refinancing needs. Group Treasury is responsible for monitoring cash balances and cash forecasts to keep liquidity risk at manageable level. The Group has not identified any significant concentrations of liquidity risks in sources of available financing.

Cash and bank balance was at solid level throughout 2024. In total, Group's cash and cash equivalents were EUR 27.3 million (EUR 36.6 million euro in 2023). The Group also holds a revolving credit facility (RCF) of EUR 20 million which remains unused at the end of the year. The management and the Board of Directors monitors Group's liquidity through a regular cash forecast on a monthly basis.

Market risk

The Group invests liquidity in excess of operative requirement according to Investment Policy approved by the Board of Directors. Assets available for investing are determined based on cash and liquidity forecasts. The objective is to generate stable positive returns and at minimum ensure that the invested nominal amounts can be redeemed. Market risk arising from investments is managed by defining neutral allocation per asset class complemented by minimum and maximum limits. The Board of Directors approves allowed counterparties and issuers for the Group's investments

Foreign currency risk

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

Transaction risk

Majority of sales is invoiced in Euros. Other main currencies for invoicing are GBP, USD and JPY. Currency risk arising from sales invoicing is notably diminished by operational expenses arising in same currencies as the sales invoicing. In order to minimize the impact of the fluctuation of the exchange rates, the Group can use forward currency contracts to eliminate the currency exposure of the estimated cash flow of these currencies. Group has forward contracts to hedge internal loan receivable in USD. As of 31 December 2024, the nominal value of the forward contracts was EUR 7 million and the market value was EUR -285 thousand.

	Consolidated	
	2024	2023
Sales in different currencies	%	%
EUR	54	52
GBP	16	18
USD	12	13
JPY	9	10
SEK	3	3
Other currencies	6	4
	100	100

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

Financial assets	Consolidated		Consolidated	
	2024	%	2023	%
EUR	25,662	41	37,943	54
JPY	8,967	14	7,901	11
GBP	10,383	17	10,956	16
USD	9,874	16	6,817	10
Other currencies	7,556	12	6,423	9
	62,442	100	70,040	100

Financial liabilities	Consolidated		Consolidated	
	2024	%	2023	%
EUR	19,811	64	7,237	42
USD	5,247	17	5,200	30
GBP	3,772	12	3,914	23
Other currencies	2,361	7	802	5
	31,192	100	17,154	100

The table below demonstrates how sensitive the Group's profit before taxes is to foreign exchange rate fluctuations when all other variables are held constant. The open exposure against USD, GBP and JPY arising from Group treasury, trade receivables and trade payables have an impact on Group's profit before taxes. The sensitivity calculation is based on a change of 10% in the Euro exchange rate against the functional currencies the Group operates in.

EUR million	Consolidated	
	2024	2023
USD	+0,4/-0,4	+0,2/-0,3
GBP	-0,1/+0,1	-0,2/+0,3
JPY	-0,2/0,2	+0,0/-0,0

Translation risk

Translation risk arises from the Group's net investments in foreign currencies. Most significant translation risks arise from goodwill generated in MWR InfoSecurity acquisition. Main currencies in goodwill are GBP and EUR. In the divestment of the South African subsidiary, ZAR based goodwill was reallocated to GBP and EUR. Translation differences also arise from translating Group companies' balance sheets into euros using exchange rates prevailing on the reporting date. Internal loans are granted mainly in subsidiaries' home currencies. According to current policy, WithSecure does not hedge equity investments made in its subsidiaries.

The table below demonstrates how sensitive the Group's equity is to foreign exchange rate fluctuations when all other variables are held constant. The sensitivity calculation is based on a change of 10% in the Euro exchange rate against the main functional currencies exposing the Group to translation risk.

EUR million	Consolidated 2024	Consolidated 2023
GBP	+7.6/-6.8	+7.7/-6.3
DKK	+0.7/-0.7	+0.8/-0.7

Interest rate risk

The Group has no bank loans as of 31 December 2024. Interest rate risk is limited to interest bearing liabilities in subsidiaries from asset transfers related to the demerger (EUR 3.8 million). There is no significant interest rate risk related to interest bearing receivables due to their short-term nature (asset transfer related receivables from F-Secure, EUR 5.4 million) or due to their general nature (sublease receivables and earn-out receivables from 3rd parties, EUR 5.3 million).

Capital management

The Group's shareholders' equity is managed as capital. The objective of the Group's capital management is to maintain an efficient capital structure that ensures the functioning of business operations and promotes shareholder value. After June 2022, the Group has not had external financing. Capital structure is reviewed regularly as a part of financial performance monitoring. The capital structure can be adjusted among other things by distribution of dividends, share repurchase or capital repayment. The dividend policy of WithSecure is to pay approximately half of its annual profit as dividend. Subject to circumstances, the Company may deviate from its policy.

19 Deferred tax

Combined operations				
Deferred tax assets and liabilities	1.1.2024	Recognised in profit and loss	Exchange rate differences	31.12.2024
Deferred tax assets				
R&D	5,385	1,781		7,166
Tax losses	3,033	639	68	3,740
Fixed assets	1,019	876		1,895
Accruals and provisions	4,457	165	-98	4,524
Total deferred tax assets	13,894	3,461	-30	17,325
Offset against deferred liabilities	-3,212	-576	87	-3,875
Net deferred tax assets	10,682			13,450
Net deferred tax assets Continuing operations				12,115
Net deferred tax assets, Assets held for sale				1,335
Deferred tax liabilities				
Fixed assets	2,231	269	-298	2,202
Accruals and provisions	2,255	790	-82	2,963
Total deferred tax liabilities	4,486	1,059	-380	5,165
Offset against deferred tax assets	-3,212	-576	-30	-3,875
Net deferred tax liabilities	1,274			1,290
Net deferred tax liabilities Continuing operations				1,279
Net deferred tax liabilities, directly associated with the assets held for sale				11

Deferred tax assets and liabilities	1.1.2023	Recognised in profit and loss	Exchange rate differences	31.12.2023
Deferred tax assets				
R&D	2,132	3,253		5,385
Tax losses	2,630	680	-276	3,033
Fixed assets	1,019			1,019
Accruals and provisions	5,625	-862	-306	4,457
Total deferred tax assets	11,406	3,070	-582	13,894
Offset against deferred liabilities	-4,639	1,487	-61	-3,212
Net deferred tax assets	6,767			10,682
Deferred tax liabilities				
Fixed assets	2,738	-563	56	2,231
Accruals and provisions	3,524	-1,100	-169	2,255
Total deferred tax liabilities	6,262	-1,664	-112	4,486
Offset against deferred tax assets	-4,639	1,487	-61	-3,212
Net deferred tax liabilities	1,623			1,274

On December 31, 2024 the Group had EUR 64.7 million losses carried forward that are available to be offset against future taxable profits in the companies in which the losses have been generated. Cumulative tax losses will expire after the next five years and the rest will expire later or never. Deferred tax asset has been recognized for losses in total of EUR 28.2 million.

20 Provisions

EUR 1,000	Consolidated	
	2024	2023
Provision at 1.1.	3,486	
Provision for the period		9,046
Provision reversed	-813	-263
Provision used	-2,673	-5,298
Total 31.12.	0	3,486

Provision was related to restructuring in the last quarter of 2023.

21 Other liabilities

EUR 1,000	Consolidated	
	2024	2023
Material amounts shown under accrued expenses		
Accrued personnel expenses	4,314	8,802
Deferred royalty	58	96
Other accrued expenses	2,323	3,406
Total	6,694	12,303

22 Contingent liabilities

EUR 1,000	Consolidated	
	2024	2023
Guarantees for other group companies		
Other liabilities	110	110

23 Related party disclosures

The Group's related parties include members of the Board, CEO and members of the Leadership Team as well as their close family members and entities where the aforementioned persons have either control or shared control.

EUR 1,000	Consolidated	
	2024	2023
CEO		
Wages and other short-term employee benefits	342	510
Share-based payments	266	
Post-employment benefits	58	81
Termination benefits	175	
Total	841	591
Leadership Team		
Wages and other short-term employee benefits	1,480	2,132
Share-based payments	54	437
Post-employment benefits	210	296
Termination benefits		221
Total	1,745	3,086
Members of the Boards of Directors		
Wages and other short-term employee benefits	315	313
Total	315	313
Total	2,900	3,989

Board of Directors 2024 and Managing Director

EUR 1,000	Wages	Fees
Antti Koskela, Managing Director (8 April 2024–)	231	
Juhani Hintikka, Managing Director (1 January–8 April 2024)	111	
Risto Siilasmaa, Chair of the Board		80
Tuomas Syrjänen		48
Kirsi Sormunen		48
Ciaran Martin		42
Amanda Bedborough		40
Niilo Fredrikson		38
Harri Ruusinen		13
Keith Bannister		3
Päivi Rekonen		3
Total	342	315

Share-based payments granted to the CEO are presented at the IFRS 2 expense of the share plans. The share-based payments are equity-settled and are measured at the fair value of the WithSecure Corporation share on the date they were granted. The cost is recognized over the period in which the performance conditions are fulfilled (earning period).

The CEO's retirement age and the determination of his pension conform to the standard rules specified by Finland's Employee Pension Act (TYEL). The pension cost of the CEO during the period was 58 thousand euro (81 thousand euro in year 2023). The period of notice for the CEO is six (6) months both ways and CEO is entitled to severance payment equivalent of six (6) months' salary.

24 Subsidiaries

Name	Country of incorporation	Group (%)
WithSecure A/S, Copenhagen	Denmark	100.00
WithSecure AB, Stockholm	Sweden	100.00
WithSecure B.V., Utrecht	The Netherlands	100.00
WithSecure BV, Heverlee-Leuven	Belgium	100.00
WithSecure Cyber Security Services Oy, Helsinki	Finland	100.00
WithSecure GmbH, Munich	Germany	100.00
WithSecure Inc., Camden	United States	100.00
WithSecure KK, Tokyo	Japan	100.00
WithSecure Limited, Basingstoke	United Kingdom	100.00
WithSecure Norge AS, Oslo	Norway	100.00
WithSecure Pte. Ltd., Singapore	Singapore	100.00
WithSecure SARL, Maisons-Laffitte	France	100.00
WithSecure Sdn Bhd, Kuala Lumpur	Malaysia	100.00
WithSecure SP. z.o.o., Poznan	Poland	100.00
WithSecure Srl, Milano	Italy	100.00
Bytegeist GmbH, Oldenburg	Germany	100.00
F-Secure Software (Shanghai) Co Ltd, Shanghai	China	100.00
F-Secure Digital Assurance Ltd, Basingstoke	United Kingdom	100.00
F-Secure Informatica S de RL de CV, Mexico City	Mexico	99.41
F-Secure Argentina S.R.L., Buenos Aires	Argentina	95.00

25 Events after period end

WithSecure Corporation has signed 23.1.2025 a share purchase agreement, under which its cyber security consulting business will be sold to Neqst.

The transaction is executed by the sale of shares of the parent company of a to-be-established WithSecure cyber security consulting group, to which the consulting business will be transferred prior to the completion of the transaction. As a result of the agreement, total of approximately 250 employees located in Finland, UK, Sweden, Denmark, Singapore, Italy, and US are expected to transfer to the buyer.

The parties have agreed on a total enterprise value of EUR 22.5 million. Of this, 60% becomes payable as fixed cash and debt-free purchase price upon completion of the transaction. The remaining 40% is variable purchase price, based on the performance of the business in 2025 and 2026, and it becomes payable in two installments in the beginning of 2026 and 2027.

The transaction is expected to be completed during the second quarter of 2025. The completion of the transaction is subject to customary closing conditions and regulatory approvals.



WithSecure Corporation Financial Statements

Income statement January 1 - December 31, 2024

EUR	Note	2024	2023
REVENUE	1	93,886,376.27	79,051,349.83
Cost of revenue	4	-19,092,710.79	-18,928,442.47
GROSS MARGIN		74,793,665.48	60,122,907.36
Other operating income	2	9,893,550.02	15,892,880.57
Sales and marketing	3,4	-46,227,375.47	-46,255,012.90
Research and development	3,4	-37,285,770.96	-43,260,260.15
Administration	3,4	-14,344,593.01	-18,575,859.70
EBIT		-13,170,523.93	-32,075,344.81
Financial income and expenses	6	-32,426,503.12	2,409,113.80
PROFIT (LOSS) BEFORE APPROPRIATIONS AND TAXES		-45,597,027.05	-29,666,231.01
Appropriations	7		3,456,219.00
Income taxes	8	1,630,704.39	3,044,675.81
RESULT FOR THE FINANCIAL YEAR		-43,966,322.66	-23,165,336.20

Balance sheet December 31, 2024

ASSETS				SHAREHOLDERS' EQUITY AND LIABILITIES			
EUR	Note	2024	2023	EUR	Note	2024	2023
NON-CURRENT ASSETS				SHAREHOLDERS' EQUITY			
Intangible assets	9	12,298,700.99	14,238,999.72		15,16		
Tangible assets	9	2,338,234.33	843,111.47	Share capital		80,000.00	80,000.00
Investments in group companies	10	87,488,261.37	121,565,483.93	Share premium			
Long-term receivables	12	21,331.35	8,325,632.42	Treasury shares		-154,558.06	-154,558.06
Total non-current assets		102,146,528.04	144,973,227.54	Reserve for invested unrestricted equity		84,438,441.61	84,438,441.61
CURRENT ASSETS				Retained earnings		46,503,953.42	69,669,289.62
Trade and other receivables	12	51,501,443.22	41,269,461.75	Profit for the financial year		-43,966,322.66	-23,165,336.20
Deferred tax assets	11	7,165,534.05	5,384,977.72	Total shareholders' equity		86,901,514.31	130,867,836.97
Short-term investments	13	26,071.99	26,071.99	APPROPRIATIONS			
Cash and cash equivalents	14	14,377,201.30	27,855,507.07	Depreciation reserve		90,614.56	90,614.56
Total current assets		73,070,250.56	74,536,018.53	LIABILITIES			
TOTAL ASSETS		175,216,778.60	219,509,246.07	Long-term liabilities	17	22,729,283.39	25,693,038.53
				Short-term liabilities	17	65,495,366.34	62,857,756.01
				Total liabilities		88,224,649.73	88,550,794.54
				TOTAL SHAREHOLDERS' EQUITY AND LIABILITIES		175,216,778.60	219,509,246.07

Cash flow statement January 1 - December 31, 2024

EUR 1,000	2024	2023
Cash flow from operations		
Result for the financial year	-43,966	-23,165
Adjustments		
Depreciation and amortization	4,300	4,091
Profit / loss on sale of fixed assets	149	5
Other adjustments	21	4,600
Financial income and expenses	32,427	-2,409
Income taxes	-1,631	-3,045
Cash flow from operations before change in working capital	-8,700	-19,924
Change in net working capital		
Current receivables, increase (-), decrease (+)	-2,229	-3,746
Non-interest bearing debt, increase (+), decrease (-)	-1,713	-1,610
Cash flow from operations before financial items and taxes	-12,643	-25,280
Interest expenses paid	-160	-144
Interest income received	2,262	2,705
Other financial income and expenses	-1,075	-570
Income taxes paid	-150	-110
Cash flow from operations	-11,765	-23,399

EUR 1,000	2024	2023
Cash flow from investments		
Investments in intangible and tangible assets	-4,075	-5,991
Proceeds from sale of intangible and tangible assets	71	111
Proceeds from sale of business	301	
Dividends received		150
Investments in financial assets ¹		13,977
Cash flow from investments	-3,703	8,247
Cash flow from financing activities		
Increase / Decrease in Intra Group liabilities	1,978	530
Cash flow from financing activities	1,978	530
Change in cash	-13,490	-14,622
Effect of exchange rate changes on cash	12	-60
Cash and bank at the beginning of the period	27,855	42,537
Cash and bank at period end	14,377	27,855

¹ Investments in financial assets include Group's investments in financial assets measured at amortized cost, such as corporate commercial papers. Investments in short term money market instruments with maturity less than three months are presented as Cash and cash equivalents.

Notes to the parent company Financial Statements

Accounting principles for the parent company financial statements

Basic information

WithSecure provides cyber security products and services globally for businesses.

WithSecure Corporation (previously known as F-Secure Corporation) is the parent company of WithSecure Group, incorporated in Finland and domiciled in Helsinki. Company's registered address is Välimerenkatu 1, 00180 Helsinki. Copy of consolidated financial statements can be downloaded from www.withsecure.com or can be received from the Company's registered address.

Accounting principles

The financial statements of WithSecure Corporation has been prepared in accordance with Finnish Accounting Standards (FAS).

Foreign currency translation

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

Revenue recognition

From 1 January 2024 onwards, WithSecure Group has reported three business areas: Elements Company, Cloud Protection for Salesforce (CPSF) and Cyber security consulting which is also reflected in the revenue reporting.

Elements Company includes Elements Cloud products and services, Managed services (including Countercept Managed Detection and Response, MDR), On-

premise, and Other products. Elements Company revenue is presented separately for Cloud, On-premise and Other products.

Cloud Protection for Salesforce (CPSF) includes revenue from the CPSF product. It is a software product, ensuring scanning of external content for potential malware, before it is loaded into Salesforce. Customers are primarily enterprise-sized companies, with extensive use of Salesforce platforms.

Cyber security consulting includes the consulting services sold to large enterprise customers.

Cloud-based Elements products and services, Managed services and CPSF are sold as recurring Software-as-a-Service (SaaS). On-premise products are sold by granting the customer access to use the intellectual property during the license period. WithSecure delivers the product and provides continuous automated updates against new threats. The software and the accompanied services are highly interdependent and therefore treated as one performance obligation for which revenue is recognized over time on a straight-line basis for the contract period. Cyber security consulting services are recognized as revenue based on the delivery of the work.

Cloud-based products and services and on-premise security products are provided either as a continuous service or for a fixed term. Continuous services are invoiced on a monthly basis and fixed term fully upfront or monthly, quarterly or annually upfront. Cyber security consulting services are invoiced as agreed with the customer. The standard payment term within the Group is 30 days period.

Presentation of receivables and liabilities from contracts with customers

Receivables from contracts with customers are presented in the balance sheet as *Accrued income*. Liabilities from contracts with customers are presented in the balance sheet as *Deferred revenue* and included in *Total non-current liabilities* or *Total current liabilities* depending on the duration of the liability.

Pensions

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

Leases

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

Income taxes

Current income taxes are calculated in accordance with the local tax and accounting rules. Deferred tax assets from losses carried forward are recognized to the extent that it is probable that future taxable profit will be available.

Tangible and intangible assets

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

Machinery and equipment	3–8 years
Capitalized development costs	3–8 years
Intangible rights	3–8 years
Intangible assets	5–10 years

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

Research and development expenditure

Research expenditure is recognized as an expense at the time it is incurred. Development expenditures are capitalized as intangible assets.

Financial assets and liabilities

Cash and cash equivalents in the balance sheet comprise cash at bank and in hand and other highly liquid short-term investments.

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

Treasury shares

The company has acquired treasury shares in 2008–2011. The purchase price of the shares has been deducted from equity.

Share-based payment transactions

WithSecure provides incentives to employees in the form of equity-settled share-based instruments. Currently the Company has share-based programs.

WithSecure's share-based incentive programs are targeted to the Group's management and key personnel. In addition, employee share savings plan was launched in 2022 for all employees. The programs are equity-settled and recognized in the Company's equity on vesting date.

Presentation of expenses

Classification of the functionally presented expenses has been made by presenting direct expenses in their respective functions and by allocating other expenses to operations on the basis of average headcount in each function.

1 Revenue

EUR 1,000	2024	2023
Geographical information		
Nordic countries	27,514	23,454
Europe excl. Nordics	6,488	42,931
North America	48,360	1,379
Rest of the world	11,525	11,287
Total	93,886	79,051

2 Other operating income

EUR 1,000	2024	2023
Service fees charged from F-Secure under TSA		6,939
Rental revenue	1,621	1,489
Government grants	274	543
Other	7,999	6,922
Total	9,894	15,893

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

Other category includes administrative and other fees charged from group companies.

3 Depreciation, amortization, and impairment

EUR 1,000	2024	2023
Depreciation and amortization of non-current assets		
Other intangible assets	-1,017	-762
Capitalized development	-2,961	-3,073
Intangible assets	-3,978	-3,834
Machinery and equipment		
	-322	-256
Tangible assets	-322	-256
Total depreciation and amortization	-4,300	-4,091
Depreciation and amortization by function		
Sales and marketing	-231	-124
Research and development	-3,667	-3,605
Administration	-401	-362
Total depreciation and amortization	-4,300	-4,091

4 Personnel expenses

EUR 1,000	2024	2023
Personnel expenses		
Wages and salaries	-32,448	-36,205
Pension expenses	-5,813	-5,885
Other social expenses	-679	-1,945
Total	-38,940	-44,036

Compensation of key management personnel

EUR 1,000	2024	2023
Wages and other short-term employee benefits	-2,137	-2,415
Wages and other short-term employee benefits		
Managing Directors	342	510
Members of the Board of Directors	315	313

Wages and other short-term employee benefits of the Board of Directors and Managing Director: see group disclosure [23 Related party disclosures](#).

The Managing Director's retirement age and the determination of his pension conform to the standard rules specified by Finland's Employee Pension Act (TYEL). The pension cost of the Managing Director over the period was 58 thousand euro (81 thousand euro in year 2023). The period of notice for the Managing Director is six (6) months both ways and Managing Director is entitled to severance payment equivalent of six (6) months' salary.

	2024	2023
Average number of personnel	408	463
Personnel by function Dec 31		
Consulting and delivery	24	42
Sales and marketing	89	110
Research and development	211	228
Administration	60	61
Total	384	441

5 Audit fees

EUR 1,000	2024	2023
Auditing, PricewaterhouseCoopers	-147	-131
Other actions referred to in section 1, subsection 1, paragraph 2 of the Auditing Act, PricewaterhouseCoopers	-29	-22
Other Services, PricewaterhouseCoopers	-91	
Total	-267	-153

6 Financial income and expenses

EUR 1,000	2024	2023
Interest income	2,262	2,705
Interest expense	-160	-144
Other financial income	2	2
Dividends		150
Exchange gains (+) and losses (-)	303	-130
Impairment of non-current investments	-34,600	
Other financial expenses	-233	-173
Total	-32,427	2,409

Impairment of non-current investments relates to WithSecure Limited. It's shares have been written down during the financial year.

7 Appropriations

EUR 1,000	2024	2023
Group contribution		3,456
Total		3,456

8 Income taxes

EUR 1,000	2024	2023
Income tax for the year	-140	-177
Adjustments for income tax of prior periods	-10	-32
Deferred tax	1,781	3,253
Total	1,631	3,045
Result before appropriations and tax	-45,597	-29,666

9 Non-current assets

EUR 1,000	Intangible assets			Tangible assets			
	Other intangible	Capitalized development	Incomplete development	Total	Machinery & equip.	Other tangible	Total
Acquisition cost Jan 1, 2022	8,844	28,422	1,441	38,706	4,810	5	4,816
Additions	2,544		3,007	5,551	333		333
Transfers		674	-674				0
Disposals					-16		-16
Acquisition cost Dec 31, 2023	11,389	29,096	3,773	44,258	5,127	5	5,133
Additions	346		1,716	2,062	2,013		2,013
Transfers		1,639	-1,639	0			
Disposals	-785			-785	-2,502	-5	-2,507
Acquisition cost Dec 31, 2024	10,949	30,735	3,850	45,534	4,638	0	4,639
Acc. depreciation Jan 1, 2022	-7,005	-19,181		-26,185	-4,040		-4,040
Depreciation for the period	-762	-3,073		-3,834	-256		-256
Acc. depreciation of disposals					7		7
Acc. depreciation Dec 31, 2023	-7,766	-22,253		-30,019	-4,289		-4,289
Depreciation for the period	-1,017	-2,961		-3,978	-322		-322
Acc. depreciation of disposals	762			762	2,311		2,311
Acc. depreciation Dec 31, 2024	-8,022	-25,215		-33,236	-2,300		-2,300
Book value as at Dec 31, 2023	3,622	6,844	3,773	14,239	838	5	843
Book value as at Dec 31, 2024	2,927	5,522	3,850	12,299	2,338	0	2,338

10 Investments in group companies

EUR 1,000	Shares in group companies	Total
Book value as at Jan 1	121,565	121,565
Additions	524	524
Decreases	-34,601	
Book value as at Dec 31	87,488	122,089

Name	Country of incorporation	Share of ownership (%)
Parent WithSecure Corporation, Helsinki	Finland	
WithSecure A/S, Copenhagen	Denmark	100
WithSecure AB, Stockholm	Sweden	100
WithSecure B.V., Utrecht	The Netherlands	100
WithSecure BV, Heverlee-Leuven	Belgium	100
WithSecure GmbH, Munich	Germany	100
WithSecure KK, Tokyo	Japan	100
WithSecure Limited, Basingstoke	United Kingdom	100
WithSecure SARL, Maisons-Laffitte	France	100
WithSecure Sdn. Bhd., Kuala Lumpur	Malaysia	100
WithSecure Sp. z o.o., Poznan	Poland	100
WithSecure Srl, Milan	Italy	100
F-Secure Argentina SRL, Buenos Aires	Argentina	95
F-Secure Digital Assurance Ltd, Basingstoke	United Kingdom	100
F-Secure Software (Shanghai) Co Ltd, Shanghai	China	100

11 Deferred tax

EUR 1,000	2024	2023
Deferred tax assets	7,166	5,385
Total	7,166	5,385

12 Receivables

EUR 1,000	2024	2023
Non-current receivables		
Other receivables	21	72
Total	21	72
Receivables from group companies		
Loan receivables		8,254
Total		8,254
Non-current receivables total	21	8,326
Current receivables		
Trade receivables	12,329	12,316
Loan receivables	53	53
Other receivables	39	135
Prepaid expenses and accrued income	5,166	5,462
Total	17,587	17,966
Receivables from group companies		
Trade receivables	12,414	9,099
Loan receivables	19,331	10,068
Other receivables	2,009	4,021
Prepaid expenses and accrued income	160	116
Total	33,915	23,303
Current receivables total	51,501	41,269
Material items included in prepaid expenses and accrued income		
Prepaid royalty	2,003	2,015

EUR 1,000	2024	2023
Grant receivables	413	279
Other prepaid expenses	2,435	2,641
Accrued income	315	527
Total	5,166	5,462

13 Short-term investments

EUR 1,000	2024	2023
Fair value as at Jan 1	26	26
Fair value as at Dec 31	26	26
Shares - unlisted	26	26
Fair value as at Dec 31	26	26
Original purchase price as at Dec 31	26	26

14 Cash and short-term deposits

EUR 1,000	2024	2023
Cash at bank and in hand	14,377	27,856

Cash at bank in 2023 includes also investments in short term deposits with maturity of less than 3 months (EUR 15 million).

15 Statement of changes in shareholders' equity

Parent Company						
EUR 1,000	Share capital	Treasury shares	Unrestricted equity reserve	Retained earnings	Total equity	
Equity Dec 31, 2022	80	-155	84,439	69,670	154,033	
Result of the financial year				-23,165	-23,165	
Equity Dec 31, 2023	80	-155	84,439	46,505	130,868	
Result of the financial year				-43,966	-43,966	
Equity Dec 31, 2024	80	-155	84,439	2,539	86,902	

16 Shareholders' equity

The company's share capital amounted to 80,000.00 euros, and the number of shares was 176,098,739 at the end of the year 2024.

See group disclosure [14 Shareholder's Equity](#).

Treasury shares

See group disclosure [14 Shareholder's Equity](#).

Distributable shareholders' equity on December 31, 2024	
EUR 1,000	
Unrestricted equity reserve	84,439
Retained earnings	46,349
Result of the financial year	-43,966
Less capitalized development expense	-9,371
Distributable shareholders' equity on December 31, 2024	77,450

17 Liabilities

EUR 1,000	2024	2023
Non-current liabilities		
Deferred revenue	13,435	15,862
Other liabilities	93	
Total	13,528	15,862
Liabilities to the group companies		
Cashpool	9,201	7,223
Other liabilities		2,608
Total	9,201	9,832
Total non-current liabilities	22,729	25,693
Current liabilities		
Deferred revenue	31,306	30,336
Trade payables	3,010	3,064
Other liabilities	1,353	2,116
Accrued expenses	10,564	11,415
Total	46,234	46,932
Liabilities to the group companies		
Advance payments	669	1,308
Trade payables	13,504	12,397
Other liabilities	5,089	2,221
Total	19,262	15,926
Total current liabilities	65,495	62,858

EUR 1,000	2024	2023
Material amounts shown under accruals and deferred income		
Accrued personnel expenses	7,665	8,496
Deferred royalty	58	96
Accrued expenses	2,842	2,824
Total	10,564	11,415

18 Financial risk management

See Group disclosure [18 Management of financial risks](#).

19 Operating lease commitments

The Group has entered into commercial leases on office space and on motor vehicles. Motor vehicle leases have an average life of three years and office spaces between two and five years with renewal terms included in the contracts.

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

As lessee	2024	2023
EUR 1,000		
Within one year	2,576	3,912
After one year but not more than five years	19,290	200
Total	21,866	4,112

20 Contingent liabilities

EUR 1,000	2024	2023
Guarantees for other group companies	110	110

Signatures of the Board of Directors' report and Financial statements

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

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

Helsinki, February 11, 2025

Risto Siilasmaa
Chair

Tuomas Syrjänen

Kirsi Sormunen

Ciaran Marin

Amanda Bedborough

Niilo Fredriksson

Harri Ruusinen

Antti Koskela
Managing Director

Auditors' note

Our auditors' report has been issued today.

Helsinki, February 12, 2025

PricewaterhouseCoopers Oy
Authorized Public Accountants

Jukka Karinen
Authorized Public Accountant



To the Annual General Meeting of WithSecure Oyj

Report on the Audit of the Financial Statements (Translation of the Finnish Original)

Opinion

In our opinion

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

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

What we have audited

We have audited the financial statements of WithSecure Oyj (business identity code 0705579-2) for the year ended 31 December 2024. The financial statements comprise:

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

Basis for Opinion

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

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

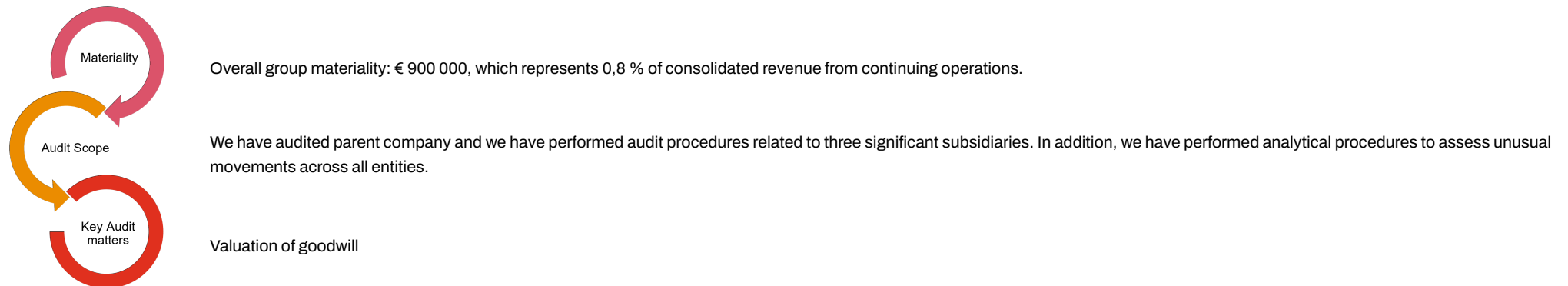
Independence

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

To the best of our knowledge and belief, the non-audit services that we have provided to the parent company and group companies are in accordance with the applicable law and regulations in Finland and we have not provided non-audit services that are prohibited under Article 5(1) of Regulation (EU) No 537/2014. The non-audit services that we have provided are disclosed in note 7 to the Financial Statements.

Our Audit Approach

Overview



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

Materiality

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

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

Overall group materiality	€ 900 000 (previous year €1 100 000)
How we determined it	0,8% of consolidated revenue from continuing operations
Rationale for the materiality benchmark applied	The groups profitability has been volatile during the last years due to restructuring related costs, significant investments in product development and a change in strategy. We chose revenue as the benchmark because, in our view, it is the benchmark against which the performance of the group is commonly measured by users and is a generally accepted benchmark. We chose 0,8% which is within the range of acceptable quantitative materiality thresholds in auditing standards.

How we tailored our group audit scope

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

The Group operates globally through several legal entities. The Group's sales are mainly generated by the parent company and we have audited the parent company as part of our audit of the consolidated financial statements. In addition, we have performed audit procedures related to three significant subsidiaries. We have considered that the remaining subsidiaries do not present a reasonable risk of material misstatement for consolidated financial statements and thus our procedures have been limited to analytical procedures performed at group level.

By performing the procedures above at the legal entities, combined with additional procedures at the group level, we have obtained sufficient and appropriate evidence regarding the financial information of the group as a whole to provide a basis for our opinion on the consolidated financial statements.

Key Audit Matters

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

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

Key audit matter in the audit of the group	How our audit addressed the key audit matter
<p>Valuation of goodwill</p> <p><i>Refer to accounting principles and note 12 for the consolidated financial statements.</i></p> <p>Goodwill is a significant item in the consolidated statement of financial position and amounted to €35.8 million as at 31 December 2024. During the financial year an impairment of €15.6 million was recognized for the goodwill related to Consulting business.</p> <p>As at 31 December 2024 the assets (including goodwill) related to Consulting have been classified as assets held for sale and measured at fair value less cost to sell. As a result an additional impairment of €13.3 million was recognized for the goodwill related to Consulting business. The remaining goodwill in the statement of financial position subject to annual impairment testing pertains solely to Elements Company business.</p> <p>Impairment testing of goodwill requires significant degree of management judgement, including identifying cash generating units, meaning the level at which the goodwill is tested, estimating the future profitability of the business and the discount rate applied for the expected future cash flows.</p> <p>Due to materiality and judgment associated we have considered valuation of goodwill as key audit matter in the audit of the group.</p>	<p>Our audit focused on assessing the appropriateness of management's judgment and estimates used in the goodwill impairment analysis through the following procedures:</p> <p>We tested the methodology applied in the value in use calculation by comparing it to the requirements of IAS 36, Impairment of Assets, and we tested the mathematical accuracy of calculation;</p> <p>We evaluated the process by which the future cash flow forecasts are drawn up, including comparing them to the latest Board approved targets and long-term plans</p> <p>We tested the key underlying assumptions for the cash flow forecasts, including sales and profitability forecasts, discount rate used and the implied growth rates beyond the forecasted period</p> <p>We compared the current year actual results included in the prior year impairment model to consider whether forecasts included assumptions that, with hindsight, had been optimistic</p> <p>We tested whether the sensitivity analysis performed by the management around key assumptions of the cash flow forecast are appropriate by considering the likelihood of the movements of these key assumptions.</p>
<p>We have no key audit matters to report with respect to our audit of the parent company financial statements</p>	
<p>There are no significant risks of material misstatement referred to in Article 10(2c) of Regulation (EU) No 537/2014 with respect to the consolidated financial statements or the parent company financial statements.</p>	

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

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

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

Auditor's Responsibilities for the Audit of the Financial Statements

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

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

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

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

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

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

Other Reporting Requirements

Appointment

We were first appointed as auditors by the annual general meeting on 7 April 2016. Our appointment represents a total period of uninterrupted engagement of nine years.

Other Information

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

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

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

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

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

Helsinki 12 February 2025

PricewaterhouseCoopers Oy

Authorised Public Accountants

Jukka Karinen

Authorised Public Accountant (KHT)



Assurance Report on the Sustainability Report (Translation of the Finnish Original)

To the Annual General Meeting of WithSecure Oyj

We have performed a limited assurance engagement on the group sustainability report of WithSecure Oyj (business identity code 0705579-2) that is referred to in Chapter 7 of the Accounting Act and that is included in the report of the Board of Directors for the reporting period 1.1.–31.12.2024.

Opinion

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

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

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

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

Basis for Opinion

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

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

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

Other Matter

We draw attention to the fact that the group sustainability report of WithSecure Oyj that is referred to in Chapter 7 of the Accounting Act has been prepared and assurance has been provided for it for the first time for the reporting period 1.1.–31.12.2024. Our opinion does not cover the comparative information that has been presented in the group sustainability report. Our opinion is not modified in respect of this matter.

Authorised Group Sustainability Auditor's Independence and Quality Management

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

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

Responsibilities of the Board of Directors and the Managing Director

The Board of Directors and the Managing Director of WithSecure Oyj are responsible for:

- the group sustainability report and for its preparation and presentation in accordance with the provisions of Chapter 7 of the Accounting Act, including the process that has been defined in the sustainability reporting standards and in which the information for reporting in accordance with the sustainability reporting standards has been identified
- the compliance of the group sustainability report with the requirements laid down in Article 8 of the Regulation (EU) 2020/852 of the European Parliament and of the Council on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088;
- such internal control as the Board of Directors and the Managing Director determine is necessary to enable the preparation of a group sustainability report that is free from material misstatement, whether due to fraud or error.

Inherent Limitations in the Preparation of a Sustainability Report

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

Responsibilities of the Authorised Group Sustainability Auditor

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

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

- Identify and assess the risks of material misstatement of the group sustainability report, whether due to fraud or error, and obtain an understanding of internal control relevant to the engagement in order to design assurance procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the parent company's or the group's internal control.
- Design and perform assurance procedures responsive to those risks to obtain evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.

Description of the Procedures That Have Been Performed

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

Our procedures included for example the following:

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

Helsinki 12 February, 2025

PricewaterhouseCoopers Oy

Authorised Sustainability Auditors

Jukka Karinen

Authorised Sustainability Auditor



Independent Auditor's Reasonable Assurance Report on WithSecure Oyj's ESEF Financial Statements

To the Management of WithSecure Oyj

We have been engaged by the Management of WithSecure Oyj (business identity code 0705579-2) (hereinafter also "the Company") to perform a reasonable assurance engagement on the Company's consolidated IFRS financial statements for the financial year 1 January – 31 December 2024 in European Single Electronic Format ("ESEF financial statements").

Management's Responsibility for the ESEF Financial Statements

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

Our Independence and Quality Management

We have complied with the independence and other ethical requirements of the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

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

Our Responsibility

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

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

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

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

Opinion

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

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

Helsinki 12 February 2025

PricewaterhouseCoopers Oy

Authorised Public Accountants

Jukka Karinen

Authorised Public Accountant (KHT)

WI



Corporate Governance

Contents

WithSecure's Corporate Governance Statement 2024	172
Corporate Governance at WithSecure	172
Governing bodies	172
Internal control and risk management	177
Risk Management	177
Internal Control	177
Internal audit	177
Related party transactions	178
Insider management	178
Auditors	178
Board of Directors	179
Global Leadership Team	183

WithSecure’s Corporate Governance Statement 2024

Corporate Governance at WithSecure

WithSecure’s corporate governance practices are based on applicable Finnish laws, the rules of Helsinki Stock Exchange (NASDAQ Helsinki Oy) and the regulations and guidelines of Finnish Financial Supervisory Authority as well as the company’s Articles of Association. This Corporate Governance Statement is issued separately from the Board of Directors’ report. The statement has been prepared in accordance with the Finnish Corporate Governance Code 2025 (publicly available at <http://cgfinland.fi/en/>) issued by the Securities Market Association of Finland.

Up-to-date information about WithSecure’s governance is available on the company’s website at <https://www.withsecure.com/en/about-us/investor-relations>.

Governing bodies

WithSecure’s highest decision-making body is the General Meeting of Shareholders which elects the members of the Board of Directors. The Board of Directors is responsible for the administration of WithSecure and appropriate organization of its operations. The Board of Directors appoints the CEO. The CEO, assisted by the Global Leadership Team, is responsible for managing the company’s business and implementing its strategic and operational targets.

WithSecure governing bodies



General Meeting of Shareholders

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

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

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

Each share carries one vote in the General Meeting.

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

The AGM was held on 20 March 2024.

The meeting was held as a hybrid meeting, so that shareholders were able to exercise their shareholder rights fully during the meeting either via remote connection or at the meeting venue at the address Tammasaarenkatu 7, 00180 Helsinki, Finland. Shareholders were also able to exercise their voting rights by voting in advance.

The resolutions and the meeting minutes of the AGM are available on WithSecure’s website.

Board of Directors

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

- approving the strategy of WithSecure, overseeing its operations and annual budgets
- appointing and dismissing the CEO
- approving any major investments, acquisitions, changes in corporate structure or other matters that are significant or far-reaching
- ensuring that the supervision of the company's accounting and financial management is duly organized
- Approving the sustainability report as well as the program-level priorities and objectives for sustainability
- ensuring that internal control and risk management systems are in place
- approving personnel policies and rewards systems
- election of the authorised sustainability auditor and the decision on the authorised sustainability auditor's remuneration
- preparing matters to be handled at the General Meeting

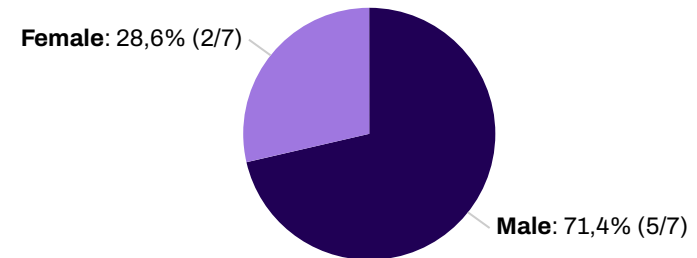
The Board of Directors meets as frequently as necessary and, according to the Board Charter, at least five times during its term. The Board of Directors has a quorum when more than half of the members are present. An annual self-assessment is carried out by the Board to evaluate its operations. The Board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

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

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

Board of Directors aim to strive towards appropriately balanced gender distribution. Both genders are represented in the Board of Directors.

Board gender diversity ratio



To create openness, one member of the Board of Directors is elected from among WithSecure's personnel. An election is arranged annually for WithSecure personnel and each permanent WithSecure employee is eligible to stand as a candidate. The Personnel Committee interviews three individuals who have obtained the highest number of votes in the elections and chooses a candidate from among them to be proposed for election as a member of the Board by the Annual General Meeting. Harri Ruusinen was appointed to the Board of Directors through this process in 2024.

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

In 2024 the Board of Directors convened 15 times, Audit Committee 5 times and Personnel Committee 6 times.

Members of the Board of Directors and the Committees

Member	Independence of the company	Independence of major shareholders	Board (Meeting attendance)	Audit Committee (Meeting attendance)	Personnel Committee (Meeting attendance)
Risto Siilasmaa	Yes	No ¹	Chair (15/15)	-	Member (6/6)
Tuomas Syrjänen	Yes	Yes	Member (15/15)	-	Chair (6/6)
Kirsi Sormunen	Yes	Yes	Member (15/15)	Chair (5/5)	-
Ciaran Martin	Yes	Yes	Member (13/15)	Member (4/5)	-
Amanda Bedborough as of 20 March 2024	Yes	Yes	Member (9/11)	Member (2/4)	-
Niilo Fredrikson as of 20 March 2024	Yes	Yes	Member (10/11)	-	Member (5/5)
Harri Ruusinen as of 20 March 2024	No ²	Yes	Member (9/11)	Member (4/4)	-
Päivi Rekonen until 20 March 2024	Yes	Yes	Member (3/4)	-	Member (1/1)
Keith Bannister until 20 March 2024	Yes	Yes	Member (4/4)	Member (1/1)	-
Camilla Perselli until 20 March 2024	No ³	Yes	Member (3/4)	Member (1/1)	-

¹ Risto Siilasmaa is the founder of WithSecure and on 31 December 2024 owned 34.11% of WithSecure shares.

² Harri Ruusinen was elected from among WithSecure's personnel in 2024, according to the process described above.

³ Camilla Perselli was elected from among WithSecure's personnel in 2023, according to the process described above.

Board Committees

In 2024, the Board established two committees: Audit Committee and Personnel Committee (nomination and remuneration matters). The Board of Directors appoints from among itself the members and the Chair of the committee. Each committee must have at least three members. The Board of Directors confirms the main duties and operating principles of each committee. The duties of each committee are defined in the committee charters which are available on WithSecure's website at <https://www.withsecure.com/en/about-us/investor-relations>.

Audit Committee

The Audit Committee reviews, instructs and evaluates risk management, internal supervision systems, IT strategy and practices, financial reporting as well as auditing of the accounts and internal auditing. Additionally, the Audit Committee monitors the progress and key results of the sustainability program. The Audit Committee is neither a decision-making nor an executive body. Audit Committee also prepares a proposal for the election of auditor to the Board of Directors and regularly considers the need for a separate internal audit function. Members of the Audit Committee must have broad business knowledge, as well as sufficient expertise and experience with respect to the committee's area of responsibility and the mandatory tasks relating to auditing. The majority of members of the Audit Committee shall be independent from WithSecure and at least one member shall be independent of the company's significant shareholders. A person who participates in the day-to-day management of WithSecure group companies (for example as the managing director) cannot be appointed to the Audit Committee. The Board elects the chair and secretary of the Audit Committee. The Audit Committee calls in experts to its meetings if they are necessary for the matters to be discussed. All members of the Board of Directors may, at their discretion, attend Audit Committee meetings. Materials of the Audit Committee meetings are made available for all members of the Board of Directors.

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

Personnel Committee

The Personnel Committee prepares material and instructs with issues related to the composition and compensation of the Board of Directors and remuneration of the other members of the top management of the company. The Committee assists in the preparation of Board proposals to the shareholders related to these matters,

as governed by the Finnish Limited Liability Companies Act. Personnel Committee is neither a decision-making nor an executive body. Personnel Committee calls in experts to its meetings when necessary for the issues to be discussed. Materials of Personnel Committee meetings are made available for all members of the Board of Directors.

The Personnel Committee convenes at least two times a year as notified by the Chair of the Committee. Members of the Personnel Committee are listed in the table above.

President and CEO

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

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

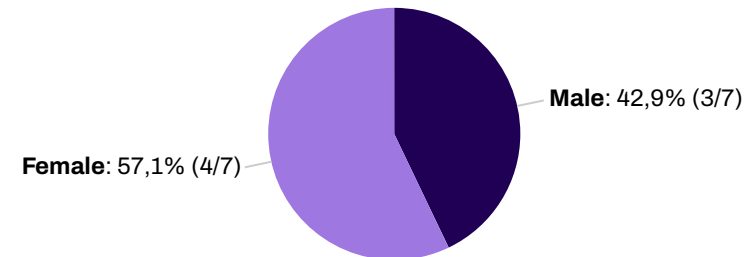
Juhani Hintikka acted as WithSecure's President and CEO until 8 April 2024. Antti Koskela was appointed as the interim CEO of WithSecure, effective 8 April 2024, and as the President and CEO of WithSecure, effective 1 July 2024.

The biographical details of the CEO including the shareholdings are specified later in this report. The remuneration of the CEO is specified in WithSecure's Remuneration Policy and Report.

Global Leadership Team

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

Global Leadership Team's gender diversity ration (including President and CEO)



Current information on the WithSecure Global Leadership Team can be found on our website at <https://www.withsecure.com/en/about-us/investor-relations>.

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

Internal control and risk management

Risk Management

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

WithSecure's Board of Directors defines the principles of risk management and internal controls which are followed within the company. The Audit Committee assists the Board in the supervision of WithSecure's risk management function. The CEO is accountable for ensuring that the risk management principles are implemented and applied constantly and consistently across the organization.

The primary goal of WithSecure's risk management principles is to empower the organization to identify and manage risks more effectively. The potential negative impact and probability of different situations arising from our business operations on the company, its customers, or its partners are monitored as part of the risk management process. Another objective of the risk management is to constantly monitor and pro-actively control the impact and/or probability of situations derived from our business operations which may have a negative impact on WithSecure, its customers, or its partners. Proactive monitoring, risk simulation and stress testing also allows building strategic resilience in the company and its business operations. Risk management may also be utilized to identify opportunities for benefit.

WithSecure promotes continuous risk evaluation by the company's personnel. The relevant operational risks identified through the risk management process are regularly reviewed by the CEO and Global Leadership Team and the company's statutory auditor. Risk Management is an integrated part of WithSecure's governance and management, and the risk management process is aligned with the ISO 31000 standard. The Audit Committee regularly conducts a review of top operational risks and evaluates the effectiveness of the risk management system.

Internal Control

Internal Control, supported by Risk Management, is an important element of WithSecure's management system. The Board of Directors is responsible for ensuring that the operating principles for internal control have been defined, and that the company monitors the functioning of internal control.

WithSecure has defined its objectives for internal control based on the globally applied principles. Internal control consists of e.g. policies, processes, procedures as well as control and monitoring activities. Internal Control is designed to provide reasonable assurance regarding the achievement of WithSecure's objectives in following categories:

- Effectiveness, efficiency and transparency of operations on all levels in accordance with the WithSecure strategy
- Reporting, including financial and sustainability, external and internal, to the Board, management, shareholders and stakeholders being complete, reliable, relevant and timely
- Compliance with applicable laws, regulations and WithSecure policies and instructions

WithSecure's Internal Control Operating Principles define the roles, design and practices of internal control. The principles provide guidance on how internal control is implemented at different levels, systems and amongst employees and outsourced functions. Internal control over financial reporting consists of risk identification and assessment, processes and internal control points and internal control monitoring and reporting.

Internal audit

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

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

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

To facilitate transparency and exchange of information on Internal Audit related matters, the financial management team has frequent meetings with the auditors. The Audit Committee also meets regularly with the auditors.

WithSecure provides an effective, objective, confidential and secure Whistleblowing Channel which allows both WithSecure employees and other stakeholders to express their concerns or suspicions openly and safely. The Whistleblowing Channel is available to all stakeholders 24/7. It is maintained by impartial and independent service provider to ensure objective and timely handling of reports.

Related party transactions

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

Insider management

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

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

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

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

Persons discharging managerial responsibilities comprise the Board of Directors, the CEO and other members of the Global Leadership Team. These persons have a duty to notify WithSecure and the Finnish Financial Supervisory Authority of every transaction in their own account relating to Financial Instruments of WithSecure within three business days. The company publishes these notifications as a stock exchange release, as specified by MAR. All releases published on managers' transactions are available on the company's website.

Auditors

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

In 2024 WithSecure Corporation has been audited by PricewaterhouseCoopers with Jukka Karinen, Authorized Public Accountant, as the responsible auditor.

WithSecure Corporation paid the auditor EUR 288,000 in audit fees (2023: EUR 210,000), EUR 29 000 (2023: EUR 22,000) in other actions referred to in section 1, subsection 1, paragraph 2 of the Auditing Act and EUR 91 000 (2023: EUR 0) in other Services.

Board of Directors



Risto Siilasmaa

Chair of the Board of since 2006
Born 1966, M. Sc. (Engineering)
Male

Main employment history:

Founder, President and CEO, Member of the Board, WithSecure, 1988–2006
Chair of the Board 2012–2020, Member of the Board 2008–2020, Interim CEO 2013–2014, Nokia Corporation
Chair of the Board, Elisa Corporation, 2008–2012
Chair of the Board 2016–2018, Vice-Chair of the Board 2007–2010 and 2013–2015, Member of the Board 2007–2019, The Federation of Finnish Technology Industries
Vice Chair of the Board 2017–2018, Member of the Board 2007–2010 and 2013–2018, Confederation of Finnish Industries EK
Chair of the Working Group, The Future of the Finnish General Conscription System, The Finnish Ministry of Defence, 2009–2010

Current board memberships and public duties:

Founder and Member of the Board, F-Secure Corporation, 2022–
Member of the Board, Hamina Wireless Oy, 2024–
Chair of the Aalto Fundraising Committee, 2023–
Member of the Board, CybExer Technologies, 2022–
Member of the Board, Quanscient Oy, 2022–
Chair of the Board, Upright Oy, 2022–
Member of the Board, Pixieray Oy, 2021–
Senior Advisor, Boston Consulting Group, 2020–
Member, International Advisory Board of IESE, 2019–
Member of the Board, Futurice Oy, 2018–
Founding Partner, Chair of the Board, First Fellow Partners, 2016–



Tuomas Syrjänen

Member of the Board since 2019
Chair of the Personnel Committee
Born 1976, M.Sc. (Engineering)
Male

Main employment history:

Data & AI Renewal, Futurice Oy, 2019–
CEO, Futurice Oy, 2008–2018
Head of Business Unit, Futurice Oy, 2003–2008
Business Development, Futurice Oy, 2001–2002

Current board memberships and public duties:

Chair of the Board 2024–, Member of the Board 2018–, Futurice Oy
Member of the Board, Vastuu Group Oy, 2023–
Chair of the Board 2022–2024, Member of the Board 2022–, Flow Technologies Oy
Member of the Board, Vaisala Corporation, 2019–



Kirsi Sormunen

Member of the Board since 2022
 Chair of the Audit Committee
 Born 1957, M.Sc. (Economics)
 Female

Main employment history:

Member of the Board, DNA Plc, 2014–2021
 Member of the Board, VR Group, 2017–2020
 Member of the Board, Sitra, 2013–2020
 Member of the Board, Neste Corporation, 2013–2017
 Vice President, CSR/Sustainability/CSO, Nokia Corporation, 2004–2014
 Various leadership positions in F&C, Nokia Corporation, 1993–2004

Current board memberships and public duties:

Member of the Board, Exel Composites, 2020–
 Senior Advisor, DIF / Directors Institute of Finland, 2016–



Ciaran Martin

Member of the Board since 2023
 Born 1974, MA, History
 Male

Main employment history:

Professor of Practice, Blavatnik School of Government, University of Oxford, 2020–
 Founding Chief Executive of the UK National Cyber Security Centre and Board Member of GCHQ, 2014–2020
 Director of Constitutional Policy, UK Government, 2011–2014
 Director of Security and Intelligence Policy, UK Government, 2008–2011
 Chief of Staff to the Head of the UK Civil Service and HM Treasury, 2002–2008
 Public spending roles, HM Treasury and National Audit Office UK, 1997–2005

Current board memberships and public duties:

Director of SANS CISO Network and Events, 2023–
 Advisory Board, RedSift (UK), 2022–
 Non-Executive Director, Our Future Health (UK, medical research charity), 2022–
 Advisory Board, CyberCX (Australia), 2021–
 Managing Director, Paladin Capital (United States), 2020–



Amanda Bedborough

Member of the Board since 2024

Born 1969

Female

Main employment history:

Chief Revenue Officer, DataCore Software, 2021 –

Senior Vice President, EMEA Operations, DataCore Software, 2015–2021

Senior Vice President, Global Strategy, DataCore Software, 2014–2015

Consultant and Business Advisor for Venture Capital, Private Equity and private companies, 2013 –2014

Executive Vice President, Global Sales & Field Marketing, Corel Corporation, 2009–2013

Executive Vice President, International Operations, Corel Corporation, 2003–2009

Executive Vice President, EMEA Operations, Corel Corporation, 2001–2003

Vice President, EMEA Operations, 3dfx Interactive, Inc., Slough, 1999–2001

International Sales & Marketing Director, STB Systems, Inc., Slough, 1993–1999

Current board memberships and public duties:

Operating Advisor, DN Capital, 2012–



Niilo Fredrikson

Member of the Board since 2024

Born 1980, M.Sc. (Engineering), M.Sc. (Economics)

Male

Main employment history:

CEO, Matrix42, 2024–

CEO, Efecte Plc, 2018–2024

Vice President, Nokia Corporation, 2018

Executive Vice President, Comptel, 2016 –2017

Various leadership positions, Microsoft, 2006–2016

Partner and head of unit, Ch5 Finland Oy, 2002–2005

Founder and CEO, Nobman Informatics Oy, 1999–2002

Current board memberships and public duties:

Member of the Board, Technology Industry Employers of Finland, 2024–



Harri Ruusinen

Member of the Board since 2024

Born 1979, B.Sc. (Business Information Technology)

Male

Main employment history:

Director, Sales Enablement and Engineering, WithSecure, 2025–

Director, Global Sales Engineering, WithSecure, 2020–2024

Director, North America Presales and Customer Success, WithSecure, 2019–2020

Solution Architect, Global Business Development, WithSecure, 2015–2019

Manager, Sales Engineering, Sales Nordics, WithSecure, 2015

Manager, Sales Engineering, Sales Finland, WithSecure, 2014–2015

Senior Sales Engineer, Sales Finland, WithSecure, 2006–2014

System Specialist, Finland, Fujitsu Services, 1996–2006

Non-current members

PÄIVI REKONEN

Board member from 2017 until March 2024

KEITH BANNISTER

Board member from 2020 until March 2024

CAMILLA PERSELLI

Board member from 2023 until March 2024

WithSecure shares owned by the members of the Board

Board member	Shareholding	
	31 December 2024	31 December 2023
Risto Siilasmaa	60,067,188	60,038,063
Tuomas Syrjänen	59,112	41,637
Kirsi Sormunen	33,427	15,952
Ciaran Martin	23,665	9,831
Niilo Fredrikson	16,972	-
Amanda Bedborough	13,834	-
Harri Ruusinen	27,678	-

Global Leadership Team



Antti Koskela

President and Chief Executive Officer
Born 1971, M.Sc. (Electrical Engineering)
Member of the Global Leadership Team since 2021
Male

Main employment history:

President and CEO, WithSecure, 2024–
Chief Product Officer, WithSecure, 2021–2024
Vice President, Business Development, Elisa Corporation, 2020–2021
CDO and Vice President, Nokia Software, 2018–2020
CTO and Executive Vice President, Comptel Corporation, 2011–2017
Various leadership positions, Nokia Siemens Networks, 2007–2011
Various leadership positions, Nokia Networks, 1999–2007

Current board memberships and public duties:

Member of the Board, QPR Software Corporation, 2021–



Christine Bejerasco

Chief Information Security Officer
Born 1982, B.Sc. (Computer Science)
Member of the Global Leadership Team since 2021
Female

Main employment history:

Chief Information Security Officer, WithSecure, 2023–Chief Technology Officer, WithSecure, 2021–2022
Vice President, Tactical Defense Unit, WithSecure, 2019–2021
Various technical & leadership roles, WithSecure, 2008–2019
Malware Researcher, PC Tools, 2006–2008
Various threat analysis positions, Trend Micro, 2003–2006



Lasse Gerdt

Chief Revenue Officer

Born 1974, M. Sc. (Telecommunications and Management)

Member of the Global Leadership Team since 2024

Male

Main employment history:

Chief Revenue Officer, WithSecure, 2025–

Chief Customer Officer, WithSecure, 2024

Head of Cloud/Azure Sales, Enterprise and Public Sector, Microsoft (Netherlands), 2022–2023

Director, Azure Sales, Global and Strategic Accounts, Microsoft (Netherlands), 2019–2021

Head of Strategic and Global Alliances, Amazon Web Services, EMEA HQ (Luxembourg), 2015–2019

Various Leadership Positions for Channel and SaaS Sales and Business Development, Microsoft (Finland), 2010–2014

Global Account Executive, Nokia, Microsoft (Finland), 2007–2010

VP Sales and Marketing, Cidercone Oy (Finland), 2002–2007

Global Accounts and Solution Sales Manager, Compaq Computer, 1998–2002

Current board memberships and public duties:

Member of Advisory Board, DeliwiAI, 2023–

Member of Advisory Board, Mannerheim-ristin ritarien säätiö Foundation, 2022–



Charlotte Guillou

Chief Culture and Performance Officer

Born 1978, M.A. (Adult Education)

Member of the Global Leadership Team since 2021

Female

Main employment history:

Chief Culture and Performance Officer, WithSecure, 2025–

Chief People Officer, WithSecure, 2021–2024

Various leadership positions in human resources, OP Financial Group, 2018–2021

HR & Change Lead for Finance, KONE Corporation, 2018

Country Manager North, Scan-Horse A/S, 2017–2018

Various leadership positions in human resources, Fiskars Group, 2013–2017

Various leadership positions in human resources, Nokia Corporation, 2007–2012

Management Consultant, Deloitte Finland, 2004–2007

HRD Consultant, Psykologitoimisto Cresco, 2000–2003



Tom Jansson

Chief Financial Officer

Born 1968, M.Sc. (Econ.)

Member of the Global Leadership Team since 2021

Male

Main employment history:

Chief Financial Officer, WithSecure, 2021–

CFO, Posti Group Corporation, 2018–2021

CFO, Comptel Corporation, 2013–2017

Various leadership & finance positions, Tellabs Inc., 1994–2013



Tiina Sarhimaa

Chief Legal Officer

Born 1976, LL.M.

Member of the Global Leadership Team since 2021

Female

Main employment history:

Chief Legal Officer, WithSecure, 2021–

Vice President, General Counsel, WithSecure, 2018–2021

Director, Legal and Compliance, Nokia Corporation, 2017–2018

General Counsel, Head of Legal, Comptel Corporation, 2015–2017

Legal Counsel, Comptel Corporation, 2004–2015

Legal Counsel, HEX Corporation, 2002–2003



Pilvi Tunturi

Chief Customer Officer

Born 1976, M.Sc. (Information Processing Science)

Member of GlobalLeadership team since 2024

Female

Main employment history:

Chief Customer Officer, WithSecure, 2025–

Interim Chief Product Officer, WithSecure, 2024

Vice President (different R&D roles), WithSecure, 2021–2024

Principal Architect, WithSecure, 2019–2021

Various technical & leadership roles in Oulu & Kuala Lumpur, WithSecure, 2004–2019

Changes in Global Leadership Team composition

On 8 April 2024, Juhani Hintikka, President and CEO of WithSecure, announced that he steps down from his position in the company. The decision to step down follows the Supreme Court ruling of 5 April 2024 where Juhani Hintikka was found guilty of abuse of inside information related to a matter dating back to 2014, years before he joined WithSecure. The Board of Directors appointed Antti Koskela to act as the interim CEO of the company. As of 1 July 2024, Antti Koskela was appointed as President and CEO of WithSecure. Pilvi Tunturi was appointed as interim Chief Product Officer.

As of 1 November 2024, following the organizational updates of WithSecure, Scott Reininga's position ceased to be a part of the Global Leadership Team.

At the end of the year, the composition of the Global Leadership Team was the following: Antti Koskela (President and CEO), Christine Bejerasco (Chief Information Security Officer), Lasse Gerdt (Chief Customer Officer), Charlotte Guillou (Chief People Officer), Tom Jansson (Chief Financial Officer), Tiina Sarhimaa (Chief Legal Officer), Pilvi Tunturi (interim Chief Product Officer), and Ari Väänttinen (Chief Marketing Officer).

On 1 January 2025, following the organizational updates of WithSecure, Charlotte Guillou became Chief Culture and Performance Officer, Lasse Gerdt became Chief Revenue Officer, and Pilvi Tunturi became Chief Customer Officer. Nina Laaksonen and Artturi Lehtiö are sharing the Chief Product Officer responsibilities as interim arrangement. On 1 January 2025, Ari Väänttinen left the company and Global Leadership Team.

Non-current members

JUHANI HINTIKKA

President and Chief Executive Officer – until April 2024

SCOTT REININGA

EVP, Global Consulting – until October 2024

ARI VÄÄNTTINEN

Chief Marketing Officer – until December 2024

WithSecure shares owned by the members of the Global Leadership Team

Global Leadership Team Member	Shareholding	
	31 December 2024	31 December 2023
Antti Koskela	90,476	63,767
Christine Bejerasco	90,517	90,517
Lasse Gerdt	-	-
Charlotte Guillou	61,267	61,267
Tom Jansson	61,267	61,267
Tiina Sarhimaa	77,583	77,583
Pilvi Tunturi	37,861	-



Remuneration Report

Contents

Letter of the Chair of the Personnel Committee	189
Remuneration of the Executives and company performance during the last five financial years	191
Remuneration of the Board of Directors	192
Remuneration of the President and CEO	193
President and CEO Pay mix 2024	194
Short-term incentive (STI)	195
Long-term incentive (LTI)	196
Key terms of service of the President and CEO	197

Letter of the Chair of the Personnel Committee

Dear Shareholders,

On behalf of WithSecure's Personnel Committee, I am pleased to share the Remuneration report for 2024. The report presents remuneration paid in 2024 to the Board members and the President and CEO in line with the Remuneration Policy approved at the Annual General Meeting 2021. WithSecure Remuneration Policy and the Remuneration Report comply with the EU Shareholder Rights Directive (SHRD) and Finnish Corporate Governance Code 2025.

The purpose of the Personnel Committee is to ensure that the variety of remuneration programs and elements reinforce the execution of the business strategy, support paying for performance and ensure that the remuneration is designed to be competitive in comparison to relevant peer groups. The other focus areas of our personnel Committee are the organization culture and value development, and talent development.

The remuneration principles in WithSecure have been defined so that the remuneration programs promote the business objectives and long-term shareholder value creation as well as long-term profitability of the company. For the President and the CEO this means that a significant part of the remuneration is based on performance. If targets are met, the short- and long-term incentives comprise approximately 57% of the total remuneration of the President and the CEO, as defined in the WithSecure Remuneration Policy 2021-2024. In 2024, the short-term incentive plans were tied to the company's revenue and profitability and the ongoing performance based long-term incentive plans to increase the total shareholder value and to revenue growth.

WithSecure's financial performance in 2024 was impacted by the continued economic uncertainty in the European markets, as well as the tense competition in the cyber security industry. WithSecure's total revenue grew by approximately 3% year-on-year. Revenue growth of the Continued operations (after elimination of the Cyber security consulting that will be divested), was approximately 5%. Revenue growth is primarily driven by our cloud-based Elements products and services, as well as the Cloud Protection for Salesforce product. The growth is offset by decline in the on-premise and other legacy products, due to the customers' transformation to cloud environments. WithSecure has been systematically working on improving its profitability for the past couple of years. In 2024, the Adjusted EBITDA of WithSecure (before split to Continuing and Discontinued operations) was EUR 3.1 million, which indicates a significant improvement from the previous year (EUR -16.1 million).

Our well-established remuneration principles will remain the same as in 2024. We have gone through a large transformation of our strategy, structure, and financials and will continue to drive profitable growth as well as the positive development of the shareholder value.

Engaged and competent people are imperative to our success and our purpose is to create a place of work where colleagues can thrive both personally and professionally to drive the success of our business. We offer our people an inclusive, flexible and caring workplace built on our values. We continue to invest in the development of our people with the aim to offer equal and inspiring opportunities to learn and grow.



We will continue with our comprehensive offers of STI and LTI programs. Aside of the current STI program offerings mainly to the sales employees and employees in the managerial roles, we will offer profit sharing programs for all employees who are not covered in STI programs. We will also continue the Employee Share Savings Plan for a new plan period. The aim of this long-term incentive plan is to increase the alignment of shareholders and our people and to offer an attractive opportunity to benefit from the company's success to all employees. In the new

plan period, we have increased the company's share matching prorated to employee's purchased shares from one for two to one for one.

We are positively looking into 2025 and our focus is on building the growth mindset and experimentation culture and driving towards further growth and profitability.

Chair of the Personnel Committee

Tuomas Syrjänen

Remuneration of the Executives and company performance during the last five financial years

The development of WithSecure's compensation and financial performance in 2020–2024 is described in the table below. The remuneration of the Board of Directors has stayed on the same level since 2018. The total remuneration of the President and CEO has varied year by year as a significant part of the remuneration is tied to the company's financial performance.

Average annual remuneration (EUR)	2020	2021	2022	2023	2024	
					Juhani Hintikka (1 Jan - 8 Apr)	Antti Koskela (8 Apr - 31 Dec)
<i>President and CEO¹</i>	482,863	375,327	555,519	509,923	203,032	231,207
<i>Chair of the Board</i>	80,000	80,519	80,000	80,000		80,000
<i>Other Board Members²</i>	40,000	44,508	44,000	43,800		43,200
<i>Average employee³</i>	61,832	67,443	74,158	82,797		78,109
Financial Performance (EUR million)⁴						
<i>Revenue⁵</i>	220	130	135	143		147
<i>Adjusted EBITDA⁵</i>	36	-11	-23	-16		3

¹ Remuneration paid during the financial year, including the base salary as well as short- and long-term incentives.

² Average remunerations paid to the Board Members, excluding the employee representative and members until 20.3.2024.

³ Total wages and salaries of the calendar year / average headcount during the year in all countries. Year 2020 include the consumer security (F-Secure). 2021 and 2022 are restated to include only WithSecure.

⁴ Year 2023 and 2024 figures include cyber security consulting business, to be divested in 2025.

⁵ Year 2020 include the consumer security (F-Secure). 2021 and 2022 are restated to include only WithSecure.

Remuneration of the Board of Directors

The Annual General Meeting decided on March 20, 2024 that the Board of Directors is paid fixed annual compensation for the term ending at the end of the next Annual General Meeting. The annual fee for the Chairman of the Board is EUR 80,000, for the Committee Chairs EUR 48,000, for Members of the Board EUR 38,000, and for a Board Member belonging to the personnel of the company EUR 12,667.

The Annual General Meeting decided that approximately 40% of the annual remuneration is paid in WithSecure's shares repurchased from the market. There are no special terms or conditions associated with owning the shares received as remuneration. The company will pay any applicable transfer tax arising from remuneration paid in shares.

For the Members of the Board of Directors, changes in the holdings of the company shares and rewards paid in shares are reported according to the

Market Abuse Regulation. Related stock exchange releases are available on the company's website.

A separate meeting fee of EUR 1,000 is paid to the Board members travelling from another country to an on-site meeting within the European continent. If inter-continental travel is required, the fee is EUR 2,000.

The travel expenses and other costs directly related to the Board work of the members of the Board of Directors are paid in accordance with the company's compensation policy in force at any given time. In addition, the Chairman of the Board of Directors is offered assistant and administrative services.

Paid remuneration in 2024

Member	Total annual fee, EUR	Share reward portion, EUR	Cash portion, EUR	Meeting fees, EUR ¹	Total, EUR
Risto Siilasmaa	80,000	32,000	48,000		80,000
Tuomas Syrjänen	48,000	19,200	28,800		48,000
Kirsi Sormunen	48,000	19,200	28,800		48,000
Ciaran Martin	38,000	15,199	22,801	4,000	42,000
Amanda Bedborough	38,000	15,199	22,801	2,000	40,000
Niilo Fredrikson	38,000	15,199	22,801		38,000
Harri Ruusinen ²	12,667	5,066	7,601		12,667
Keith Bannister ³				3,000	3,000
Päivi Rekonen ³				3,000	3,000
Total	302,667	121,063	181,640	12,000	314,667

¹ Meeting fees paid based on international travel

² Board of Directors' personnel representative

³ Member until 20.3.2024

Remuneration of the President and CEO

Juhani Hintikka served as WithSecure's CEO until 8 April 2024. Antti Koskela was first nominated to an interim CEO from 8 April and was nominated to WithSecure's President and CEO on 1 July 2024.

During Juhani Hintikka's CEO time, EUR 203,032 was paid as total remuneration for the CEO role. Payment consists of base salary, phone benefit and long-time incentive payments. Upon the termination of the employment on the date of October 8, 2024, aside of earned monthly base salary, fringe benefits and compensation for unused holiday days, Juhani Hintikka was paid also with: 1) cash compensation for termination amounting to EUR 175,002 (corresponding to six months' fixed base salary in accordance with the CEO's contract), 2) PMSP compensation EUR 156,980.04 based on board decision on "Approach to PMSP in the case of termination of employment" made in the year of 2023, 3) STI 2024 payout EUR 16,581, based on Q1 2024 actual performance compared to Q1 2024

budgeted performance estimation. All payments associated with Juhani Hintikka's 2024 compensation as well as employment termination were all paid out already in 2024.

During Antti Koskela's CEO time, EUR 231,207 was paid as total remuneration. Payment consists of base salary, phone benefit, STI 2023 payout and holiday bonus. Among these, STI 2023 payout and holiday bonus (holiday bonus amount EUR 8,364) were paid during Antti Koskela's CEO period but earned before he took the CEO role.

The remuneration of the President and CEO is decided by the Board of Directors. The main components of the President and CEO's total remuneration are base salary and short- and long-term incentives. Salaries and financial benefits paid in 2024 are described below:

	Payments done in 2023	Payments done in 2024, Juhani Hintikka (1 January 2024 – 8 April 2024) ³	Payments done in 2024, Antti Koskela (Interim 8 April – June 30 2024, President and CEO 1 July – 31 December 2024)
Base salary, Including phone benefits, EUR	350,244	94,510.85	208,229.99
Pension/Other financial benefits, EUR	-	- ¹	- ¹
Short-term incentives (STI), EUD	159,679 ²	-	14,613.06
Long-term incentive (LTI), EUR	-	108,520.96 ³	-
Holiday Bonus, EUR	-	-	8,364
Total	509,923	203,031.81	231,207.05

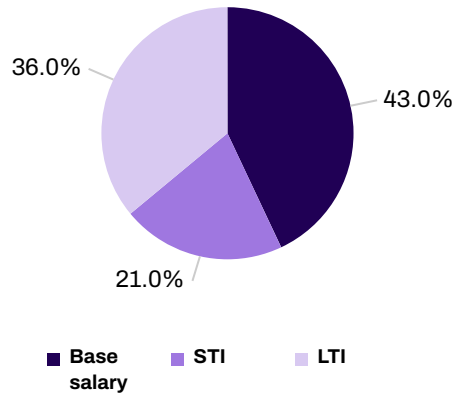
¹ As a resident in Finland, the President and CEO is covered by the statutory state pension arrangement in Finland (TyEL). No supplementary pension arrangements were offered.

² The amount paid to the President and CEO's pension fund. The amount equals to the actual STI reward amount (EUR 145,162.50) multiplied by 1,1, as decided by the BoD.

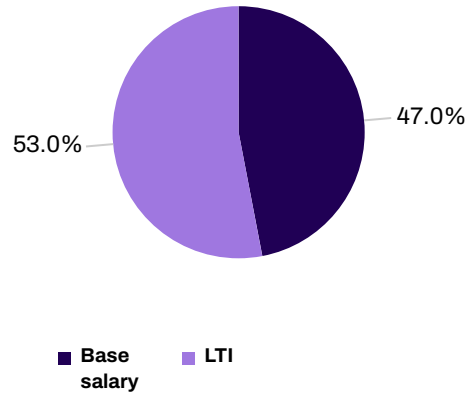
³ RSP plan 2021-2023 payment, including cash amount to cover taxes and share amount value.

President and CEO Pay mix 2024¹

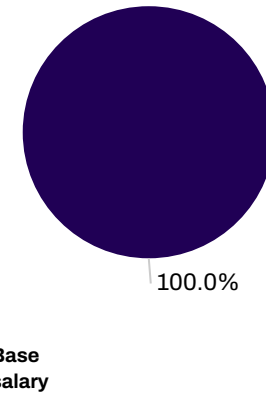
CEO - Target remuneration



Actual remuneration, Juhani Hintikka



Actual remuneration, Antti Koskela



¹ Data for graphs doesn't include Antti Koskela's STI 2023 payout which were paid during Antti Koskela's CEO period but earned before he took the CEO role.

Short-term incentive (STI)

The target STI reward for the President and CEO is 50% of annual base salary, maximum reward being two times the target.

STI Plan 2023 (payable in 2024)

The STI Plan 2023 for the President and CEO, Juhani Hintikka was based on WithSecure's revenue with 60% weight and adjusted EBITDA with 40% weight of total. The performance criteria for the STI Plan 2023 were not met and there was no payment based on the STI 2023.

STI Plan	Performance Criteria	Weight	Minimum	Target	Maximum	Outcome	Performance	Achievement
2023	WithSecure Adjusted EBITDA	60%	-13.0	-11.0	-9.0	-16.1	0.0%	0.0%
	WithSecure Revenue	40%	150.0	158.0	166.0	142.8	0.0%	

STI Plan 2024 (payable in 2025)

The STI Plan 2024 for the President and CEO was based on WithSecure's adjusted EBITDA with 60% weight and revenue with 40% weight of total. The overall achievement of the STI Plan 2024 for the President and CEO based on the performance criteria was 27,24%.

STI Plan	Performance Criteria	Weight	Minimum	Target	Maximum	Outcome	Performance	Achievement
2024	WithSecure Adjusted EBITDA	60%	2.1	4.1	6.1	3.0	45%	27.24%
	WithSecure Revenue	40%	148.5	156.5	164.5	147.4	0.0%	

Long-term incentive (LTI)

The LTI reward at the target level for the President & CEO is 85% of annual base salary, maximum reward being two times the target. The following Long-term incentive (LTI) payments were made to the President and CEO during 2024.

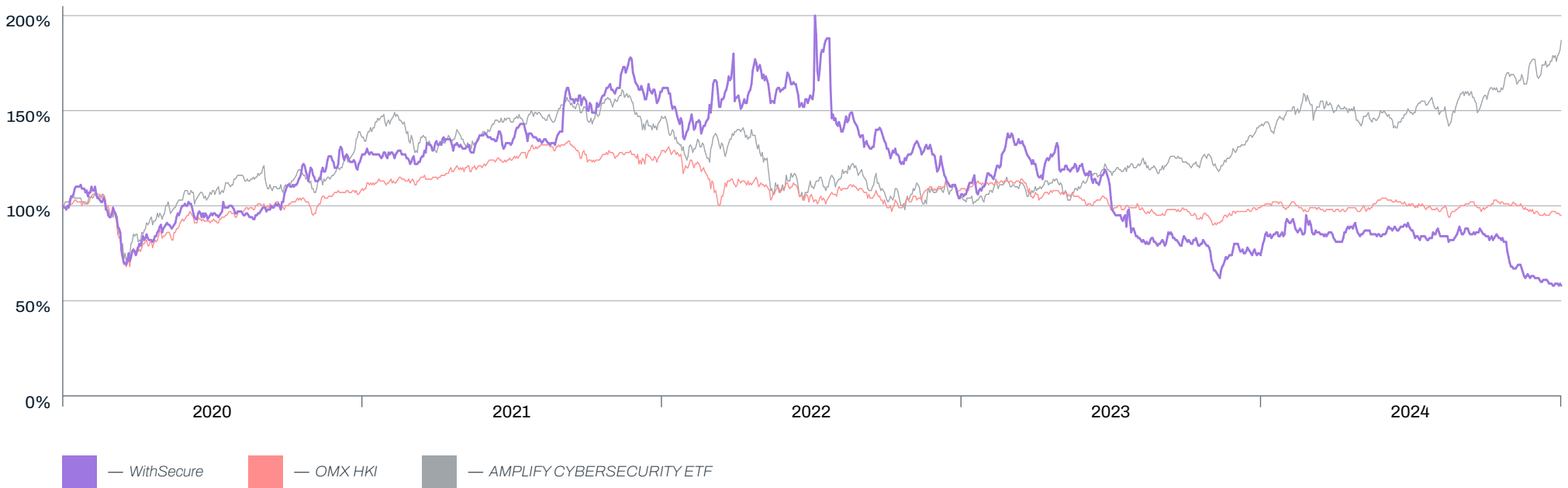
To Juhani Hintikka: In Restricted Share Plan 2021-2023's gross payout 106,833 shares were paid, gross reward value as EUR 108,520.96 with transfer price

EUR 1.0158. 50% of the reward were paid as net share amount 53,417 and 50% as cash amount EUR 54,259.97.

President and CEO Juhani Hintikka was eligible to participate the program Performance Share Plan 2021-2023 but the program didn't have any payout.

Share Plan	Performance Criteria	Minimum	Target	Maximum	Outcome	Performance	Individual Target reward	Maximum reward	Reward payment
Performance Share Plan 2021-2023	Absolute TSR	EUR 1.73	EUR 2.01	EUR 2.30	1.10	-23.9%	202,983 shares	405,966 shares	No reward payment made

Share price development of WithSecure and indices



The President and CEO (Antti Koskela) participates currently in two share based long-term incentive plans.

Performance Share Plan (PSP) 2024-2026

The President and CEO was granted 120,000 shares within the PSP 2024–2026 in 2024. This grant represents the target level reward, the maximum reward being two times the target. The PSP 2024-2026 is based on WithSecure's Revenue Growth during the performance period. After the three-year performance period, the reward is paid in the first half year of 2027.

Performance Matching Share Plan (PMSP) 2022-2026

The President and CEO participates in the PMSP 2022-2026 that was launched in 2022, starting on 1 September 2022 and ending on 30 November 2026. This

4-year performance-based plan offers an opportunity to invest in WithSecure and earn shares through a matching reward. The performance criterion of the PMSP 2022-2026 is WithSecure market capitalization development result at the end of the program time. The outcome is calculated in October-November 2026 and rewards are paid by the end of December 2026. The vesting period of the plan is from starting time of the program to the payment time. The PMSP 2022–2026 replaced two typical annual performance share plan allocations for the participants and there were no grants done within the PSP 2022-2024 or PSP 2023-2025 for the President and CEO.

The President and CEO (Antti Koskela) - Current LTI Plans

Share Plan	Performance Criteria	Target reward	Maximum reward	Reward payment
Performance Share Plan 2024–2026	Revenue Growth	120,000 shares	240,000 shares	Q1 / 2027
Performance Matching Share Plan 2022–2026	WithSecure market capitalization	3 x matching of initial investment of 61,267 shares	5.5 x matching of initial investment of 61,267 shares	Q4 / 2026

Key terms of service of the President and CEO

The contract of the President and CEO is an indefinite contract with a six-month period of notice both ways. If the company terminates the contract of employment, the President and CEO is entitled to a severance payment equivalent of six months' base salary.

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

Information for shareholders

Financial Calendar

During the year 2025, WithSecure Corporation will publish financial information as follows:

- 25 April 2025: Interim Report for January–March 2025
- 16 July 2025: Half-Year Financial Report for January–June 2025
- 22 October 2025: Interim Report for January–September 2025

Contact information



Tom Jansson
CFO
WithSecure Corporation



Laura Viita
Vice President, Controlling, investor relations and sustainability
WithSecure Corporation
+358 50 487 1044
investor-relations@withsecure.com

WithSecure observes at least a three-week (21 days) silent period prior to publication of financial reports, during which it refrains from engaging in discussions with capital market representatives or the media regarding WithSecure's financial position or the factors affecting it.

The Annual General Meeting is scheduled for Tuesday, 18 March 2025. The Board of Directors will convene the meeting.



WithSecure Corporation

Välimerenkatu 1
00180 Helsinki
Finland

Tel. +358 9 2520 0700

Investor-relations@withsecure.com

<https://www.withsecure.com/fi/about-us/investor-relations>

<https://www.withsecure.com/en/about-us/investor-relations>