



# Trapets Vendor Audit Report 2024

## Contents

1.	Introduction .....	4
	Purpose and Scope .....	4
	Trapets in brief .....	5
2.	Organisation and employees.....	6
	Core Values .....	6
	Organisation.....	6
	Recruitment and onboarding .....	7
	Organisational resilience .....	8
	Code of conduct .....	8
3.	Information security .....	9
	Information security management overview .....	9
	Information security goals and objectives.....	9
	Information security management process.....	9
	Services/systems .....	10
	Security awareness training .....	11
	Secure data handling .....	12
	Data backup.....	12
	Access management.....	13
	Datacentres .....	13
4.	Processing of personal data .....	14
5.	Availability .....	15
6.	Support .....	15
7.	Cyber security incident & personal data breach.....	15
	Cyber security incident .....	15
	Personal data breach .....	15
8.	Risk management framework .....	16
9.	Incident and problem management .....	18
10.	Business Continuity Planning (BCP) .....	19
11.	Third parties / sub-contractors.....	20
12.	Quality management.....	21
13.	Financial results.....	21

14.	Sustainability .....	22
15.	Major adverse events.....	23
16.	Looking ahead into 2025.....	23

# 1. Introduction

---

## Purpose and Scope

Trapets provides services to customers in the EU financial industry that are or may be subject to regulatory requirements, including:

- Regulation (EU) 2022/2554 on Digital Operational Resilience for the financial sector ("DORA"), applicable as of 17 January 2025. Trapets' services may be deemed by our customers to support critical or important functions.
- EBA/GL/2019/02, Guidelines on outsourcing arrangements issued by the European Banking Authority (EBA)
- Guidelines on the use of cloud service providers issued by the European Securities and Market Authority (ESMA) (ESMA50-164-4285) or the European Insurance and Occupational Pension Authority (EIOPA) (EIOPA-BoS-20-002)
- General Data Protection Regulation (EU) 2016/679 ("GDPR")

The relevant regulatory frameworks include obligations for the customer to ensure its ability and right to audit its service providers. Where requested, Trapets' customer agreements include a right of access and audit rights for the customer in accordance with the relevant requirements.

Also outside the direct scope of regulatory requirements, Trapets' customers may need to conduct periodic reviews or audits of Trapets' service delivery with respect to information security and operational resilience. Similar information may be required in pre-sales due diligence of Trapets as a potential service provider.

To facilitate a cost-effective due diligence, review or audit process, Trapets has summarised key information in this report. The report is updated by Trapets on an annual basis.

This report covers the period 2024.

Trapets company details	
Company name	Trapets AB
Corp. reg. no.	556586-4773
LEI Code	894500MU214PEPODCB40
Company address	Kungsgatan 56, SE-111 22, Stockholm, Sweden
E-mail	info@trapets.com
CEO	Gabriella Bussien, gabriella.bussien@trapets.com
CISO	Daniel Cederhierta, daniel.cederhierta@trapets.com
DPO	Ulrika Ersman, ulrika.ersman@trapets.com dpo@trapets.com
Website	www.trapets.com

## Trapets in brief

Trapets is a company specialising in (SaaS) solutions for financial crime prevention. Trapets provides complete solutions, including software products, hosting, support, expert consulting, managed services and training. Trapets has developed and owns all rights to the Instantwatch platform, with the following solutions:

- **Screening** - for screening of customers and prospects against different screening lists.
- **Transaction Monitoring** - for detecting and preventing money laundering and terrorism financing.
- **Customer Due Diligence** - for customer onboarding and ongoing due diligence.
- **Fraud Protection** – for preventing and detecting fraudulent payment transactions<sup>1</sup>
- **Market and Trade Surveillance** – for detecting market abuse and insider trading.

Trapets also offers Know Your Customer and screening services in certain non-financial segments in Sweden via the service Trapets KYC (formerly Regtech KYC).

Trapets' vision is a future free from financial crime and our mission is to help businesses with the technology and knowledge needed to fight financial crime.

Founded in Sweden in 2000, Trapets has grown to become a Nordic market leader within Transaction Monitoring, Screening and Market and Trade Surveillance via the modular-based compliance platform – Instantwatch. Today, Trapets has over 70 employees operating from 3 locations: Stockholm, London, and Hanoi (as a clarification, service delivery is performed from Sweden only).

The Instantwatch platform monitors, among other things, transaction flows to detect various patterns or behaviours. It is a secure and easy-to-use platform for surveillance purposes with a focus on efficiency and usability.

The Instantwatch platform has proven to be extremely reliable with world-class performance. Trapets also provides managed services, primarily within securities trading surveillance and anti-money laundering transaction monitoring.

Trapets' main AML customers are financial service providers such as banks, asset managers, credit companies, payment solution providers and insurance companies. We also have stock exchanges, marketplaces, financial regulators, and securities firms that are operating under the MAR regulation. The company's core market is the Nordic region, but in recent years with an increased focus on markets outside the Nordic region, with an emphasis on the UK.

---

<sup>1</sup> Fraud Protection planned to be launched in 2025

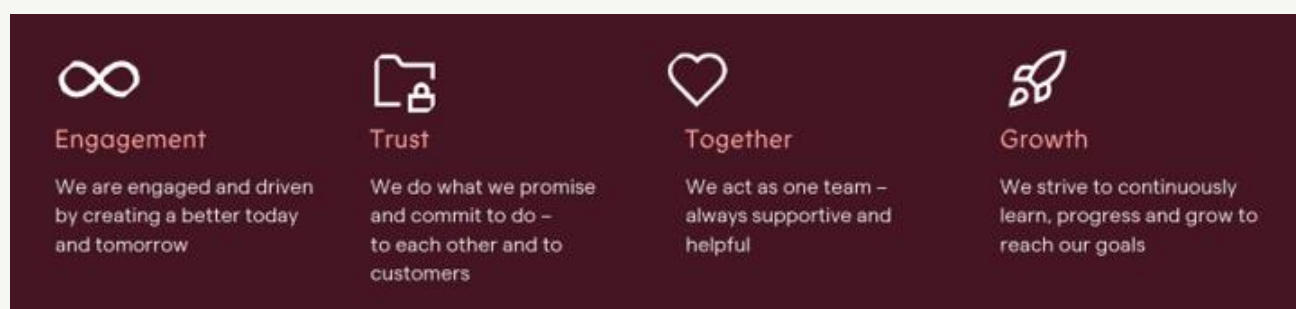
Information security is core at Trapets. Trapets started early with a continuous improvement effort within our information security management system (ISMS), with internal training, internal and external security audits, and other security measures. The company has been ISO27001 certified since 2018 and successfully completed a re-certification during 2024.

Trapets is a healthy company with high solidity, liquidity, and the highest credit rating. No product development or goodwill is balanced. The company is majority owned by Monterro, a Nordic private equity firm, together with minority ownership by the founders and employees of the company.

## 2. Organisation and employees

### Core Values

The guiding principles in our daily operations are our core values – Engagement, Trust, Together and Growth.

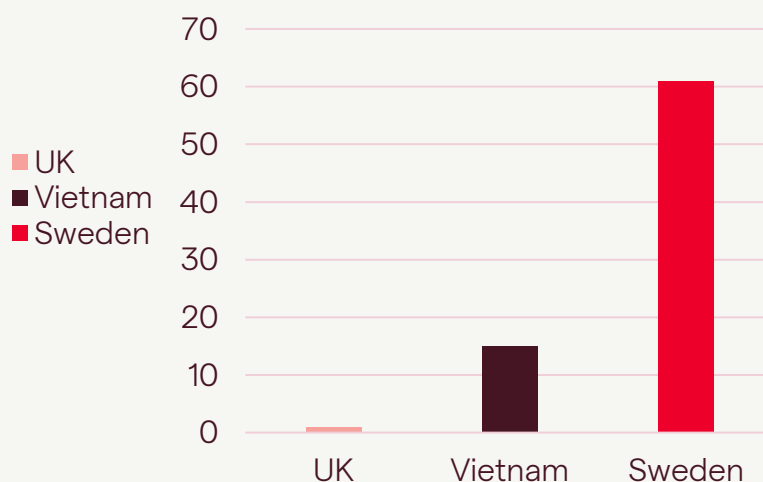


### Organisation

As Trapets grows, Trapets continuously develops and enhances our organizational structure. At the end of 2024, the total number of employees was 77. The FTE gender distribution is 64 % male and 36 % female. At the end of 2024, the gender distribution within the management team is 43% male and 57% female.



## NUMBER OF EMPLOYEES PER COUNTRY END OF 2024



## Recruitment and onboarding

As a growing company, Trapets emphasizes our recruitment process to ensure we hire employees with the right skills and personality who meet our needs and fit into our company.

Within the recruitment process, each candidate is subject to interviews with key persons at Trapets, and the final candidate performs relevant tests. Before a final decision, references are taken. To the extent permitted under local legislation, Trapets requires each new employee to provide an extract from criminal records. During the end of 2024, Trapets has as an alternative initiated the use of a third-party provider for background checks for recruitments in Sweden. All employment agreements include a confidentiality agreement, with a continued obligation of confidentiality after employment termination.

As part of onboarding, all new employees are requested to confirm in writing to have read, understood, and commit to complying with the Code of Conduct and information security policies.

AUDIT				
ISO 27001	Date	Result	Owner	Auditor
Organisation, roles, all HR processes, responsibilities, competences, awareness, updated policies for employees etc	Q4 2024	Passed	CISO	Internal audit, Q-branch
Organisation, roles, all HR-processes, responsibilities, competences, awareness, updated policies for employees etc	Q2 2024	Passed	CISO	External audit, SBcert

## Organisational resilience

At Trapets, we want to create a work culture that is both collaborative and dynamic. Tying into two of our core values, growth and together, we believe in a workplace where everyone helps each other, sharing knowledge and learning through curiosity. United in our passion for Trapets' purpose and mission, we trust in each other's accountability and are engaged to walk the extra mile, earning us the trust of our customers.

Trapets works continuously to enhance organizational clarity, roles and responsibilities, the employee lifecycle, training and development, and employee satisfaction. Defined role descriptions guide recruitment processes, ensuring the right profiles and skillsets are identified based on organizational needs. This role clarification is crucial for strengthening operational resilience and aligning the organization to meet both current and future customer demands.

Our risk management framework includes risk related to human resources, such as potential dependencies on key individuals, and our business continuity plan as well as the crisis management plan provide support for managing uninterrupted business operations in case of loss of key personnel.

## Code of conduct

Trapets' Code of Conduct gives internal guidance on business principles and policies in our daily operations. It covers Anti-Corruption, Confidentiality, Conflicts of Interest, Corporate Assets, Diversity, External Communication, Fair Competition, Human Rights and Labour Relations, Information Security, Protection of personal data, Quality, Social Media, Sustainability and Work Environment.

The current version of the Trapets Code of Conduct was approved by Trapets Management on 14 November 2024. All new employees are requested to confirm in writing to have read, understood, and commit to complying with the Code of Conduct and information security policies. The same is done on an annual basis for all employees.

Confirmation of Code of Conduct			
	Date	Result	Owner
Confirmation by all employees	Q1 2024	100 %	Chief Legal Officer



## 3. Information security

---

### Information security management overview

Trapets information security management is structured and risk-oriented, according to the principles of the international standard ISO/IEC 27001. Trapets have been certified according to ISO27001 since 2018, with yearly audits and with the next re-certification audit due in 2027.

### Information security goals and objectives

Trapets current tactical information security goals and objectives are:

- Remediate all identified critical security vulnerabilities.
- Penetration testing performed, documented, and stored, annually or in conjunction with major changes.
- 100% attendance by Trapets engineers at the OWASP Top 10 training session.
- Ensure server availability for Trapets products, in accordance with SLA.
- Ensure that all recommendations outlined in Trapets' SOC report are implemented and adhered to.

### Information security management process

Trapets performs recurring risk assessments as part of our risk control procedures. The risk analysis, conducted annually, aims to identify the critical information assets requiring protection and to provide a documented rationale for what to protect. The risk analysis also relates the identified information assets to the identified threats the business may be exposed to and to identified potential vulnerabilities. Finally, the quantitative risk analysis is aimed at developing a basis for decision-making for the introduction of controls with the purpose of:

- Preventing unauthorised access to information (*Confidentiality*)
- Ensuring that the information produced and processed is accurate, current, and complete (*Integrity*)
- Maintaining the accessibility of information as it is needed (*Availability*)

For each security discipline, organisational, administrative, and technical controls are implemented and documented to ensure a satisfactory level of information security protection is achieved.

Trapets' management is ultimately responsible for information security and for information security management on a strategic level. This responsibility includes ensuring the availability of adequate financial resources and personnel with the right skills.

The responsibility for operating the information security management system, which includes the identification of critical information assets, conducting of risk analysis, selecting, and implementing controls and measures aimed at improving Trapets' information security posture, initiating security

audits and regular evaluation of information security management is delegated to the Trapets Chief Information Security Officer (CISO).

All employees who handle confidential or sensitive information in performing their tasks are responsible for protecting that information and for complying with applicable information security policies and instructions. Customer information is always classified as confidential, with access restricted to a very limited set of employees.

The information security management processes are reviewed and evaluated annually. Discrepancies, inadequacies, and the occurrence of incidents are systematically documented to secure lessons learned that can be considered in work for continuous improvement. The result of the information security-related activities and the estimated risk levels are subject to management review twice a year.

AUDIT				
ISO 27001	Date	Result	Owner	Auditor
Surveillance audit	Q2 2024	Passed	CISO	External audit, SBCert

## Services/systems

The systems in scope of Trapets information security measures are the Instantwatch services.

- Transaction Monitoring
- Customer Due Diligence
- Screening
- Fraud Protection
- Market and Trade Surveillance

In addition, **Trapets KYC** is in scope of Trapets information security measures.

The systems are managed within Trapets ISMS without any exclusion of information security policies, security mechanisms, operational processes, or measures to ensure operational resilience. The measures in place provide security by design in the development process, security in the procurement process, security in daily operations, and regular testing to guarantee that the changing landscape is always considered when evaluating our systems from a security and resilience perspective. In addition to the ISO 27001 audit, the Instantwatch products delivered as a service are regularly subject to penetration tests, annual Disaster Recovery (DR) tests, and continuous reviews to strengthen operational resilience.

AUDTIS				
System	Area	Date	Owner	Firm
Transaction Monitoring	Penetration test	Q2 2023	CISO	Certezza
Transaction Monitoring	DR test	Q2 2024	Head of IT Operations	Trapets
Customer Due Diligence	Penetration test	Q2 2023	CISO	Certezza
Customer Due Diligence	DR test	Q2 2024	Head of IT Operations	Trapets
Screening	Penetration test	Q4 2022	CISO	Certezza
Screening	DR test	Q3 2024	Head of IT Operations	Trapets
Market and Trade Surveillance	Penetration test	Q1 2023'4	CISO	Sentor
Market and Trade Surveillance	DR test	Q2 2024	Head of IT Operations	Trapets
Trapets KYC	Penetration test	Q3 2023	CISO	Certezza

## Security awareness training

Security awareness training on cyber threats, how to recognize them, and steps to keep themselves and the Trapets company safe is approached as a long-term strategy and part of Trapets ISMS.

Given the significant role of human error in cyber-attacks today, adequately trained employees are key to effective security. At Trapets, a solid security awareness training program drives information security awareness and provides employees and contractors with the knowledge and confidence to recognize security threats and how to appropriately respond and report a threat or incident. Security awareness training is done on an ongoing basis to build a security-aware culture.

Trapets' security awareness program is a key element in reducing risks related to data breaches or other consequences caused by cybersecurity threats. With Trapets' security awareness program, employees will be mindful of information security best practices as they pertain to regularly used applications and technologies, including social media, email, and websites.

Trapets' security awareness program is carried out as an annual security training session, as well as micro training sessions, pushed out regularly, with the support of AI to customize training based on roles and responsibilities.

In addition, a tool is used to conduct simulated phishing attacks, where deceptive emails are sent to Trapets employees. The simulation tool supports raised awareness of attacks and how employees respond when a phishing email is received, prompting further training for certain individuals if necessary.

AUDIT					
Description	Attendance	Date	Result	Owner	Auditor
Annual security awareness training	Employees & consultants	Q2 2024	100% attendance	CISO	External, SBCert
Security awareness & attack simulation	Employees & consultants	Q4 2024	100% participation	CISO	Internal, Qbase

## Secure data handling

All data processed in Trapets systems are classified according to Trapets' data classification policy. The data classification activates a given set of security measures to be implemented to secure the data in scope. Trapets constantly strive to beat industry benchmarks when designing and implementing information security measures. Various sets of standards are used as inspiration as well as external cyber firms and communities when deciding on measures to implement, software to use, or consultants to hire.

Only authorized users are allowed to access sensitive data, including networks and servers, and other devices used to directly provide the Instantwatch services. The principle of least privilege is adopted across the organization. Access to classified environments is made possible, for an authorized user, via jump hosts and temporary account elevation. MFA with application auth is always enforced. The resources used in the IT platforms are protected with antimalware and ransomware protection, data encryption is applied for data in transit and for data in rest, using best-practice encryption algorithms.

EDR is used to identify suspicious behaviour and advanced persistent threats on endpoints in the Trapets environment and alert administrators accordingly. It does this by collecting and aggregating data from endpoints and other sources.

Monthly security reports are conducted to secure the SOC findings, and that actions are taken to mitigate any identified threats.

AUDIT				
Activity	Date	Result	Owner	Auditor
Review of security measures	Q2 2024	Passed	CISO	Internal, Qbase

## Data backup

Trapets has implemented a comprehensive backup policy that covers all critical data in our organization. Our backup policy includes a combination of backup types, offsite storage, encryption, retention policies, disaster recovery plans, operational resilience testing, access control, monitoring, and staff training.

Trapets customers' data is protected against possible risks such as hardware failure, software issues, natural disasters, cyber-attacks, and human error. Our data backup policy helps to minimize

the risk of data loss and ensures that we can quickly and easily restore data in the event of a critical event.

AUDIT					
Product	Activity	Date	Result	Owner	Auditor
Transaction Monitoring (AML)	Restore from database	Q2 2024	Passed	Product Owner	Internal, Qbase
Customer Due Diligence	Restore from database	Q2 2024	Passed	Product Owner	Internal, Qbase
Screening (KYC)	Restore from database	Q3 2024	Passed	Product Owner	Internal, Qbase
IMarket Trade Surveillance	Restore from database	Q2 2024	Passed	Product Owner	Internal, Qbase

## Access management

Trapets' access management policy is established, documented, and reviewed based on business and information security requirements and includes access control rules, access rights and restrictions for specific user roles.

All access to classified information assets is, by default, restricted, and granted access rights are added based on roles and responsibilities. Access is only permitted on a need-to-know basis and is only permitted upon approval. Access controls are both logical and physical. The scope of Trapets access management is limited to information processed within Trapets IT platforms or within Trapets facilities.

Segregation of duty and the principle of least privilege are adopted throughout the access management process. Access policies based on roles and security groups are used to secure correct and minimum access rights. A formal process is implemented to secure user access rights in relation to onboarding, change of roles and termination. All access rights are subject to monthly review and audit.

AUDIT				
Activity	Date	Result	Owner	Auditor
Access	Q4 2023	Passed	CISO	Internal, Qbase

## Datacentres

Trapets only use datacentres that are compliant with Trapets' security requirements. The datacentres are geographically separated, subject to rigorous controls and recurring audits performed by Trapets staff in collaboration with Trapets' hosting partner (Iver Sverige AB). All data centres are located within the EU and ISO27001 certified and SOC II compliant. More detailed information can be provided upon request.

## 4. Processing of personal data

---

Trapets recognizes the importance of respecting the privacy rights of individuals. In addition to the GDPR, some of the personal data we process for our customers are also covered by legislation on bank secrecy, or similar legislation. We are committed to govern privacy accordingly. Trapets' Data Protection Policy (Processor) describes the organizational and technical safeguards Trapets has implemented to protect Personal Data processed by Trapets within our service delivery, as processor for our customers (the controllers). Trapets is committed to integrate privacy in our products and services to enable our customers to be compliant in using our offerings.

Trapets' privacy management is governed by the CEO, supported by the DPO function consisting of the Data Protection Officer and CISO.

Trapets customers (or their end customers) are controllers of their personal data and utilize Trapets' services primarily for compliance with legal obligations they are subject to, primarily within the areas of anti-money laundering and terrorism financing and/or market abuse. In relation to our customers, Trapets is by default a processor of personal data. In this capacity, Trapets will only process personal data for the purpose of delivering our services and fulfilling our obligations under the relevant agreement, including data processing agreement, with each customer.

Prior to engaging Trapets as processor, each controller shall ensure that the processing by Trapets, including technical and organizational measures, fulfils that controller's requirements and comply with legal or other requirements on the controller. Each Customer is responsible to ensure it complies all applicable laws and regulations, including relevant data protection legislation, in its use of Trapets services.

The agreement between Trapets and its customers includes a data processing agreement that covers the subject-matter and the duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects and the obligations and rights of the customer and Trapets.

Unless otherwise agreed in writing Trapets will only store and process customer personal data within the EU/EEA area.





The current Data Protection Policy (Processor) was approved by the Trapets management team on 14 November 2024.

Privacy Awareness Training is held annually for all employees, the latest one was held in June 2024.

AUDIT				
ISO27001	Date	Result	Owner	Auditor
Part of ISO27001 recertification	Q2 2024	Passed	DPO	External, SB Cert
Compliance	Q4 2024	Passed	DPO	Internal, Qbase

## 5. Availability

Instantwatch server uptime (in aggregate annual average 2024).

			
Transaction Monitoring (TM)	Customer Due Diligence (CDD)	Screening (SCR)	Market & Trade Surveillance (MTS)
Achieved (%)	Achieved (%)	Achieved (%)	Achieved (%)
SLA (%)	SLA (%)	SLA (%)	SLA (%)
99.87	99.87	99.89	99.95
99.7	99.7	99.7	99.5

## 6. Support

Service requests (on annual basis 2024)

Reported requests	Solved requests	First reply median (mins.)
3818	3798	42

## 7. Cyber security incident & personal data breach

### Cyber security incident

Service	Date	Impact	ID
None identified	-	-	-

### Personal data breach

Service	Date	Impact	ID
None identified	-	-	-

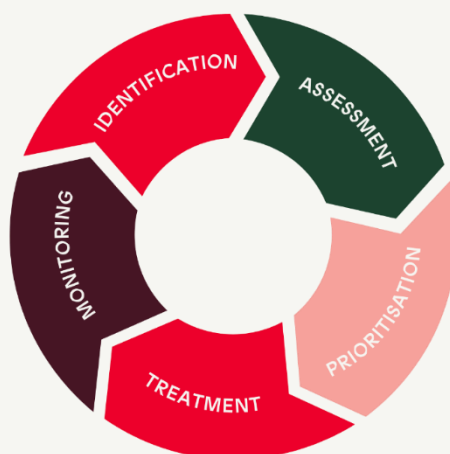
## 8. Risk management framework

---

The purpose and goal of Trapets' risk management framework is to provide a systematic and structured approach to identifying and managing risks that could affect Trapets' ability to achieve our objectives of high-quality, competitive and trusted products and service delivery to our current and future customers.

The risk management framework provides a set of guidelines and processes to manage risks across all areas of our business. Key elements of Trapets' risk management:

1. **Identification** - Risks are identified and reported within day-to-day operations, regular risk workshops or within risk assessments in connection with a major internal change or within supplier evaluation.
2. **Categorisation** – Risks are categorized within the different categories: External, Business, Product, Information Security, and Project risks. Each risk is assigned a Risk Owner responsible for management and follow-up.
3. **Assessment & Prioritisation** – Risks are evaluated based on Likelihood and Impact using a predefined matrix. High-priority risks are addressed immediately.
4. **Treatment Plans** – For critical risks, we develop and implement mitigation plans with clear actions and deadlines to reduce or eliminate risks.
5. **Monitoring & Review** – We regularly review all risks and mitigation activities. Critical risks are monitored regularly by our management team to ensure they remain under control.



Trapets promotes a risk-aware culture where all employees and sub-contractors are encouraged to report potential risks, and regular risk workshops and management reviews help us stay proactive. All employees must have a good understanding of their own area and the risk associated with it. Risk awareness and management shall be an integrated part of operational responsibility. All managers must work for a high level of risk awareness and a healthy risk culture.

Within our alignment with DORA requirements, we are further enhancing our framework, including by strengthening risk assessments for third-party suppliers.



## Threat intelligence

Trapets leverages a Security Operations Centre (SOC) as a service through its hosting partner, Iver Sverige AB. The SOC integrates Endpoint Detection & Response (EDR) tools (SentinelOne) and a team of security specialists to protect Trapets' IT environments.

## Managed Detection & Response (MDR)

- AI & Machine Learning: Detects malicious files, vulnerabilities, and credential attacks using AI-driven tools.
- Automatic Threat Management: Handles threats with isolation, termination, quarantine, and rollback capabilities.
- Custom Rules & Grouping: Allows black/whitelisting and dynamic device grouping.
- Security Operations Centre (SOC):
  - Provides 24/7 threat detection, incident management, and reporting.
  - SOC specialists monitor and respond to threats, escalate issues, and produce monthly reports.
- Incident management includes classification and resolution based on severity, with an enhanced response team available when needed.

## Additional Measures

- Code Scanning (Mend): Weekly scans of source code in Azure DevOps for vulnerabilities and legacy code, with findings reported to the Trapets security team.
- End-User Support: 24/7/365 security advice and incident response.
- Monthly Oversight: Security reports and meetings to assess risks and actions.

Trapets' Threat Intelligence is managed by the CISO-led security team, focusing on threat analysis, awareness, and risk management through regular collaboration and task monitoring.

AUDIT				
ISO 27001	Date	Result	Owner	Auditor
Risk process	Q1 2023	Passed	CISO	Internal audit, Qbranch
Risk process	Q2 2024	Passed	CISO	External audit, SBCert

## 9. Incident and problem management

---

Trapets has an incident and problem management process to ensure that all identified incidents are reported, prioritized, communicated, managed and learned from in a structured manner. This process includes defined responsibilities, with an appointed incident manager for incidents that are prioritized as critical or high according to a defined prioritization matrix.

The incident routine includes determining whether an incident constitutes a personal data breach that must be managed in accordance with applicable legal and contractual requirements and/or whether it qualifies as an information security incident. In case of an emergency related to an information security incident, an external Incident Response Team is available.

Communication to customers regarding incidents will follow the incident response times. If a major incident occurs, Trapets will inform customers directly and provide information to support intermediate and final reporting in accordance with DORA regulations.

Upon the closure of an incident, a decision is made in each case whether to also register a problem for further root cause analysis and learning in accordance with the problem management routine. Trapets conducts root cause analysis to facilitate learning, improvement and quality assurance. Lessons learned and corrective actions are regularly followed up in problem learning meetings.

AUDIT				
ISO 27001	Date	Result	Owner	Auditor
<b>Incident Management</b>	Q4 2024	Passed	CISO	Internal audit, Qbranch
<b>Incident Management</b>	Q2 2024	Passed	CISO	External audit, SBCert

## 10. Business Continuity Planning (BCP)

---

Trapets' Business Continuity Planning (BCP) framework incorporates guidance and methodology from the FSPOS (Finansiella sektorns Privat Offentliga Samverkan).<sup>2</sup> Trapets has applied the method outlined in FSPOS for creating a BIA (Business Impact Analysis), aiding in the formulation of strategy and the Business Contingency Plan.

Considering what is deemed most critical for Trapets and our customers, the focus is on addressing the need for operational resilience and high service availability to support our customers in fulfilling their legal obligations and business needs. Trapets is committed to achieving and maintaining high availability and rapid restore procedures for each Instantwatch product. Consequently, Trapets has developed contingency plans for each Instantwatch product and for our infrastructure.

The scope of Trapets' BCP framework is IT system and services, organization, Trapets HQ office, and external suppliers with direct impact on service delivery. Our objective is to attain high availability and rapid restore procedures for each product, ensuring resilience and minimizing downtime. Information security is a fundamental aspect of Trapets business contingency planning.

Trapets adopts a proactive approach to risk assessment and mitigation activities to prevent incidents and to aim for quality assurance. In the event of an incident, our focus is on swift resolution to prevent significant disruptions.

Testing of disaster recovery instructions mainly consists of restoration from backups as internal activities and supplier review to secure that the core IT is covered by BCP and DR testing. In general, cloud services are designed to provide high availability while on-premises solutions rely more on manual testing. Trapets utilizes a combination of cloud services and on-premise.

Trapets never compromise with information security during an adverse event. Trapets setup is designed so that it cannot be restored with reduced security. Security is maintained on servers that install software, replicate the entire server with the same permission rules, etc. All recovery plans ensure the same security levels as during normal operation.

Trapets follows a continuity management process, reviewing, testing, and updating both the process and contingency plans on an annual basis.

---

<sup>2</sup> FSPOS (Finansiella Sektorns Privat-Offentliga Samverkan: FSPOS Vägledning för Kontinuitetshantering, Version 5.0, 2021-03-16



AUDIT				
ISO 27001	Date	Result	Owner	Auditor
<b>BCP Surveillance audit</b> <b>Routines, plans, infrastructure</b> <b>etc.</b>	Q1 and Q2 2023	Passed	COO	Internal audit, Qbranch
<b>BCP Surveillance audit</b> <b>Routines, plans, infrastructure</b> <b>etc.</b>	Q2 2024	Passed	CISO	External audit, SBCert

## 11. Third parties / sub-contractors

Trapets uses certain third parties to deliver our services, primarily within IT infrastructure and certain third-party data providers for external screening and/or market data.

Trapets selects and evaluates third party suppliers and sub-contractors as stipulated in the Trapets Supplier Management Policy. Evaluation includes supplier categorization, risk assessment, information security & privacy evaluation based on categorization, and legal review of contractual terms. This includes ensuring that necessary data processing agreements and/or contractual provisions required under DORA or other relevant regulatory requirements are included in the agreement between Trapets and the third party.

All Critical suppliers are subject to annual audits.

Upon request, Trapets will separately make available sub-contractor information that our customers may need under in particular DORA requirements.

## 12. Quality management

---

Trapets is committed to continuous improvement of quality, objective target setting and measurement of processes and operational quality. Trapets Quality Policy was adopted in 2023 and serves as the foundation for our quality management. We use data and key performance indicators to drive informed decisions and continually monitor our performance. This includes measuring, on a monthly basis, a number of KPI's, as well as regular Net Promoter Score (NPS) surveys among our customers. The current Quality Policy was approved by the Trapets management team on 14 November 2024.

## 13. Financial results

---

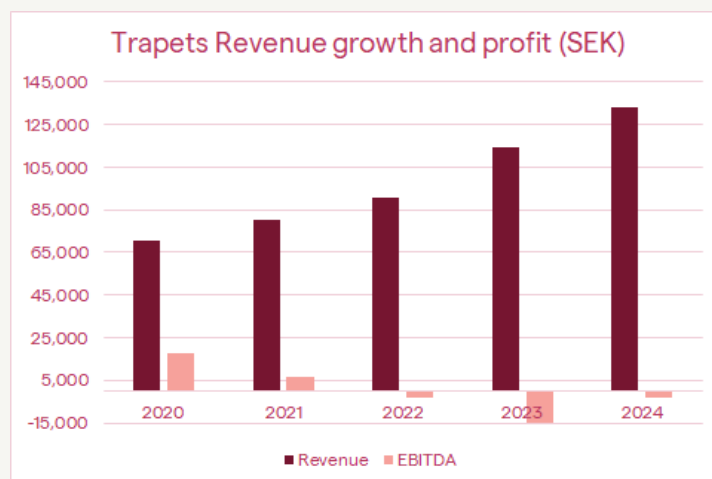
In 2024, Trapets achieved continued growth, with revenue increasing by 17% to SEK 133 million<sup>3</sup>, up from SEK 114 million in 2023. This growth was driven by a solid rise in recurring revenue, which saw a 19% increase, reaching SEK 127 million compared to SEK 107 million in the previous year.

Despite the positive revenue development, the company's EBITDA remains negative, with a loss of SEK -3.0 million, which is in line with Trapets' long-term plan. Trapets' strategic investments in expanding its international presence, particularly in the UK market, continue to play a significant role in revenue growth. Additional investments were made to introduce new technologies that drive scalability. These initiatives remain key to Trapets' long-term objectives of broadening market coverage and solidifying its customer base.

Overall, 2024 represents a year of substantial progress for Trapets, both in terms of revenue growth and operational improvements, positioning the company for sustainable growth in the years ahead.

---

<sup>3</sup> As of the date of this report, the 2024 numbers are preliminary and not audited.



## 14. Sustainability

Trapets is committed to conducting its business in a sustainable and environmentally responsible manner. We recognize the importance of environmental protection, social responsibility and ethical business practices.

Given Trapets' business operations, our environmental footprint is limited and consists mainly of energy consumption at our offices and key suppliers, primarily data centres, and the procurement, use and disposal of laptops and other hardware or electronic equipment. Business travel is limited as both internal and external collaboration is carried out primarily on a remote basis, using digital tools. Travel between Sweden and Trapets' operation in Hanoi, Vietnam is done only as reasonably required for adequate business reasons in each case. Our central Stockholm HQ office location with easy access to public transportation combined with a hybrid work model means employee commuting by car is very limited.

The current Sustainability Policy was approved by the Trapets management team on 14 November 2024. The policy outlines our commitment within the areas environmental protection, social responsibility and ethical business practices, and our approach to achieving our sustainability goals. More detailed sustainability objectives will be set annually, to be evaluated and reported on an annual basis. New or updated objectives for the next year shall be defined in a spirit of continuous improvement.

Sustainability objectives for 2024 has included (examples)

- 100 % renewable energy at Trapets HQ and partner datacentres (as documented by Iver) (excl. Hanoi).
- Increase sustainability considerations in Trapets' procurement of products and services
- ISO 27001 upgrade and recertification
- Community engagement

## 15. Major adverse events

---

During 2024, Trapets, our operations or our service delivery have not suffered any material adverse events negatively affecting Trapets' ability to deliver our services. We do not currently foresee any such events for 2025.

## 16. Looking ahead into 2025

---

During 2025, Trapets will continue the implementation of identified measures related to compliance with DORA requirements. Trapets also continuously monitors relevant regulatory frameworks, primarily within the EU financial industry, governing Trapets' service delivery or our customers' use of our services, as well as requirements and expectations communicated by our customers. Trapets is continuously and proactively working to evaluate and manage potential implications with an aim to ensure compliance with relevant customer and regulatory requirements. Where actions are needed, Trapets will take an incremental approach with a necessary prioritization of resources.

Trapets is committed to maintain the trust of our customers and other stakeholders.

Trapets does not currently foresee any material changes to how we operate and deliver our services during 2025.



Trapets is a software company that provides products and solutions for financial crime prevention, including anti-money laundering (AML), know your customer (KYC), and market surveillance.

Founded in 2000, Trapets has helped organisations meet regulatory needs for business success and fight financial crime for decades. We are trusted by over 500 companies ranging from small financial institutions to regulatory entities and have earned recognition as one of the top 100 RegTech companies globally.

Trapets has over 80 employees based in Stockholm, Hanoi, and London.

For more information, visit [www.trapets.com](http://www.trapets.com).