TRAPETS

Trapets Vendor Audit Report 2023

TRAPETS

Contents

TRAPETS

Introduction

Purpose and Scope

Trapets provides services which our customers may, in some cases, consider to be outsourcing of critical or important functions and/or outsourcing to a cloud service provider and therefore subject to the applicable guidelines issued by the European Banking Authority (EBA), the European Securities and Market Authority (ESMA) or the European Insurance and Occupational Pension Authority (EIOPA). The relevant guidelines include an obligation for the operator to ensure its ability and right to audit the outsourced function or cloud service using a risk-based approach. Where requested, Trapets' customer agreements include a right of access and audit rights for the customer in accordance with the relevant guidelines.

Even for customers or services outside the direct scope of the described regulatory requirements, Trapets' customers may have a need to conduct periodic reviews or audits of Trapets' service delivery with respect to information security.

Prospective customers may also have a need for the same information within their vendor due diligence process and evaluation.

To facilitate a cost-effective review process and easy access to the necessary information, Trapets has summarised key information in this report. Trapets updates the report on an annual basis. This report covers the period 2023.

Trapets facts and contact details

Company name	Trapets AB
Corp. reg. no.	556586-4773
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
Date of this report	30 January 2024

TRAPETS

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, 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.
- **Market and Trade Surveillance** – for detecting market abuse and insider trading.

Trapets' service offering also include our value-added service **Financial Crime Surveillance** (FCS), combining our solutions with professional expertise to support customers in the daily work to detect, investigate, and report suspicious behaviour.

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 offices: Stockholm, London, and Hanoi. The company is growing rapidly through geographical expansion, new customer segments, investments in product development, and via acquisitions.

The proprietary 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, Financial Crime Surveillance, 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 markets are the Nordic region, but in recent years with an increased focus on markets outside the Nordic region, with an emphasis on the UK.

Information security is core at Trapets. Trapets started early with a continuous improvement effort in this area with internal training, internal and external security audits, and a variety of other security measures. The company has been ISO27001 certified since 2018.

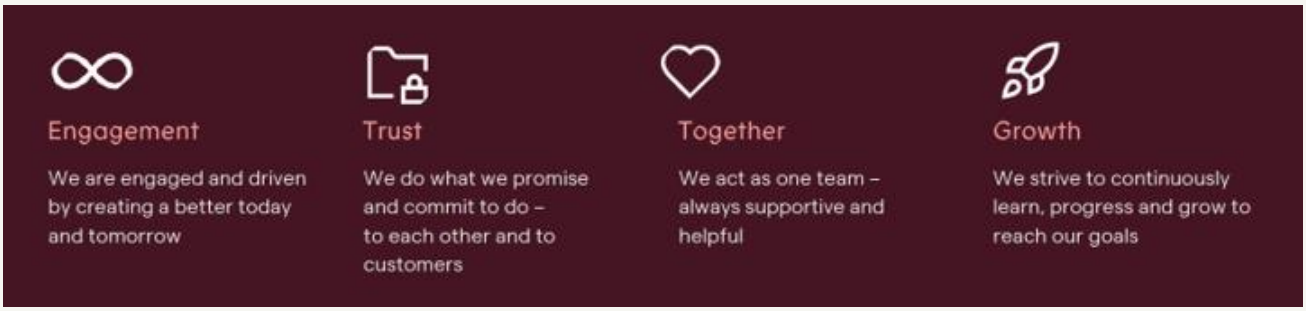
Trapets is a healthy company with high solidity, liquidity, and the highest credit rating. No product development or goodwill is balanced. The company is majority owned by Monterro, a Nordic private equity firm, together with minority ownership from the founders and employees of the company.

During 2023, Trapets acquired Regtech Solutions AB, a Swedish software company offering Know Your Customer and screening services in non-financial segments in Sweden. A legal merger of the company was completed in November 2023, and internal organisation, operations, and processes are gradually being incorporated into the Trapets framework.

Organisation and employees

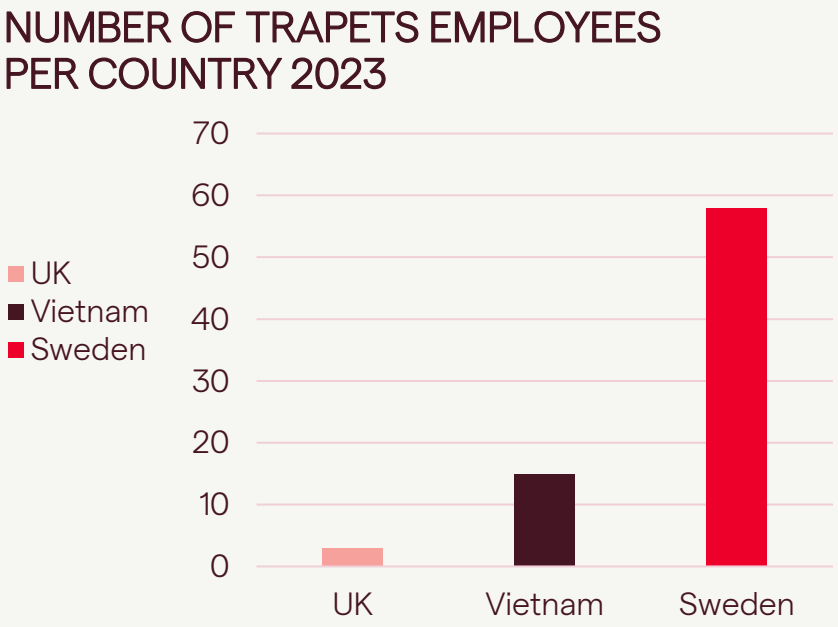
Core Values

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



Organisation

At the end of 2023, the total number of employees was 76. The FTE gender distribution is 66% male and 34% female. The gender distribution within the management team is 60% male and 40% female.



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 on the candidate. Trapets require each new employee to provide an extract from criminal records or as local legislation permits. 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, awareness, updated policies for employees etc	Q1 2023	Passed	CISO	Internal audit, Q-branch
Organisation, roles and responsibilities, competences, awareness etc	Q2 2023	Passed	CISO	External audit, SBcert

Code of conduct

Trapets' Code of Conduct gives internal guidance on business principles and policies in our daily operations. Every individual has a critical role in defining and protecting our most valuable asset - trust.

Trapets' Code of Conduct 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 25 January 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

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 2024.

Information security goals and objectives

Trapets current tactical information security goals and objectives are:

- Remediate all critical security vulnerabilities.
- Penetration testing performed, documented, and stored, in conjunction with major changes.
- 100% attendance of OWASP top 10 training session.
- Review and approval of the current OWASP top 10 list
- 12/12 Security report packages approved by CISO
    - Code scanning
    - SOC/EDR
    - Micro educations & Phishing simulation

TRAPETS

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 2023	Passed	CISO	External audit, SBCert

TRAPETS

Services/systems

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

- **Transaction Monitoring** (formerly Instantwatch AML) (Anti-Money Laundering)
- **Customer Due Diligence** (formerly Instantwatch CDD) (Customer Due Diligence)
- **Screening** (formerly Instantwatch KYC) (Know Your Customer)
- **Market and Trade Surveillance** (formerly Instantwatch Market)

The systems are managed within Trapets ISMS without any exclusion of information security policies, security mechanisms or operational processes. 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 perspective. In addition to the ISO 27001 audit, the Instantwatch products delivered as a service are regularly subject to penetration tests and annual Disaster Recovery (DR) tests.

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

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	Q4 2023	100% attendance	CISO	External, SBCert
Security awareness & attack simulation	Employees & consultants	Q4 2023	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.

The systems in use to deliver Instantwatch as a service operates on resources behind dedicated Next Generation Firewalls. The firewalls in place secure controlled access to the Instantwatch solutions by IP restriction and provide the Intrusion Protection System (IPS) service.

The IPS constantly monitors network traffic to identify threats. IPS proactively detects and prevents harm from malicious traffic. IPS protection identifies potential threats by monitoring network traffic in real time by using network behaviour analysis.

DDoS protection is secured both at the internet service provider and in the IPS. The IT platform is designed in accordance with the Trapets segmentation policy and emphasizes physical and logical segmentation. All resources are subject to security patching, and patches are applied in accordance with predefined patch schemes without any exceptions to the patch policies. Identified Zero-day vulnerabilities will always be patched to mitigate the active threat with the highest urgency, without any delay.

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.

The IT platform is monitored by a designated SOC - Security Operations Center that utilizes EDR - Endpoint Detection & Response on the servers and clients used in the IT platform or by Trapets staff to provide support for the Instantwatch services. 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. Security baselines on laptops are controlled monthly. Code scanning is performed in the build process.

AUDIT				
Activity	Date	Result	Owner	Auditor
Review of security measures	Q2 2023	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, regular 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.

Trapets regularly reviews and updates the data backup policy to ensure that it is in line with the latest best practices and industry standards. The review also includes regular tests of the backup

and recovery processes to ensure that they are running correctly and to identify any potential gaps.

AUDIT					
Product	Activity	Date	Result	Owner	Auditor
Transaction Monitorering (AML)	Restore from database	Q1 2023	Passed	Product Owner	Internal, Qbase
Customer Due Diligence	Restore from database	Q12023	Passed	Product Owner	Internal, Qbase
Screening (KYC)	Restore from database	Q1 2023	Passed	Product Owner	Internal, Qbase
IMarket Trade Surveillance	Restore from database	Q1 2023	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	Q2 2023	Passed	CISO	Internal, Qbase

Datacentres

Trapets only use datacentres that are compliant with Trapets' security requirements, certified under ISO27001 and SOC II compliant. 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.

AUDIT				
On site	Date	Result	Owner	Auditor
Stack datacentre	TBD		CISO	
Interxion datacentre	Q2 2022	Passed	CISO	External, SBCert

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.

A Privacy Awareness Training is held annually for all employees, the latest one was held in June 2023.

AUDIT				
ISO27001	Date	Result	Owner	Auditor
Compliance	Q4 2023	Passed	DPO	Internal, Qbase

Risk management framework

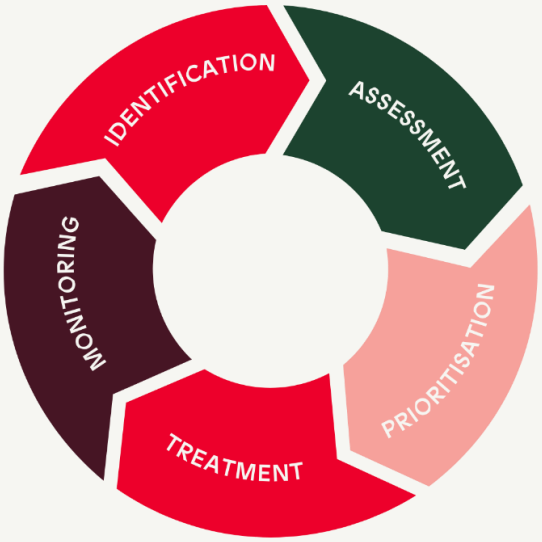
Trapets' risk management framework oversees the entire lifecycle of a risk and encompasses risk events that could potentially impact Trapets' business.

Trapets addresses risks from various perspectives:

- External risks – those arising from external events such as pandemics, macroeconomic crises, or armed conflicts.
- Asset risks – risks directly impacting Trapets' information assets.
- Product and business risks – risks with a negative impact on Trapets' service delivery

Trapets practices quantitative risk assessment, utilizing Likelihood and Consequence to establish the Risk Factor. The Risk Factor signifies the impact if the risk materializes, determining its priority and ranking. Each risk is assigned an owner with full responsibility for managing it according to Trapets' risk process. Risks can be escalated by the risk owner to Trapets management for further evaluation, and those with a Risk Factor = Extreme are directly escalated to Trapets management. Trapets has a risk committee functioning as a management team within the risk framework.

Trapets' risk management process comprises five fundamental steps; identification, starting with risk identification, proceeding to risk assessment, followed by risk prioritization, definition of a treatment plan, and ultimately, ongoing risk monitoring. Follow-up on risks and mitigating activities is conducted at least on an annual basis.



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

Incident management

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

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

Upon the closure of an incident, a decision is made in each case, regarding whether to register a problem for further root cause analysis and learning. Trapets employs the 5 why principle for root cause analysis, aiming to facilitate learning, improvement and quality assurance.

AUDIT				
ISO 27001	Date	Result	Owner	Auditor
Incident Management	Q1 2023	Passed	CISO	Internal audit, Qbranch

Business Continuity Planning (BCP)

Trapets' Business Continuity Planning (BCP) framework incorporates guidance and methodology from the FSPOS (Finansiella sektorns Privat Offentliga Samverkan).[1] Trapets has applied the method outlined in FSPOS for creating a 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 customers' need for high service availability to support them in fulfilling their legal obligations. Consequently, Trapets has developed contingency plans for each Instantwatch product and for its infrastructure. Trapets is committed to achieving and maintaining high availability and rapid restore procedures for each Instantwatch product.

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

[1] FSPOS (Finansiella Sektorns Privat-Offentliga Samverkan: FSPOS Vägledning för Kontinuitetshantering, Version 5.0, 2021-03-16

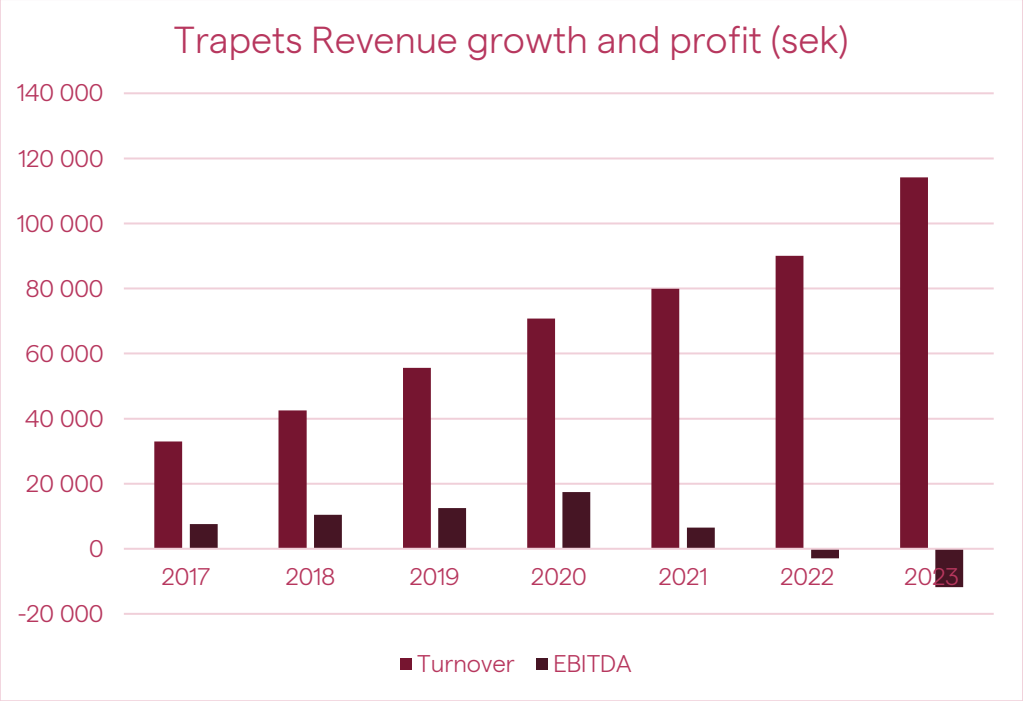
AUDIT				
ISO 27001	Date	Result	Owner	Auditor
BCP Surveillance audit Routines, plans, infrastructure etc.	Q1 and Q2 2023	Passed	COO	Internal audit, Qbranch

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 initiating during 2023 regular Net Promoter Score (NPS) surveys among our customers.

Financial results

In 2023, Trapets experienced a notable 26% growth in turnover, reaching SEK 114 million, albeit with a decrease in profit to SEK -11.8 million, marking a profit margin of -10%. This result and trend is in line with Trapets' strategic objective of broadening its international sustainable market coverage and enlarging its customer base. Investments have been directed towards bolstering resources in Stockholm, enhancing the development department in Hanoi, Vietnam, penetrating the UK market with a select team, and advancing in new technologies to foster scalability. Notably, recurring revenues increased by 26% compared to 2022, reaching SEK 106.9 million in 2023.


Trapets Revenue growth and profit (sek)
140 000
120 000
100 000
80 000
60 000
40 000
20 000
0
-20 000
2017
2018
2019
2020
2021
2022
2023
Turnover
EBITDA

TRAPETS

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 20 September 2023. 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.

Major adverse events

During 2023, 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 2024.

Looking ahead in 2024

The regulatory landscape within information security is evolving rapidly, Trapets expects customer and regulatory requirements to be further expanded and harmonized, via the DORA regulation (*Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*), the implementation of the NIS2 directive and other examples. Trapets is continuously and proactively working to evaluate and manage potential implications with an aim to ensure compliance with

TRAPETS

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 70 employees based in Stockholm, Hanoi, and London.

For more information, visit www.trapets.com.