Vanta

EBOOK

The Global Guide to Starting a Security Compliance Program

ISO 27001

SOC 2

Table of contents

03 Introduction

04 What is a security compliance program?

05 When do you need a formalised security compliance program?

06 ISO 27001 vs. SOC 2: Which is right for your organisation?

07 Similarities between ISO 27001 and SOC 2
08 Differences between ISO 27001 and SOC 2
09 How to determine which standard you need

10 Steps for starting a security compliance program

11 Step 1: Define your organisational goals and needs
12 Step 2: Define your roadmap and timeline
13 Step 3: Prioritise and start building

14 How to take advantage of compliance automation

15 Silvr turns to compliance to fuel growth in Europe and beyond
16 Cable instils customer trust with SOC 2 compliance
17 Coviu streamlines ISO 27001 to fuel growth on a global scale

Introduction

For technology startups, security compliance is often lower on the list of company priorities. After all, startups are juggling a lot these days — from getting their products off the ground to closing critical early deals.

Complying with security standards, however, can actually help boost your business. Larger (and more lucrative) clients often only do business with organisations that adhere to certain standards, such as ISO 27001 or SOC 2. Without the same brand recognition or reputation as large enterprises, a strong security compliance program can help your startup establish initial trust with customers and investors. Most importantly, with strong security compliance, startups are better able to identify and address cybersecurity threats.

Starting a security compliance program requires time, effort, and planning. And knowing where to begin is half the battle. In this guide, you'll learn when it makes sense to start a security compliance program, how to decide between ISO 27001 and SOC 2, and how compliance automation can accelerate your journey.

What you'll learn:

In this guide, you'll learn when it makes sense to start a security compliance program, how to decide between ISO 27001 and SOC 2, and how compliance automation can accelerate your journey.

What is a security compliance program?

Security compliance programs help your organisation identify, implement, and maintain appropriate security controls to protect sensitive data, comply with laws and contractual obligations, and adhere to the standards, regulatory requirements, and frameworks needed to protect customers and enable the business to succeed.

With a security compliance program in place, your company is able to demonstrate that it meets designated security requirements and objectives. These objectives can be internally-defined or established by industry-specific standards, external organisations, or government agencies.

When do you need a formalised security compliance program?

Alongside the evolution of the company's security journey, your organisation might want to proactively opt to build a security compliance program. The right time to set up a formal security compliance program will look different depending on your organisation. Indicators to consider a formal investment might include:

01 You're unable to close deals:

If you're running into compliance as a sticking point in deal cycles, you're looking at a fork in the road for the kinds of customers you'll be able to work with in the future. Your customers expect you to be compliant; more mature companies will often expect you to mature too.

02 You aren't following common best practices:

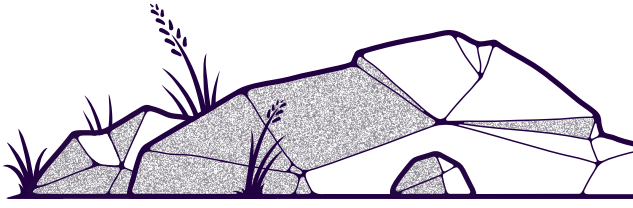
If you're increasingly noticing that what you do seems to be genuinely unique or doesn't sound like how your peers are operating, it's probably time to look to formal guidance. Remember, it's far easier to implement these practices early on—organisational inertia, process friction, and complexity sneak up quickly.

03 Increasing regulatory or social pressure:

If you know you're in violation of regulatory commitments, you could be risking fines that could jeopardise the operation of the organisation. In addition, if you're in a field or area that is highly contentious, high risk, or potentially viewed with a high level of scepticism, you may want to consider a formal investment in security compliance.

04 If you're unable to answer security questionnaires fully or transparently:

While we hope this isn't the case, if you're unable to answer questionnaires thoroughly, it may be time to start moving in a more definitive direction.



ISO 27001 vs. SOC 2: Which is right for your organisation?

Even if you haven't yet been asked by a potential customer or investor about them, you've likely heard of ISO 27001 or SOC 2. While these are both security frameworks commonly adopted by technology companies to demonstrate their security and build trust with customers, they aren't interchangeable.

ISO 27001 is a standard developed to help organisations protect their information through the adoption of an Information Security Management System (ISMS). Established by the International Electrotechnical Commission and the International Organization for Standardization (ISO), ISO 27001 helps businesses organise their people, processes, and technology and was designed to ensure the confidentiality, availability, and integrity of information.

SOC 2, or System and Organization Controls 2, is a standard created by the American Institute of CPAs (AICPA). It provides a framework for ensuring your company securely manages customer data based on five Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy. A SOC 2 report gives companies a recognized way to assure customers, prospects, and business partners that their services are reliable and trustworthy.

Here are some of similarities and differences between the two:

Similarities between ISO 27001 and SOC 2

- **Use cases:** ISO 27001 and SOC 2 are designed with the same general purposes in mind. First, they're both meant to guide you toward implementing crucial best practices for your information security so your data (and your customers' data) is safer. Second, these protocols are designed to enable you to document your security controls and practices so that you can give clients and partners a clear picture of how you're protecting sensitive information.
- **Frameworks:** In addition to sharing similar purposes, ISO 27001 and SOC 2 actually have a lot of overlap between the security controls they include. This isn't surprising because so many of these controls are best practices that are widely agreed upon by today's top information security experts.
- **External audits:** Both ISO 27001 and SOC 2 accreditation is provided by an external auditor. If you are seeking an ISO 27001 certification, you will need to work with an accredited ISO 27001 certification body. For a SOC 2, you will need to work with a licensed CPA (Certified Public Accountant) firm. If you are pursuing both ISO 27001 and SOC 2 at the same time and your audit window aligns, it's possible to work with the same auditing firm if it meets the accreditation requirements to save time.

Differences between ISO 27001 and SOC 2

Compliance requirements: While there is a lot of overlap between the security controls outlined in ISO 27001 and SOC 2, the two standards take different approaches to determining how many of those controls you actually need to implement to be compliant.

Both of these standards indicate that you only need to use the controls that are relevant to your business. ISO 27001 has a broader range of controls, and while you can create your own scope, you need to ensure you have implemented the applicable security controls to obtain the ISO 27001 certification.

SOC 2, on the other hand, is more flexible and customizable. It breaks up the security controls into five categories, and only one — security — is required for your audit. For the four other criteria—availability, processing integrity, confidentiality, and privacy — your SOC 2 report will indicate the controls that you have in place and they will make your SOC 2 report more attractive to clients and partners, but they aren't mandatory.

Locations for use: ISO 27001 and SOC 2 are both well-known in the security industry and in the technology industry. But each is more commonly requested in different geographical locations.

ISO 27001 is generally accepted in Europe and popular throughout the rest of the world. If you primarily do business with organisations outside North America, you'll need to have your ISO 27001 certification.

SOC 2, on the other hand, is generally the go-to security compliance attestation in North America, so if you are doing business with organisations in North America, expect to be asked for a SOC 2 report.

Audit results & duration: Once you've successfully completed an ISO 27001 audit, your auditor will issue a certificate of compliance. An ISO 27001 certificate is valid for three years, during which surveillance audits must be performed each year to ensure that the ISMS and its implemented controls continue to operate effectively. Note that with ISO 27001, you get a certificate telling you you're ISO 27001 certified, but it won't show any nonconformities you had.

Unlike ISO 27001, a SOC 2 audit does not result in a certification. Instead, your auditor will deliver a SOC 2 report that provides their assessment of your organisation's verified security practices against the Trust Services Criteria. Your SOC 2 report will also include insight about your business, your controls, and any non-conformities that were found during the audit period. SOC 2 report is valid for one year and is typically shared directly with prospects and customers.

How to determine which standard you need

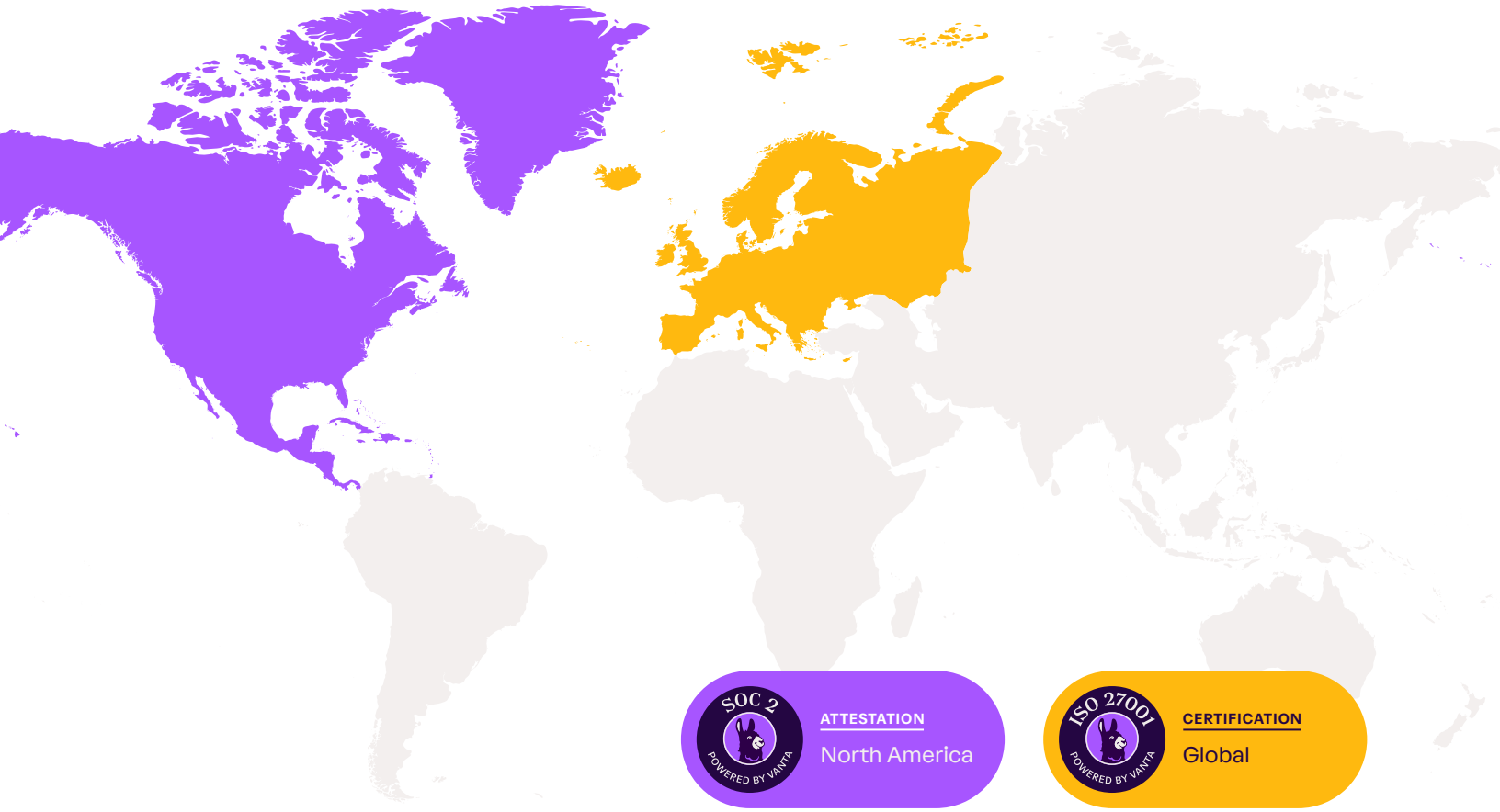
To decide whether you need an ISO 27001 or SOC 2, consider the regions in which your company does business.

If your company focuses much of its work in the UK and EU, ISO certification may be needed. Additionally, if your clients and prospects have sought proof of your company's security against an internationally accepted standard, then ISO 27001 certification will be important.

You may need a SOC 2 if you are starting to work with customers in North America. SOC 2 is a well-known US security standard and has become a common business practice.

Many companies decide they eventually need both ISO 27001 and SOC 2 based on the demands of their growing customer base. At first, your company may consider a ISO 27001 and later pursue SOC 2 as your business expands.

Ultimately, your buyers are your best source of information to help you decide which standard to pursue. If customers or prospects are requesting one or the other (or both), that should inform your decision.



Steps for starting a security compliance program

Step 1:

Define your organisational goals and needs

Start by identifying your organisational goals and needs. For instance, are you starting the program to close deals? Do you want to proactively demonstrate trust or compliance? More importantly, what are you trying to accomplish and why?

After answering these questions, we recommend identifying your desired end state and vetting and aligning this with key stakeholders and their needs. The more granular you can be about your intended goals and desired end state, the easier it will be to work backward toward your objectives and to bring others on board as well.

Before worrying about which standard to implement or what tools to buy, it's critical to ensure these goals are doing more for the organisation than just unblocking deals or solving for one problem. At Vanta, we leverage our compliance efforts as force multipliers wherever possible. For instance, a known compliant process in one business unit could potentially be adapted to work in another, which could streamline cross-functional work and alignment across different projects.

Step 2:

Define your roadmap and timeline

Next, define your roadmap and timeline to understand what you'll need to do along the way to achieve those end goals. Consider breaking your timeline down into specific milestones you'll be able to track and work toward along the way. In addition, think through whether there are any dependencies you'll need to account for and how they relate.

This step should include answering questions such as:

01

What are our known technology needs or gaps?

02

Do we expect we will need to invest in some additional tooling or support?

03

Do we have an understanding of the technical demands of where we want to go?

04

Do we build, buy, or partner?

For instance, if you'd like to build and are planning to hire for the role, consider whether you need someone who's more of a manager who can set direction or someone who's willing to roll up their sleeves as a doer. This is especially important for a foundational role like your first compliance hire.

If you opt to buy or partner, consider whether using services such as a virtual CISO (vCISO), Managed Service Provider (MSP), or other fractional resources could address your needs and objectives in a more cost-effective manner. This is especially important if you have a very broad tech stack or complex operations, as an MSP or vCISO firm will usually have access to more expert resources than any one person can be expected to know.

If you're building a program from the ground up or for the first time, it may be more cost-effective to use a trusted third party to supplement your work than to hire one or more full-time employees to build a program in-house.

Regardless of what option you go with, you're likely looking for an individual—or even a team—with privacy and/or compliance knowledge as well as technical engineering knowledge.

Part of defining your objectives also includes measuring your progress and ensuring that what you're measuring is relevant to your intended outcomes. As you develop your program, be sure to identify key metrics that help your organisation understand and share the achievements and outcomes of your security compliance program.

Remember that you'll need to prioritise what you'll build and when. This is especially true given that you'll likely have a long list of action items, and more tools and needs than you have budget for. The approach we've taken at Vanta is to align our security compliance program with our business objectives—which also ensures we're meeting the needs of our customers and our overall business.

Step 3:

Prioritise and start building

Now that you have an understanding of your needs and timeline, it's time to start prioritising your efforts based on the needs and constraints of your business.

You can start by taking the following steps:

01

Double-check alignment with business objectives—does your plan still look like what the business needs or is there scope creep that might introduce unnecessary friction?

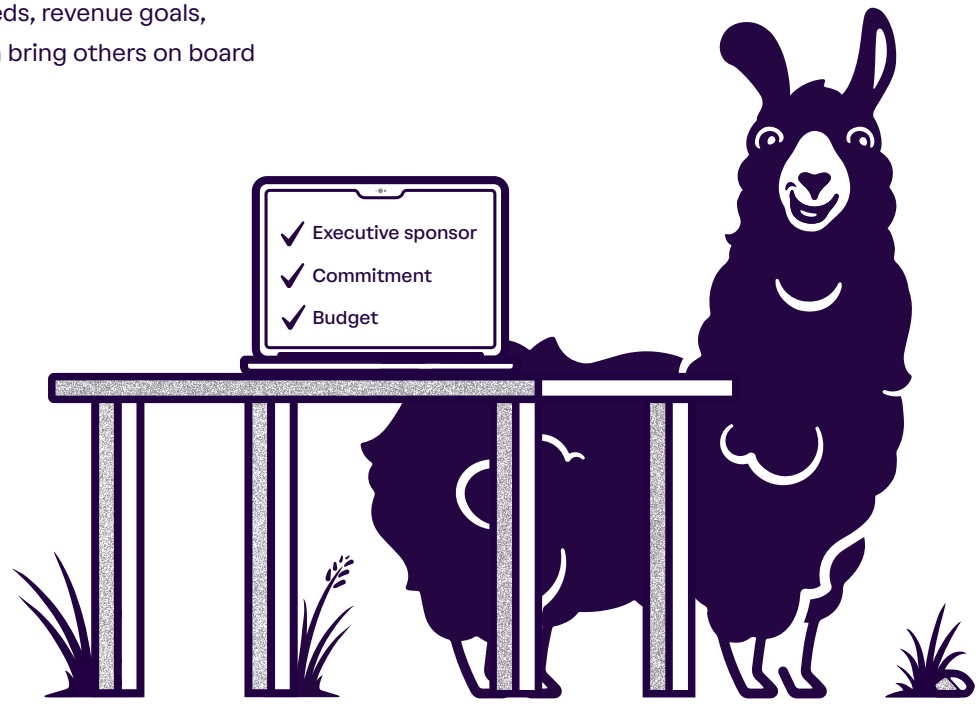
02

Set up deadlines based on your new understanding of your project goals, and officially kick off the implementation of your program.

Remember, security and compliance are infinite black holes without context. Make sure that what you are planning on doing for compliance has guardrails to ensure you're spending your time and effort in places that drive measurable business outcomes.

Lastly, understanding, defining and communicating why you're working toward these objectives—whether toward meeting customer needs, revenue goals, or internal risk reduction—can bring others on board as well.

Don't forget that executive sponsorship, commitment, and budget are some of the most critical components of a strong security compliance program. Seek these out earlier rather than later, and continue to build this bridge by highlighting risks, impact (including positive!) and your company's overall security compliance journey.



How to take advantage of compliance automation

Whether you decide to pursue ISO 27001 or SOC 2, attaining security compliance can be both cumbersome and costly. The time spent bringing your system up to the security standard you need to meet, investigating your security system to assess its readiness, preparing documentation, and more can quickly add up. That's where compliance automation comes in.

Vanta has helped more than 5,000 companies around the world demonstrate their security compliance programs and get ready for audits in weeks, not months. With Vanta's leading trust management platform, you can automate up to 90% of the work needed to become audit ready.

Here are three companies that automated compliance with Vanta:

Silvr turns to compliance to fuel growth in Europe and beyond

Silvr was established in 2020 to offer innovative financing solutions to digital businesses, allowing them to grow without collateral requirements or equity dilution. The company was founded by serial entrepreneurs Nima Karimi and Gregory Tappero with a clear objective: to support budding entrepreneurs in achieving their success stories.

Thomas Pelletier, VP of Engineering, was hired in 2022 to lead technical infrastructure and information technology at Silvr. However, due to the heavily-regulated nature of the fintech industry, his role quickly evolved and he was also tasked with leading security and compliance efforts. Silvr handles sensitive customer data, such as banking, financial, and CRM information, and Thomas quickly recognized the central role of security and compliance in establishing trust with their customers.

To tackle these challenges, Silvr adopted a proactive approach to managing risk by implementing comprehensive security controls, employee training, and regular audits. This not only bolstered their security practices but also helped foster a culture of security awareness throughout the organisation.

However, as customer expectations continued to increase, Thomas knew it was essential for Silvr to explore some of the global compliance frameworks to demonstrate trust. Without proof from a compliance standard, proving trust to prospects required more time and effort to reassure them that Silvr was handling their data safely, so they began to research the various standards recognized throughout Europe and decided on getting ISO 27001.

After partnering with Vanta, Silvr successfully achieved ISO 27001 certification — within their planned timeline. Thomas especially credits Silvr's success to his Customer Success Manager and Vanta's support team who guided him throughout the implementation process and provided advice on the best way to approach information security more broadly.

With Vanta, Thomas now has visibility into Silvr's progress to additional standards by being able to see what controls overlap with ISO 27001 — saving him valuable time from duplicating efforts. They've seen the benefits of expediting their compliance by using Vanta and their certifications to assure prospects about the protection of their financial data and plan to continue to strengthen their security posture as they expand throughout Europe.

cable Cable instils customer trust with SOC 2 compliance

Cable is the leader, and first of its kind, in automated financial crime assurance. Cable enables fintech organizations, banks, banking-as-a-service (BaaS) providers, and compliance officers to automatically monitor BSA compliance in real-time.

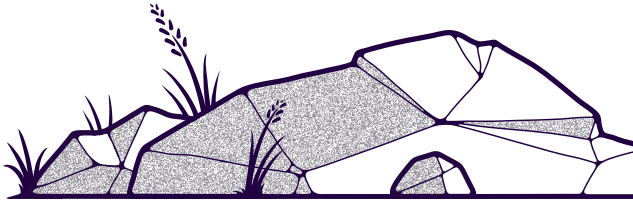
Due to the highly sensitive nature of Cable's industry, the company began designing its regtech software with a security-first approach. With SOC 2 already underway, as soon as she joined the Cable team, Business Operations Manager Valerie Priven focused on finding the right compliance partner. "Within the first few weeks, one of the big points I made was actually picking Vanta as a vendor. I realised we needed to make sure we had the right security foundations in place."

With limited resources and a small team, they didn't want to risk a DIY approach to compliance. Before turning to Vanta, Cable experienced slow progress and unclear security guidelines from using another security vendor. The evidence collection process, in preparation for their first audit, was mostly manual. These issues were greatly reduced after Cable selected Vanta's automated platform.

Cable uses Vanta's templates and documents to prove its security to prospective clients and vendors. Because the majority of Cable's prospects share highly sensitive data with Cable, the ability to quickly and easily share proof of security instils trust in the business. "Vanta's policies are really easy to read and super customizable," says Valerie. "We've already sent our reports to potential customers. As an evolving startup, it's really important to have clear policies that are easy to update."

Vanta's internal audit experts assisted Cable in procuring a trustworthy auditor whose insight and guidance made the audit experience feel comfortable throughout the whole process. Vanta's automated compliance platform enables the various teams at Cable to monitor, customise, and address events in real-time without needless back-and-forth. Cable conducts day-to-day maintenance through ticketing, tests, and dashboard alerts.

Due to Cable's positive experience with Vanta, they are now voluntary beta testers for new product features and updates. Cable regularly interacts with Vanta's product managers to improve the Vanta platform through valuable feedback. Cable plans to pursue SOC 2 Type II, ISO 27001, and ongoing penetration testing through Vanta.



Squadify uses Vanta to breakthrough into enterprise deals

Originally founded as a spin-off from a professional services firm, Squadify was created in 2019 as an innovative alternative to corporate training, by offering novel strategies to improve teamwork and performance through technology. Squadify's unique platform provides data-driven insights and a range of services to laser-target team development and deliver results fast. Unlike conventional platforms that focus on individual performance or provide collaboration software, Squadify targets the very dynamics that foster effective teamwork and drive performance.

In their early stages of growth, Squadify catered to primarily smaller organisations and HR departments, who were less concerned about stringent compliance and security standards. This segment was easily reachable through their network of coaches, who facilitated their entry into these businesses.

However, as Squadify's vision expanded, they set their sights on moving upmarket, a move that prompted a change in their sales approach. These bigger organisations had robust procurement processes that demanded strict compliance assurance that Squadify was protecting their customer data. This change marked the moment when Squadify recognized the need for compliance certification, as the lack of external validation was becoming a tangible barrier to growth, preventing them from securing partnerships with potential enterprise clients. ISO 27001 certification emerged as the primary requirement to satisfy these procurement processes and continue their ambitious growth trajectory.

To meet this challenge, Squadify initially collaborated with a local auditor in Australia who performed security audits. The plan was to tackle the ISO 27001 certification process manually, using spreadsheets and manual evidence gathering. However, it proved to take up too much of the team's valuable time, and the timeline by which they would become certified was not quick enough for the fast-moving Squadify team.

Squadify then began to explore alternatives — they needed a solution that could streamline the certification process and minimise manual effort, and thus, the appeal of compliance automation became increasingly clear.

Squadify knew that they required a solution that offered automation, expert guidance, and a robust support structure. They also knew that working with a technology partner would add value and credibility as a technology company themselves. Their search for an ideal solution ended when they found Vanta.

Navigating the labyrinth of ISO 27001 requirements can be time and resource-intensive — however, by integrating Vanta into their tech stack and automating evidence gathering, Squadify was able to reduce the number of hours spent on compliance tasks, allowing them to refocus on more business-essential tasks.

With Vanta, Squadify was able to set up their security workflows more effectively. They were able to easily assign security tasks to team members through Vanta's two-way task-tracker integration and utilise Vanta's included policy templates to create a robust set of 29 policies. "With Vanta, it wasn't about ticking the policy boxes — it was about ensuring we had proper governance," says Pia.

Vanta

Vanta is the leading trust management platform that helps simplify and centralise security for organisations of all sizes. Thousands of companies rely on Vanta to build, maintain and demonstrate their trust—all in a way that's real-time and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, New York, San Francisco and Sydney.

REQUEST A DEMO

VANTA.COM