How to start 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.

Temps de lecture : minute

---

26 July 2023

In other words, with a security compliance program in place, companies are able to demonstrate that they meet designated security requirements and objectives. These objectives can be internally-defined or established by industry-specific standards, external organisations, or government agencies.

In this post, Matt Cooper and Adam Duman from *Vanta's Privacy, Risk, & Compliance* team explain how you can start a security compliance program in your organisation.

How to identify when you need a formalised program

Alongside the evolution of a 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:

- 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.
- 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.
- 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 skepticism, you may want to consider a formal investment in security compliance.
- 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 bite the bullet and start moving in a more definitive direction.

Steps for getting started

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 to work 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 identifying the answer to questions such as:

- What are our known technology needs or gaps?
- Do we expect we will need to invest in some additional tooling or support?
- Do we have an understanding of the technical demands of where we want to go?
- 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 FTEs 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 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.

As a tip, our team likes to reference Verizon's *Five Constraints of Organisational Proficiency* as described in their *2019 Payment Security Report* to help structure our approach to our compliance program. This framework highlights the importance of capacity, capability, competence, commitment, and communication as key for the health and effectiveness of a strong data protection compliance program—we suggest giving it a quick read if you're interested!

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:

- Double-check alignment with business objectives—does your plan still look like what the business needs or has it had some scope creep or plan drift that might introduce unnecessary friction?
- Set up official 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.

Read also
ISO 27001 certification: what startups need to know

Additional considerations: stakeholders and resources

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

As discussed in our previous post, *we use Vanta as a key element* in building and scaling our own security compliance program. Vanta’s Partnerships team also has a strong network of trusted organisations who can guide you in the process of defining and getting started on your own security journey.

After you determine your goals and identify your tooling and technology needs, it helps to know what tooling is available and what meets those needs most. Referencing industry trends and feedback can be a good place to start, as well as networking with others in the industry who are or have addressed similar challenges.

Tips and suggestions for building your security compliance program

While every team and company approaches building security compliance programs slightly differently, here are a few tips we'd suggest:

- Build repeatability: While it may be tempting to aim for quick wins, focus on repeatable processes and repeatable outcomes within your program. Remember that fire drills are often an indication of broken processes.
- Start with a strong foundation: Focus on the fundamentals and do your basics well—no matter how mature your program, the fundamentals always matter.
- Avoid shiny object syndrome: Tools and technology may help, but will only exacerbate broken processes.

Matt Cooper and Adam Duman are from Vanta's Privacy, Risk, and Compliance team. Visit *Vanta's website* or watch their *on-demand demo* to learn more.

Article by Maddyness, with Vanta