Vanta

The ultimate guide to scaling your compliance program

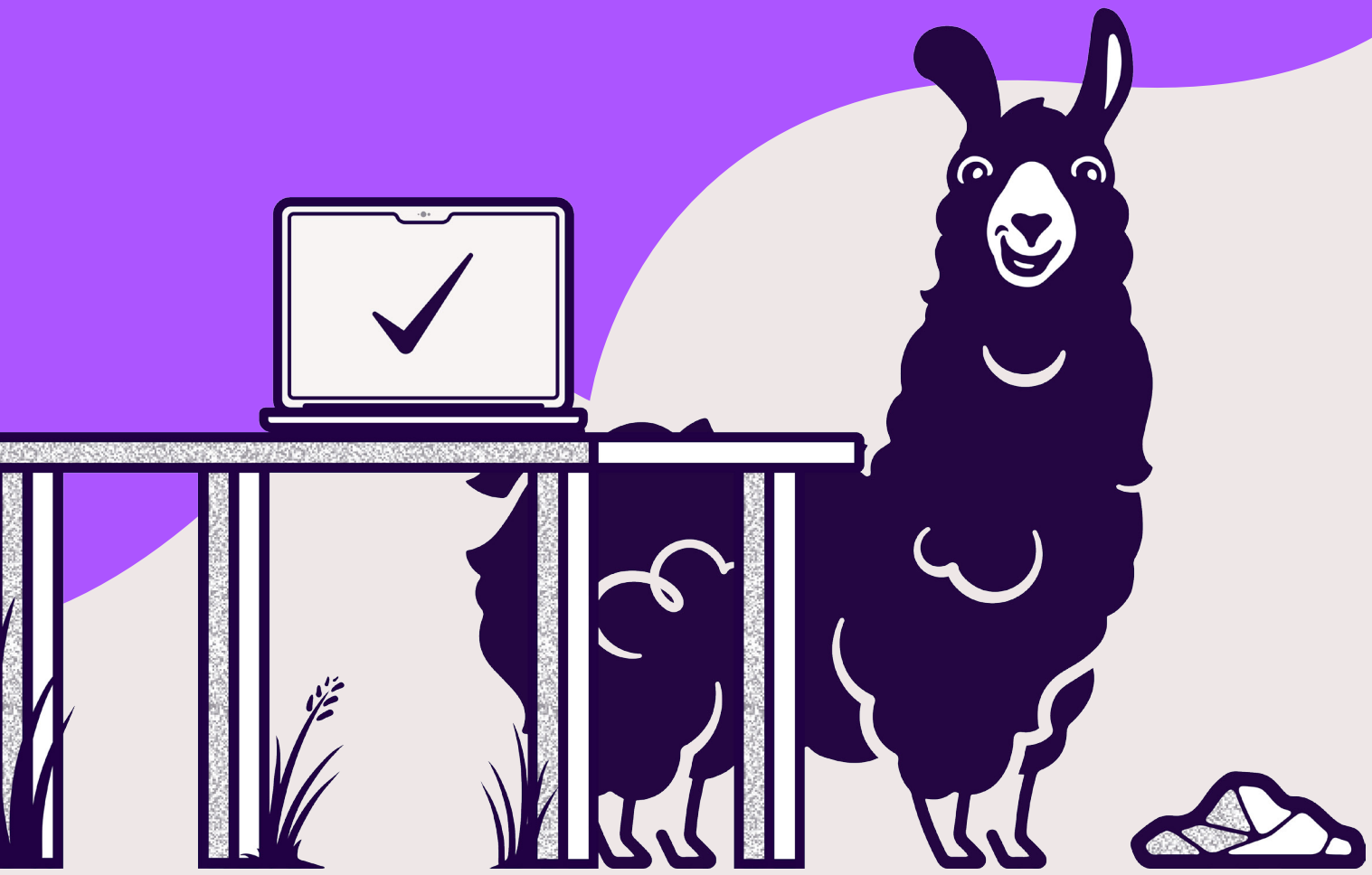


Table of contents

Introduction

At the risk of sounding dramatic, complying with the right information security standards can make or break your business. If you're too lax, you could take your business out of the running for lucrative clients who only do business with organizations that adhere to a certain standard. You could even be at risk for costly legal penalties if you don't comply with specific information security regulations.

That's why it's so important to have a robust compliance program. In a startup's early days, haphazardly combing through an ISO 27001 checklist and maybe giving it another glance every so often might have worked. However, for a business to have a future, it needs to take security and compliance seriously. You need a compliance program that is sophisticated, well-planned, and organized in a scalable and practical way.

No matter where you're starting, growing your compliance program is a sizable job that takes time, effort, strategy, and planning. Our compliance specialists are here to help.

What you'll learn:

We've put together this guide on growing your compliance program and setting up your organization to thrive at any size.

Chapter 1:

Top strategies to grow and enhance your compliance program

Establishing a consistent and productive compliance program involves bringing a variety of strategies together into one comprehensive plan. Whether your business is growing, you're struggling to manage an increasing list of standards you need to meet, or you've just found that your compliance needs to be more intentional, these strategies can help you refine your program.

Assign clear roles and responsibilities

One of the most common culprits of expensive and troublesome compliance errors is letting tasks fall through the cracks. As simple and avoidable of a mistake as it is, it can be a massive burden to your business. You can generally avoid it by having a well-planned and well-communicated division of responsibilities.

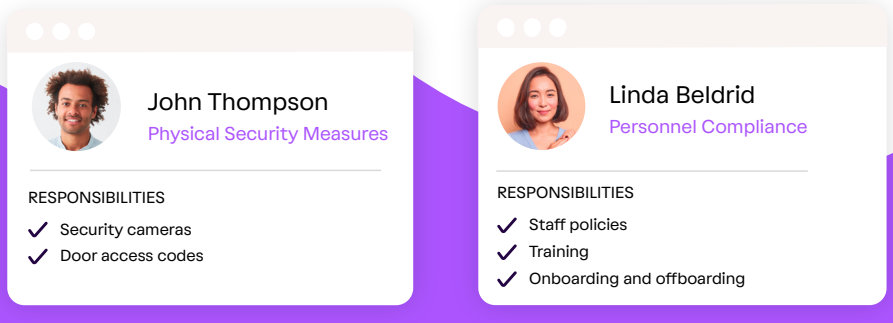
Within your compliance program, delegate both tasks and responsibilities. Appoint a person to be the responsible individual for specific initiatives, compliance issues, or aspects of your data security. For example, you can name one person to head up your physical security measures like security cameras, door access codes, and so on. Someone else can be responsible for your cloud security, while a separate person oversees all personnel-related aspects of your compliance like staff policies, training, onboarding and offboarding, and so on.

The structure and complexity of this will depend on the size of your organization, the standards you need to comply with, the compliance professionals you have available, and more. Regardless, giving specific roles and responsibilities to each person and communicating them clearly ensures that every task has someone making sure it gets done so you're less likely to overlook any essentials.

Establish a unified source for compliance management

Make no mistake: compliance management is complicated. Any standard you need to adhere to will involve a variety of security measures and requirements that span numerous aspects of your business and have many types of documentation. Your team is going in so many different directions that it's easy for your compliance program to become too cumbersome to manage effectively, especially if it needs to grow. One of the most vital ways to streamline a compliance program is to have one electronic source for everything.

Ideally, you want a single platform or digital location to track and assign compliance-related tasks, assess your adherence to each standard or regulation, collect documentation of your compliance, and so on. Having one unified source for everything allows you to grow your compliance program without heightening the chance of miscommunications, misplaced files, missed tasks, and more.



The most efficient way to do this is with a specialized compliance platform. Vanta's two-way task tracker integrations, for example, bring together everything you need for your compliance tracking: checklists, tasks, documentation, compliance automation, and more. Admins can create tickets straight from Vanta into supported task trackers on supported pages to help users fix things faster. Rather than making Vanta a task tracker, Vanta connects to them. This simple solution plays to both Vanta and the task tracker's strengths.

Establish continuous monitoring

A common growing pain many companies feel as they need to comply with more and more standards and regulations is monitoring for compliance breaches. Any change an engineer makes to your information security system runs the risk of breaking your compliance. This can happen if you don't make changes, too, such as if your version of a firewall becomes outdated or if a failure occurs in your access control system.

To develop a more growth-compatible compliance program, you need to have a way to continuously monitor your systems for adherence to the standards your organization follows. The ideal way to do this is to automate it with a software tool like Vanta which routinely scans for compliance gaps in the background. This allows you to keep up with your compliance for all the standards you need to follow without spending the time to monitor it manually.

Integrate compliance requirements into the onboarding process

Nearly all security or information management standards you may need to comply with will involve your personnel in some way. They often require you to have security policies and reporting procedures all your staff must follow, implement security training for employees so internal access log-ins are less likely to be compromised, and so on. One of the most vital ways to grow and enhance your compliance program is to integrate those requirements into your onboarding process.

If you don't already, your organization should have a documented, consistent onboarding process each person goes through. While the training in their day-to-day jobs will be different, they should each follow the same steps otherwise.

This could include:

- Reading your applicable security policies and signing a document agreeing to follow them
- Receiving an individual access control device like a fob or keycard to get into the areas of the facility they need to access
- Receiving or setting up an individual log-in that meets your standard for complexity
- Completing security training that covers topics like how to detect phishing emails and how to know when it is and isn't safe to click a link

This process needs to be thoroughly documented so every new employee or contractor goes through every step. You also need to express to your HR staff or whoever performs the onboarding that this process isn't just a matter of internal preferences; it's a necessity for meeting compliance standards that determine if your organization sinks or swims.

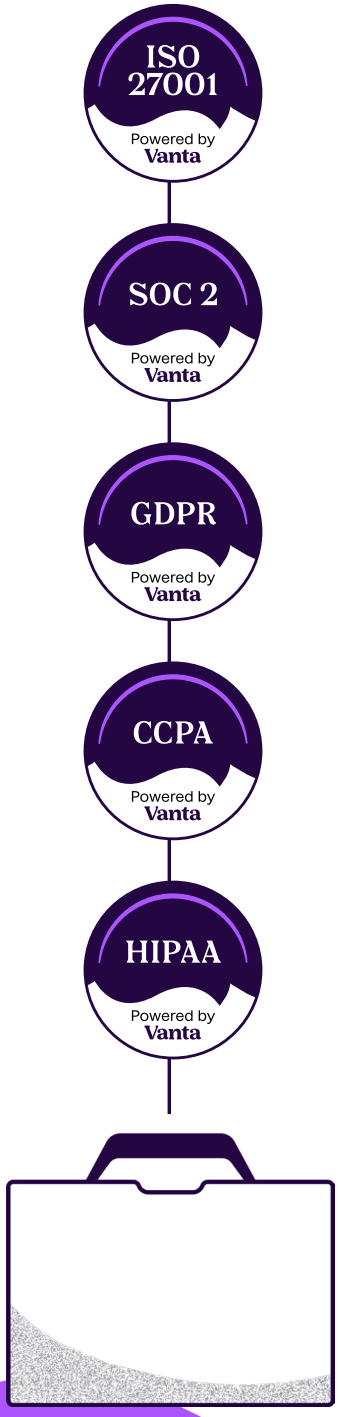
Allocate compliance funding annually

No matter how you slice it, complying with security standards and regulations costs money. It comes with expenses like security software subscriptions, physical security monitoring, secure data storage, knowledgeable compliance professionals, and so on. Funding is crucial to growing your compliance program and making it as comprehensive and organized as it needs to be.

For that reason, be sure to build compliance management into your annual budget. Allocate enough funding to maintain your ongoing compliance program as it stands today to account for the projected growth and complexity of the coming year. If you're concerned about buy-in from leadership, show them the missed opportunities of non-compliance with ISO 27001 or SOC 2. More importantly, show them the risks of not complying with GDPR, CCPA, or HIPAA.

Implement the growth strategies you need

The strategies and techniques above can all help you make your compliance program more sophisticated, productive, and organized. Keep in mind that every organization's compliance needs are different, so some of the strategies may be more applicable to you than others. Growing your compliance program is all about constructing a practical and streamlined plan that suits your needs.



Chapter 2:

How to manage compliance with multiple standards

While the world of information security has many agreed-upon principles and best practices, there isn't a universal definition of what makes a system or organization secure. There will always be differing professional opinions and requirements for different industries or business functions.

Because of this, as your organization grows, you're likely to find yourself juggling compliance with multiple standards and regulations. ISO 27001, SOC 2, GDPR, PCI DSS, CCPA, HIPAA — the more widespread and multi-functional your organization is, the more complex your compliance needs will become.

Let's take a closer look at this common way compliance programs are forced to grow, and explore ways to rise to the challenge.

Why might you need to manage multiple security standards?

As you start researching the various common information security standards, you might notice that there's some overlap. For example, many of these standards require you to operate a firewall, encrypt all potentially confidential data, and limit each staff member's access to the minimum they need to perform their job. If all these standards have the goal of keeping your organization's data secure, why would you need to comply with more than one?

Each security standard has a slightly different intent or audience. For example, while SOC 2 and ISO 27001 are both focused on ensuring to your clients and partners that you're taking adequate security measures, SOC 2 is used in North America while ISO 27001 is used throughout the globe.

You also need to follow different legal regulations based on your organization's operations: HIPAA if you serve certain functions in the US healthcare industry, PCI DSS if you play any role in accepting or processing payments, GDPR if you collect data from EU residents, and so on. If your business is expanding to serve new markets or take on new roles and products, expect to be adding more and more standards and regulations to your compliance program.

Common standards combinations

The good news about managing multiple standards and regulations is that you don't have to start from scratch every time. Because there's some degree of overlap between them, you can plan your program accordingly to save time. With the right planning and strategizing, when you add a second standard, it takes far less time than it took to reach compliance for your first standard. Adding a third is even more efficient, as is adding a fourth, and so on.

The standards you might be combining will depend on your organization, your clients, and your operations, but let's look at how some of the most common combinations work out.

Common standards combinations

The good news about managing multiple standards and regulations is that you don't have to start from scratch every time. Because there's some degree of overlap between them, you can plan your program accordingly to save time. With the right planning and strategizing, when you add a second standard, it takes far less time than it took to reach compliance for your first standard. Adding a third is even more efficient, as is adding a fourth, and so on.

The standards you might be combining will depend on your organization, your clients, and your operations, but let's look at how some of the most common combinations work out.

SOC 2 + ISO 27001

SOC 2 and ISO 27001 are both information security standards that are often requested by potential clients and business partners who want to assure that you can keep their data safe and confidential. They both focus on comprehensive data security, including cloud security, breach reporting, physical security, and so on.

While SOC 2 is more commonly used in North America, ISO 27001 is most commonly used elsewhere in the world. You're likely to need both if you're doing business in North America and across other continents, but fortunately, they cover many of the same best practices so if you're compliant with one, you're much of the way toward the second one too.

ISO 27001 + GDPR + SOC 2

GDPR is the legal regulation in the EU that guarantees certain protections for EU residents regarding their personal data. To comply with GDPR, you must not only follow certain policies like deleting a consumer's data upon request, but also use select security practices so the consumer data you collect isn't vulnerable to unauthorized access. If you're already SOC 2 compliant and ISO 27001 compliant, adhering to GDPR will be mostly a matter of setting up consumer opt-ins for data collection, policies and practices for allowing consumers to exercise their GDPR-guaranteed rights, and so on.

GDPR + CCPA

CCPA is essentially California's equivalent to GDPR. It guarantees many of the same consumer rights and requires you to implement many of the same policies and opt-ins as GDPR. If you're serving end users in both California and the EU, you'll need to follow both of these laws, but with such a significant overlap between them, adding one is easy if you already adhere to the other.

The difficulty with adding multiple security standards together

If your compliance program is growing to include multiple data security standards, expectedly, it comes with challenges.

For one, no standard has 100% overlap with any other standard. In other words, there will always be some degree of work to be done if you're adding a new standard to your compliance program.

Second, because there's never 100% overlap, every new standard you add brings a new set of protocols, tools, and tasks to manage. If your team is already spread thin or if you're already concerned about your team missing key tasks, expanding to additional security standards will add to that problem.

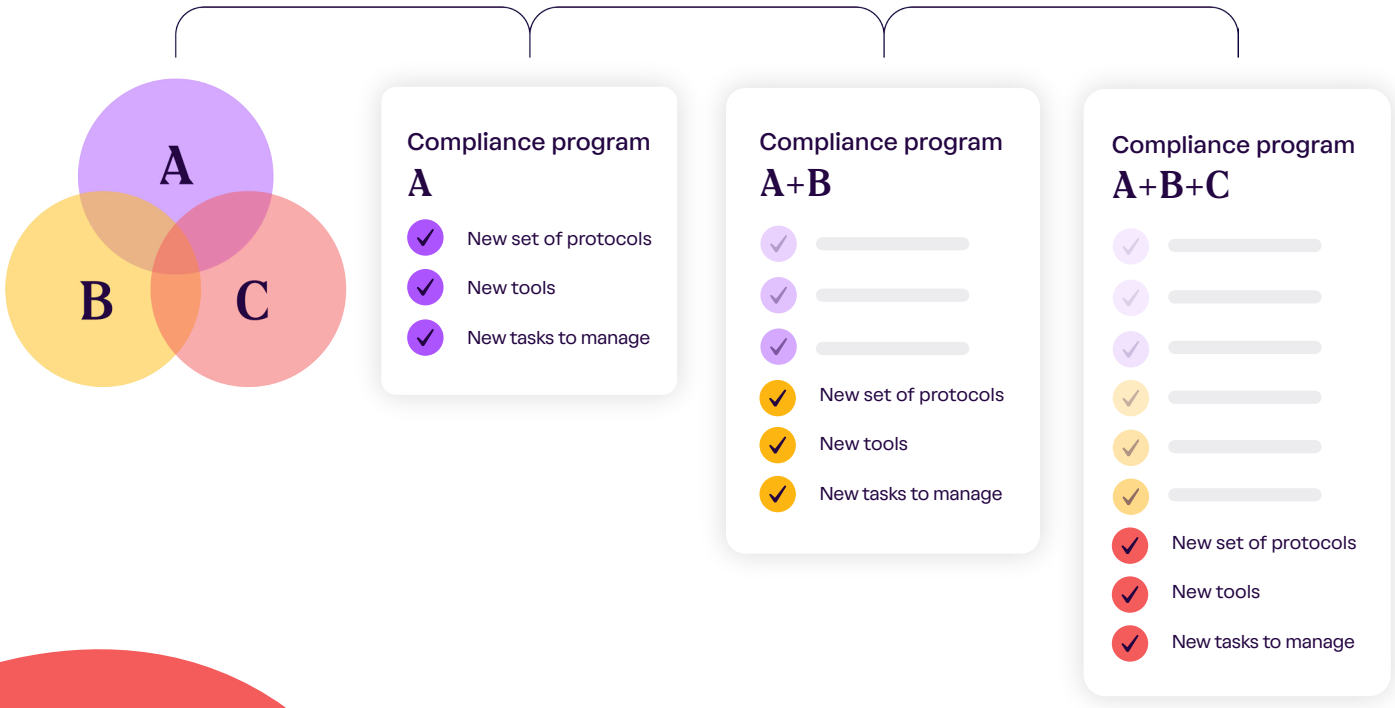
If you're relying too much on manual task tracking and other manual techniques, lengthening your team's to-do list can multiply the chances of something going wrong. Much of the challenge in managing several standards comes from finding a way to keep it all organized and stay on top of things so nothing falls through the cracks.

Use software tools to manage multi-standard compliance

If the primary challenge of adding several security standards together is keeping everything organized and well-planned, what can you do? The best answer typically lies in compliance software.

Specialized compliance tools are designed for precisely this purpose. Vanta's automated compliance software, for example, allows you to manage your compliance with several standards all in one unified platform.

This saves you from all the manual legwork of walking through a checklist of tasks and requirements for each standard one by one. Instead, it combs your system to assess your compliance with each of the standards you've selected, giving you a detailed report for each and generating a to-do list for all your standards together or specific ones.



This software also compiles the data and documentation you need for all your audits into one place. If multiple standards require the same vulnerability test or the same policy documentation, you don't need to duplicate files to have each one on a folder for that standard; you simply tell the software which audit to supply and it brings up all the applicable documentation.

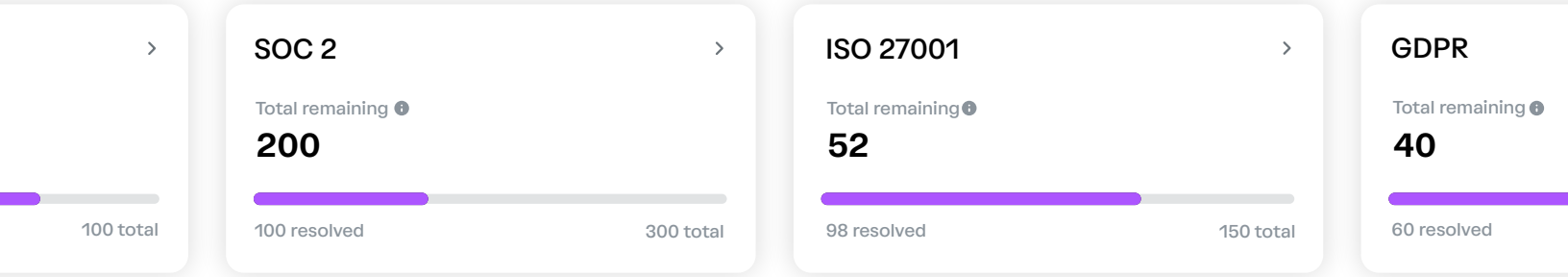
Managing audits for multiple standards

Another aspect of juggling multiple standards in your compliance program is the auditing. While not all standards require a third-party audit or certificate, many of them do, so you may be going through multiple audits each year.

This is another challenge that the right compliance management software can resolve. With tools like Vanta, which serve as a unified place for all the reports and other documentation you need for your audits, you'll have everything in one place and ready to go. The pre-audit scramble of pulling together last-minute necessities is unwieldy enough once per year, so if you have several annual audits, it's particularly important to have everything organized in advance.

Manage a growing list of standards

As your organization grows, the list of standards and regulations in your compliance program is likely to grow too. Now is the time to strategize and find a way to keep it all clean and organized before it becomes unmanageable.



Chapter 3:

How to optimize your growing compliance program

As you grow your compliance program year by year, your focus shouldn't just be on finding a way to keep up with the increasing workload. As your goals get more complicated, you need to be continuously finding ways to optimize and streamline your program so it becomes more efficient, strategic, and scalable.

Of course, that's easier said than done. Consider implementing some of these strategies below to make your compliance program more practical and efficient.

Find ways to automate

If you're trying to stay on top of an ever-expanding compliance program, automation is your best friend. The goal is to automate as many tasks and aspects of your compliance management as possible.

Every time you find a way to automate a process, you save time in the long run, making it easier for your team to absorb more standards and requirements in the future. Automating also reduces the chances that something will be missed or done incorrectly. Human error is always a possibility, so the fewer tasks humans have to do, the fewer opportunities there are for an error.

With that said, technology isn't infallible. It doesn't glitch or fail as often as people make mistakes, but it's still not a guarantee. Implementing a small amount of manual oversight can help your team keep an eye on those automated tasks without the time involved in doing it themselves.

Prioritize security in future system changes

Technology is not a constant. There are always new advances that lead to new versions of security software tools like firewalls and antiviruses, new evolutions in cloud storage or server hardware. Your organization is an ever-changing entity too.

For those reasons, your data storage and information security system will go through changes and modifications on a regular basis. Every time that happens, there's a chance that the upgrade will bring you out of compliance with a critical security standard.

To make your compliance program scalable, you need to find a way to check for compliance breaches with each of those changes or upgrades. If not, you'll constantly be cleaning up after some new migration. Or worse, you may not realize there's a newly missing piece until you fail an audit or discover a data breach.

Set up a process that can identify new compliance gaps when they appear. For example, an automated compliance tool can scan your system for gaps on an ongoing basis so you don't have to take any additional measures.

Track potential savings for future budget justification

As we mentioned above, maintaining a steady flow of funding is critical to keeping your compliance program on the right trajectory and growing it in a smart and manageable way. That might require you to plead your case to upper management, though, and that's best done by showing them how it will impact their bottom line.

As you operate your compliance program, set up a way to keep track of its financial impact. For example, each time the organization signs a new contract or renews a contract with a client, track whether that client requires SOC 2 compliance, ISO 27001 compliance, or compliance with any other security standards. If so, that's a contract your business wouldn't have received if it had not been for your compliance efforts.

It's also a good idea to keep track of problems that were avoided because of your compliance protocols. For instance, let's say your business made a change to its cloud infrastructure and the new infrastructure didn't adhere to one of the needed security standards. If your automated monitoring or other practices caught the problem and resolved it, notate the potential financial consequences if you hadn't found the problem.

Set up a way to do this with minimal time and effort on your part. If you keep a running account of all those savings, it gives you excellent fodder the next time you need to justify funding in a budget meeting.

Set a strategy for adjusting compliance scopes

Not all security standards are structured as simply as, “Here’s a list of requirements you have to meet to be compliant.” Some standards like SOC 2 have a scope that varies from one organization to the next. Essentially, each organization must examine the SOC 2 structure and identify the areas that are and aren’t applicable to it. This scoping is always the first step in attaining SOC 2 compliance.

The tricky part is that your organization’s scope could change from one year to the next. If you change your operations in a particular way or change your business model to start handling a type of data you didn’t handle before, for example, the scope of your SOC 2 report could change

To make your compliance program scalable as your organization grows and becomes more complex, set up a routine strategy for redefining your SOC 2 scope. Design a process to follow before each audit to see if your warranted scope has changed.

Maintain a high standard for documentation

As your organization grows larger and your compliance needs do too, documentation will become more and more vital. For one, you’ll need more documentation to regulate your policies and protocols because you’ll likely need to comply with more security standards and regulations.

Second, the more people you have involved in your compliance program, the more necessary documentation is. It allows everyone to understand the various tasks and strategies involved and ensures that they’re all following the same processes.

Third, larger organizations tend to have higher turnover. If your compliance program is well-documented, it allows that knowledge to be passed along from person to person when even key employees leave. Without that documentation, each new employee could address their duties differently and you lose the all-important consistency in your reporting and compliance management.

Now is the time to start upholding a high standard for your internal documentation. That might mean investing extra time in planning out and writing down the practices and tasks involved in your compliance program, but it’s better to do this now than to wait until each person on your team is operating differently and has to then re-learn everything in a new way.

Grow your compliance program seamlessly

Your compliance program is a necessary part of your business's practices and operations, and make no mistake, it's protecting you from potential disasters on a daily basis. Nurturing this program into a more sophisticated, strategized, and scalable compliance program benefits your business's bottom line and makes life easier for your compliance professionals.

As with any other aspect of a business, though, a compliance program needs its growth to be managed in a specific way so it doesn't become cumbersome and lead to a drop in the quality of your work. With the guide above, you can do precisely this in a controlled and methodical way that serves everyone involved.

If you're taking on the task of growing your compliance program, Vanta can help. Learn more about Vanta's automated compliance software today and allow us to be your partner in smart and strategic growth.

Vanta

Vanta is the easy way to get and stay compliant. Thousands of fast-growing companies depend on Vanta to automate their security monitoring and get ready for security audits in weeks, not months. Simply connect your tools to Vanta, fix the gaps on your dashboard, and then work with a Vanta-trained auditor to complete your audit.

Request Demo →

VANTA.COM