Vanta

Revolutionizing risk:

# How to manage risk with Vanta

# Table of contents

# Introduction

Risk assessment is one of those best practices that is easy to overlook or de-prioritize until it's too late. Perhaps your organization has sidelined risk assessment to take care of other tasks that bring in revenue, but when you lack a solid risk assessment program, you may not realize how many revenue opportunities are lost. Perhaps you've performed a risk assessment at a bare minimum level to tick a checkbox on a compliance audit but you know your organization is still vulnerable.

No matter where you are in your risk assessment journey, Vanta is designed to help you achieve a more robust, thorough risk assessment while also making the process easier for you to manage. We've developed this guide to explain the top risk assessment challenges Vanta relieves and to give you an in-depth look at our newly enhanced ISO-aligned Risk Management solution.

Chapter 1

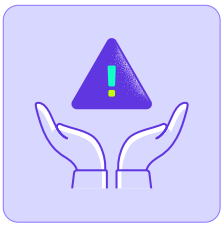
# Risk assessment 101

For starters, let's go through a crash course in risk assessment or risk management. There are countless methods and strategies for managing risk, but the industry-accepted gold standard is ISO risk assessment - the risk assessment process specifically detailed in ISO 27001. This is what Vanta has used for the basis of our enhanced Risk Management solution.

# The five stages of risk assessment

ISO risk assessment or risk management is laid out as a five-step cycle for continuous risk assessment. Let's take a brief look at each of these five stages and how they form a rich and productive risk assessment program.

## 01. Identify risks



The first stage is to identify risk scenarios that could affect your business. These are hypothetical situations that have the potential to occur. Those risks will vary based on the organization. For example, there are certain risks that are inherent to organizations that have remote employees.

At this stage, you aren't assessing vulnerabilities or how to mitigate them. You're merely determining whether the risk is hypothetically possible.

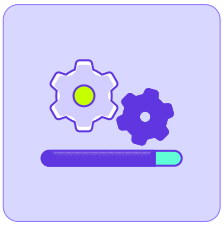
## 02. Assess and prioritize risks

Now that you have a list of potential risks for your organization, this second stage involves reviewing each of those risks individually. You'll consider each risk and determine how high-priority or low-priority it is based on factors like the likelihood of the problem occurring and the impact it would have if it were to occur.

## 03. Treat risks

The third stage is to plan how to treat each risk. Some you may be able to eliminate entirely, while for others, there may be ways to make them less likely or less impactful. Some risks may be so low-likelihood or low-impact that it isn't practical to make any changes. At this stage, you're making a plan of action (or inaction) for each risk.

## 04. Implement treatments, track progress, and verify



In the fourth stage, you're putting your risk treatments into action. You're also establishing a way to track the progress of these implementations and verify their success.

## 05. Report and re-evaluate

The final risk assessment step is to report your organization's risks, how you're approaching them, and what impact your risk management efforts have had. This stage also includes setting up a process to continuously evaluate your risks and continue the cycle.

## About ISO risk assessment

While the five stages above are commonly accepted risk assessment practices, Vanta uses this as merely a starting point. We dive into further detail by basing our Risk Management solution on the RA process in ISO 27001.

While most infosec standards provide general guidelines for your RA program, ISO 27001 takes a more thorough approach. This standard provides a very specific, robust framework for risk assessment.

If you're working toward ISO 27001 compliance, following this risk assessment framework will be inevitable. Even if you aren't, ISO 27001 risk assessment is a highly regarded framework that can give you confidence that you're protecting your organization thoroughly and complying with other information security standard you need to follow.

Chapter 2

# Top challenges with risk management

Vanta's Risk Management is designed around real-world expertise in risk assessment and a mission to address all of the top challenges organizations face in risk assessment. Let's walk through these chief challenges, many of which probably sound all too familiar to you, and consider the solutions to these difficulties.

## Excessive risk

Quite frankly, the risk assessment process can seem unconquerable and overwhelming when you first begin. Finding all the risks that could possibly affect your business might seem akin to listing all the potential illnesses you could come into contact with as you go about your daily life.

With this mountain in front of them, many organizations end up doing the bare minimum to meet any auditing needs they may have, while neglecting their long-term risk management. In the meantime, the organization remains highly vulnerable, leading to high cybersecurity risks, high cyber insurance costs, and potentially a loss of revenue opportunities.

The solution is a more proactive and continuous approach to risk assessment. Organizations need an optimized workflow that makes it all more manageable. This lowers the organization's risks and cyber insurance costs and gives them confidence that they have a long-term solution that meets any standards they need to comply with. It's all about having a genuine ongoing program, rather than checking a box on an audit.

## Manual and complex process

For many organizations, the risk assessment process is manual, complicated, and downright arduous. There's a complex web of spreadsheets, documents, and emails that are hacked together. You're creating reports and content from scratch, trying to juggle task management, and potentially spending hours of valuable analyst time or valuable consultant time to take you through the process. When audit time comes, you're also drowning in emails and phone calls with your auditor to send them the evidence and information they need.

The solution is an automated and simplified SaaS-based platform that manages everything in one place. Ideally, this SaaS platform can guide you through the process (so you can skip the expense of a consultant) in addition to providing templates, automated tracking and testing, and a unified platform that compiles all the evidence your auditor needs in one place.

## Limited and siloed pieces

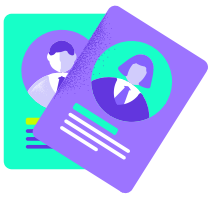
Inevitably, managing risk has a lot of moving parts. A common challenge is that these tasks and components are spread out over numerous systems, tools, and teams in the organization. To add to that frustration, some solutions only cover a single standard. This leads to a piecemeal approach that is challenging to manage because there is little or no integration between stand-alone risk assessment tools.

It can be difficult to keep track of what has and hasn't been done, which often leads to frustration which leads teams to do the bare minimum in order to get the tasks off their backs. The resulting risk assessment doesn't do a reliable job of managing the organization's risks.

The optimal solution is a smooth integration between risk assessment tools — more specifically, a solution that can handle many capabilities in one place and also offers coverage of many standards. This lets everyone collaborate on the same platform so nothing falls through the cracks and everything is organized cleanly.

## Inflexibility

Many existing platforms for assessing risk offer little or no customization. They're designed to work in a specific way, and teams end up paying top dollar, but then struggle to make its process fit their workflows when the processes simply aren't flexible enough to customize.



Many tools are highly segmented, in that they only support one infosec standard with little or no ability to work with each other. Organizations find themselves purchasing several tools and constructing a cumbersome workflow that jumps around between them. There is also the issue with a tool being so overly simplistic that it can't scale with the organization as it grows, so teams find themselves reinventing their risk management program every few years.

The solution is a single platform with scalable, robust capabilities. A tool that can handle multiple infosec standards allows organizations to integrate all their risk assessment needs into one place, and if well-constructed, these solutions are applicable for managing risk outside of compliance requirements too. Organizations need the ability to customize their risk assessment, such as by adding custom risks and treatment plans in addition to migrating existing risk assessment work from their old system.

# How Vanta's Risk Management benefits your business

Simply put, Vanta's Risk Management was designed to address all of the challenges above in order to be the unified, customizable, integrated, scalable solution you've been looking for.

Vanta's solution walks you through a more reliable and comprehensive risk assessment and reduces risk to the businesses and sensitive data. Not only can you ensure that you're ready for any audits you need to pass, but you can have confidence that you've addressed your risks as thoroughly as possible.

This enhanced solution also creates a streamlined, organized risk assessment process. No more jumping back and forth between half a dozen tools and platforms or struggling to coordinate tasks across multiple teams. Vanta brings it all together in an all-encompassing approach.

Make your risk management process less time-intensive and labor-intensive. Vanta's Risk Management is structured as a pre-built content and intuitive workflows that guides you through every stage of managing risk so you aren't poring over websites and documents to try to figure it out on your own or shelling out thousands for a consultant.

On top of it all, Vanta's platform offers reliability and thoroughness you can trust. Our solution was designed with the expertise of industry leaders, so you can rest assured that you're more likely to pass your audits the first time around, leading to lower audit costs and more revenue opportunities.

Ultimately, Vanta's Risk Management is designed to make your work easier and give you better results. In our next chapter, we'll take a look inside the platform to show you precisely how Vanta handles risk management.

Chapter 3

# How Vanta revolutionizes risk management

Vanta is designed to be a comprehensive solution to your information security and compliance needs. A core part of this, of course, is risk assessment and risk management. We're thrilled to announce our newly enhanced Risk Management solution. Allow us to walk you through this innovative system and the way it revolutionizes your risk assessment program.

# Introducing Vanta's new ISO-aligned Risk Management solution

Vanta's automated compliance platform supports a variety of standards and certifications: ISO 27001, SOC 2, HIPAA, PCI DSS, GDPR, and CCPA, with several additional frameworks. Each of these standards requires some degree of risk management, so we've used the gold standard ISO risk management framework to guide every client through a thorough, reliable, robust risk management cycle.

This feature is a fully integrated part of our compliance solution. As a feature on our unified platform, our Risk Management tool coordinates seamlessly with other aspects of your compliance process.

It is designed to be practical and easy to use for anyone, from risk assessment novices at small organizations to specialists at large enterprises. We guide you through the entire risk management cycle, from identifying risks, through reviewing and mitigating risks, to testing and re-evaluating.

To give you an in-depth look at how our risk management feature works, we'll walk you through each of the five risk assessment stages and explain how Vanta makes them easy and manageable.

# Identifying risks

Our risk management process begins with identifying the risks that your business could face. This stage can be highly challenging if you're doing it on your own because there's no way to know if and when you've done a thorough job. Vanta's solution changes this.

We have a detailed, expertly assembled library of risk scenarios. They include scenarios, like your organization violating customers' data rights, company data being compromised by insecure remote work sites, and so on. In a nutshell, Vanta takes you through each of these scenarios so you can identify how applicable they are to your organization.

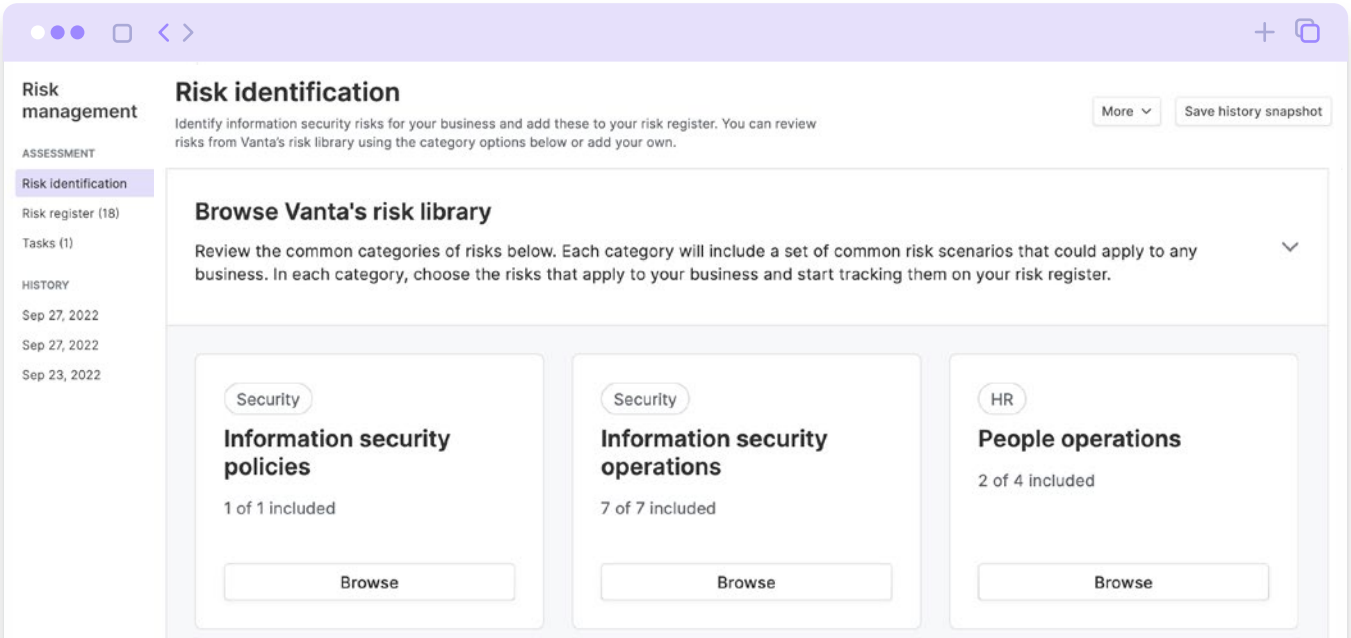
When you click into one of these categories, you'll see a list of risk scenarios. For each one, you can determine how likely it is to happen to your organization and how severe the impact would be if it were to happen. You can also add notes for further details.

As you click through these categories one by one, you'll be forming a table of possible risk scenarios that you can review and address further in the next risk assessment stages. Vanta's risk library allows you to identify the potential risks for your organization without trying to come up with risks off the top of your head and without scouring the web for example lists.

Of course, each organization is unique, and you may face risks that are not in our risk library. Our solution includes the ability to add your own custom risks and rank their likelihood and impact the same way you would with items from the risk library.

**As you enter the risk identification dashboard, you'll see numerous categories of risk scenarios. For example, some of these categories include:**

- Information security policies
- Organization of info security
- Human resource security
- Asset management
- Asset control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance
- Fraud

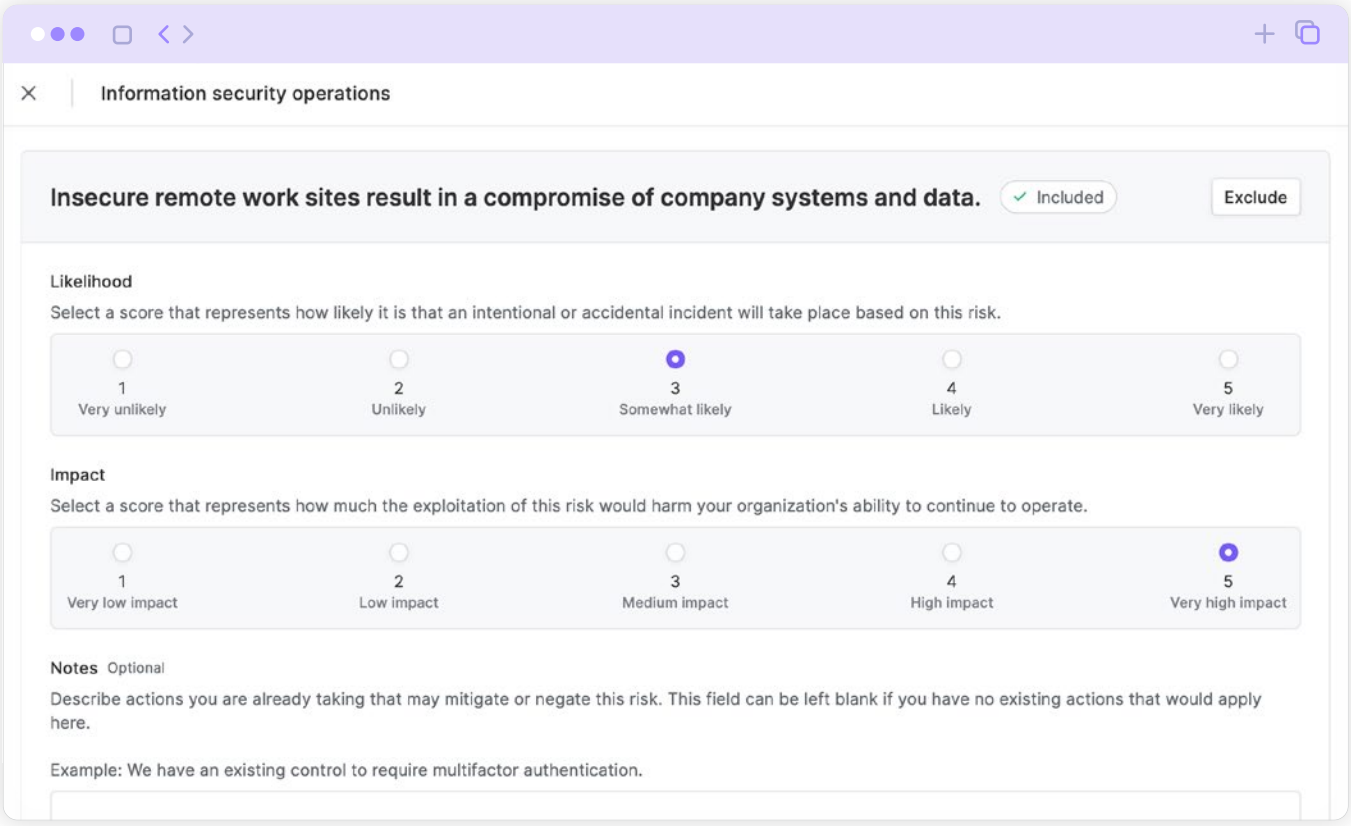


# Assessing and prioritizing risks

Once you have identified all of the potential risks to your organization, you move on to the next risk assessment stage: assessing and prioritizing risks. Within Vanta's platform, you can do this in the "Review risk" tab.

When you open this tab, you'll see a table of all the risks you identified in the last stage as well as the risk score based on the likelihood and impact you selected. When you click into each one, you can take a closer look to determine how to prioritize the risk.

The table of risks you see here will become a core part of your risk management moving forward. It shows you key details at a glance, including the assigned owner, treatment path, residual risk, and review status for each risk. This is where you'll track your progress toward treating each risk as effectively as possible.




| | | | |
|---|---|---|---|
| Insecure remote work sites result in a compromise of company systems and data. | Appropriate contacts with interest groups are not maintained resulting in a lack of understanding of current threats. | Appropriate contacts are not maintained resulting in breach response and reporting. | Information security responsibilities have not been defined or allocated. Therefore, responsibilities are unclear. |
| ✓ Included | ✓ Included | ✓ Included | ✓ Included |

# Treating risks to reduce or eliminate risks

When you select the path you want to take, Vanta will then show you suggested actions you can take. For example, if you select “Mitigate,” you will see suggested security controls you could put in place to minimize this risk.

In this way, Vanta doesn’t only help you organize and manage your risk management process, but it coaches you with best practices and expert strategies to help you with each stage of the cycle.

Of course, customization is a top priority too. In addition to the suggested controls Vanta offers, you can add your own controls or tasks too.

To help your team stay on track with all your risk management tasks, you can assign an owner to each of your risks. This ensures that each risk has a point person who is accountable for making sure it gets done. Otherwise, it’s easy for tasks to fall through the cracks.

The last step in this stage is to determine the level of residual risks. In other words, once you’ve completed your mitigation tasks and implemented your risk treatments, what will the likelihood and impact of the risk be?

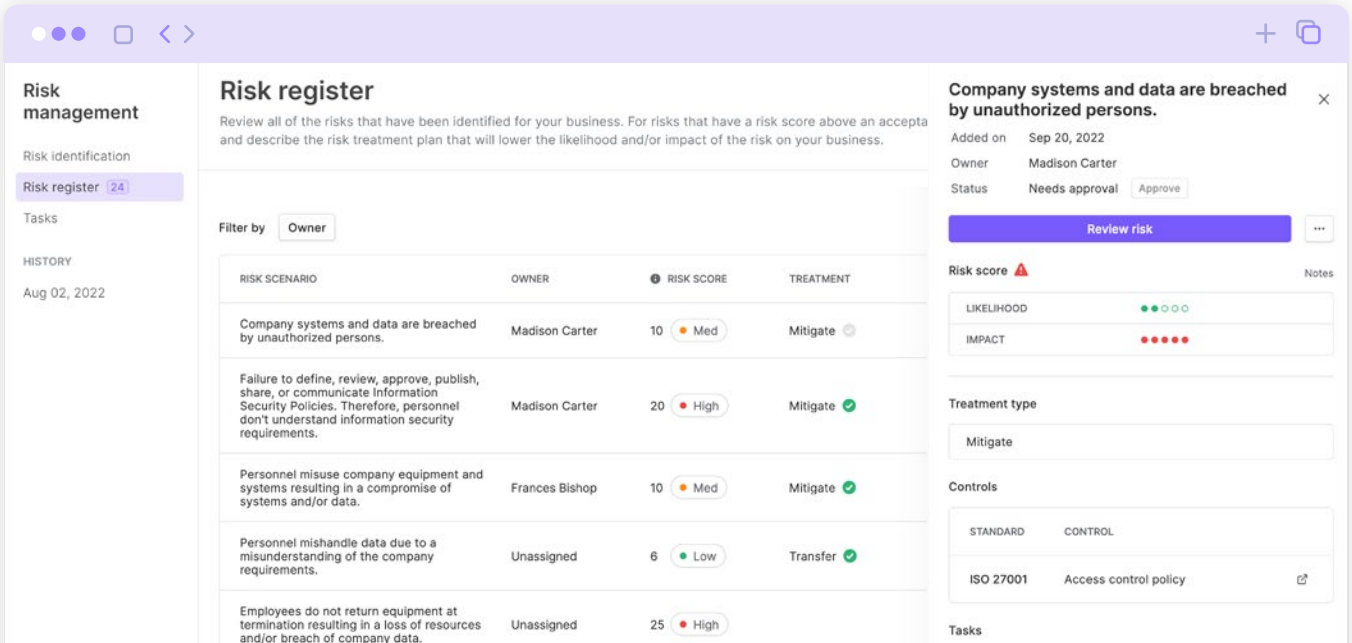
**As you review each risk in your Vanta view, you can then click into the next step — treating the risk. When you click into the “treat risk” tab for a risk, you’ll see four options:**

**01.** Accept the risk and do nothing because the likelihood and impact are so low that the benefits of taking action aren’t worth the time and effort it would require.

**02.** Transfer the risk outside the organization, such as by purchasing insurance or hiring a company to manage this risk or this aspect of your security.

**03.** Mitigate the risk by taking actions that make the risk less likely to occur, less impactful, or both.

**04.** Avoid the risk by eliminating it entirely, such as by disposing of the asset at risk or ending a program that opens the door for this risk.

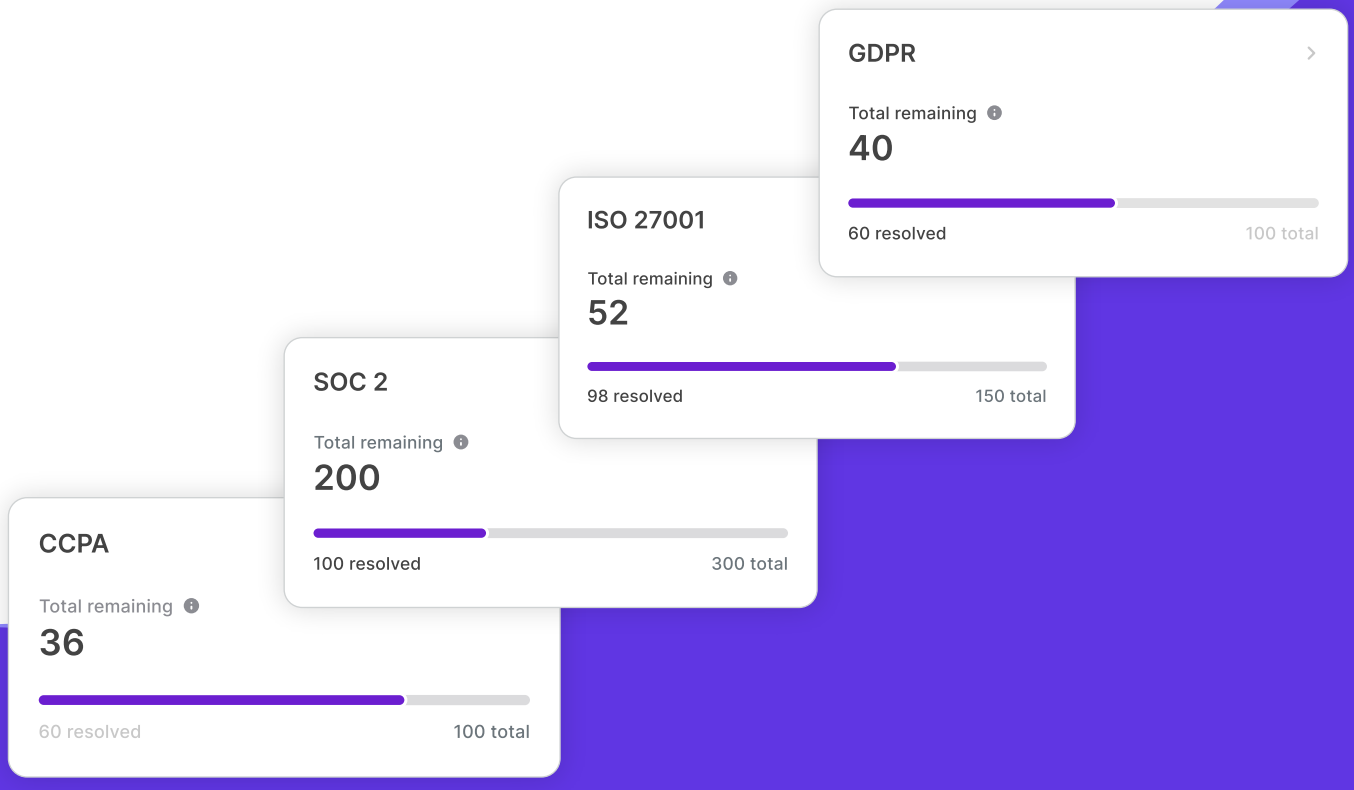


# Implementing treatment plans, tracking, and verifying progress

Now is the time to put all your planning into action. With Vanta's help, you have put together a detailed to-do list for minimizing and managing the risks for your organization. A treatment plan documents the actions to address each risk identified during the assessment process. Each risk will have a treatment plan. At this stage, your assigned risk owners begin addressing each risk one by one.

You can use the suggested controls and tasks as a guide. The assigned owner is responsible for either completing the tasks themselves or delegating and ensuring that the tasks are finished.

In Vanta, click to the next tab in the risk management feature: "Complete task." This breaks down the mitigation measures you selected into tasks and serves as a thorough task tracker where you can follow and document the progress of each task in your risk management. You can set and view due dates for each task, and each assigned owner can access this task tracker, as well to stay on top of their tasks. Moreover, you can automate task tracking and testing of control mitigation via integrations to ensure that your risk treatment plans are implemented.

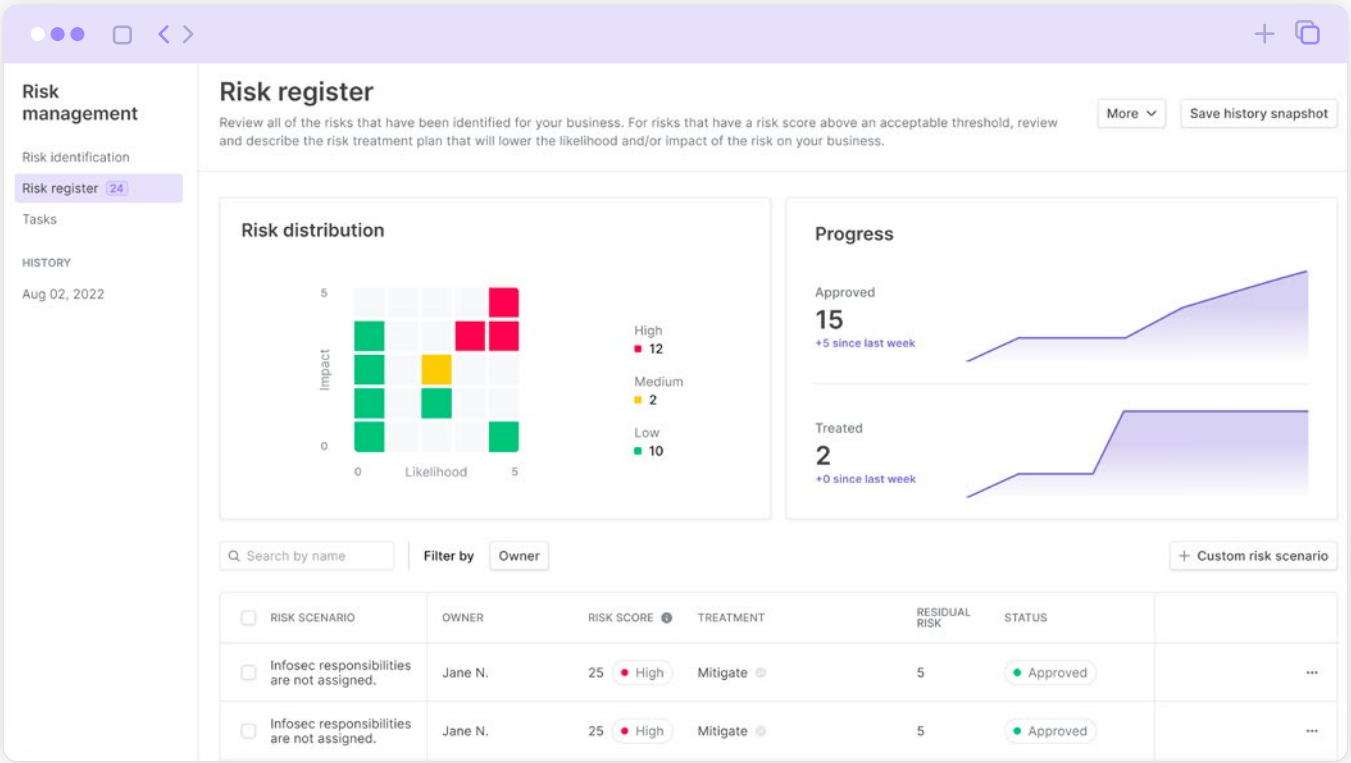


# Reporting and re-evaluating risks

As you're working through the legwork of completing all your risk mitigation and risk management tasks, Vanta makes it easy to create detailed yet readable risk assessment reports.

You can create snapshot reports of your risk management status on various dates to show your progress along the way. This snapshot capability also lets you share a specific version with your auditor when it comes time for a compliance audit. This way, your auditor can have all the information they need while you can continue working on optimizing your risk management.

These reports show everything your auditor needs, as well as everything your leadership team will want to know. They break down each identified risk with their overall risk scores, treatment selections, and residual risks along with the assigned owner.




By taking you through each of these five ISO-aligned stages, Vanta serves as your expert guide through your risk management program. With Vanta's continuous and automated security, the risk management process is not a single point in time, but an ongoing and customizable solution.

# How to take the next steps in your risk management

For so many professionals who are either new to risk assessment or have only performed risk assessment through manual and awkwardly fragmented processes, risk assessment seems like an infinitely difficult and complex endeavor. It doesn't have to be.

Vanta's intuitive workflow acts like a virtual coach that moves at your speed, guiding you through each step of the process on your timeline. With the help of our advanced solution, you can make your risk assessment both easier and more effective.

To learn more, contact the Vanta team to schedule a live demo. Our in-house team of experts will be able to show you around as you get started and answer any questions you have throughout your risk assessment work as well.

# 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 A DEMO

VANTA.COM