Vanta

Growing pains:
How to evolve and scale inherited security processes

Introduction

So you just joined a growing company as its first security hire (or one of a very few), and you find yourself working with a patchwork of security tools and policies already in place—some improvised and many undocumented.

Your first order of business? Bring clarity to the chaos by untangling what you've inherited, closing key gaps, and building a scalable, resilient security program that can keep up with your company's growth.

As your business expands, so do its risks and requirements, from more customer demands to growing security and compliance needs. But when you're buried in spreadsheets and managing workflows duct-taped together across siloed tools, it's hard to focus on long-term strategy, let alone scale.

This guide was built for security practitioners like you. It's a tactical playbook to help you assess what you've inherited, prioritize what matters, and evolve your security program into something stronger, streamlined, and future-proof.

How to know if you need to scale your security processes

Below are some challenges you may be facing that indicate it's time to update your organization's security processes:

You're bogged down by manual processes.

It's time to update your current workflows if you're spending most of your time on manual processes and repetitive work. If you use spreadsheets to manage your audits, risk assessments, vulnerabilities, and compliance monitoring, are reading through dozens of pages of SOC 2 and other compliance reports to get what you need, see a lot of errors in your results, or treat each security review as a one-off exercise, your processes may be preventing you from scaling.

You lack visibility into your growing tech stack.

The average organization has 291 SaaS applications in their tech stack. As your business grows, so does the number of tools your organization uses. It can be hard to discover and monitor them if you lack a centralized place to manage these systems and vendors. This can lead to painful workflows and inefficiencies, and increase your organization's risk if you're unable to see who has access to what and offboard appropriately.

You're outgrowing your current security tooling.

Your tools can either make managing your security program easier or they can make it a lot harder. If you're spending a lot of time managing your tools, copy and pasting from one system to another, and wishing you could automate your busy work, it's time for a change.

You're balancing meeting new expectations while struggling to keep the lights on.

The security team is a major stakeholder when it comes to scaling the business. You may be looking to deliver on new initiatives like adding additional compliance frameworks, establishing a bug bounty program, setting up new levels of encryption, or increasing your recurrence of vulnerability scanning and penetration testing. It's time to revisit your processes if you're struggling to find time to deliver on these new initiatives — while completing the security tasks you do on a regular basis.

Your cross-functional processes are filled with delays and bottlenecks.

Security teams heavily rely on their cross-functional partners to mitigate identified security vulnerabilities, provide visibility into new tools, and complete audit tasks. If you're running into delays or bottlenecks when working with these teams, you should update and co-create new workflows with them.

> "Our security process updates are driven by what the business needs from us. We continually adjust our program based on new initiatives. For example, we evaluate the security needs of customers as we expand to new markets and look into new attack vectors that might be present as we develop new products and adjust our program accordingly."
>
> **Vicky Levay, Sr. Director, Compliance, Risk, & Information Security**
> FloQast

5-step guide for updating your security processes

Now we'll walk through the five steps you should follow to update your security processes.

Step 1: Take inventory of your security tasks

The first step is to understand the current state of your security program. In this stage, you want to create a complete picture of your current tasks, processes, and workflows. Start by identifying all of the tasks on your plate. What tasks are you responsible for completing over a typical week, month, and year?

Consider these questions to help you get a clear picture of your current tasks and processes:

- What recurring tasks is your team responsible for?
- What cadence do these tasks need to be completed by?
- What tools and processes do you have in place to accomplish these tasks?
- What organizational risks do you need to manage and mitigate?
- What security and compliance frameworks can enhance your existing security processes?
- Which security tasks are performed ad-hoc without well-defined, documented processes?
- Which other teams are involved in the completion of these tasks?
- Which important security measures are missing from your current program?

Some example tasks include: Quarterly access reviews of applications and annual vendor security reviews for critical vendors.

> "Databook continuously updates our security processes. We start with an assessment of our current processes to identify gaps, redundancies, and pain points. This helps us prioritize areas needing improvement and map out an ideal future state to optimize efficiency."
>
> **Anne Simpson, Head of Privacy, Security, and Compliance, IT**
> Databook

ACTION: Track your tasks

- [ ] **Open this template and make a copy.**
- [ ] In the first column of the "Task Tracker" tab, list each security task you or your team are responsible for in a new row.
- [ ] For each task, input the following information in the corresponding row:

Cadence
How often the task is performed

Process
Any existing processes or documents about how the task is done

Stakeholders
Other teams who need to perform portions of the task to complete it

Task	Cadence	Process	Stakeholders
Vendor reviews	Every week	First we do X then Y then hand off to Z	HR, Legal
Risk monitoring	Daily	Link to process document	None
SOC 2 audit	Annually	No process	Dev team
Security training	Every 6 months	First we do X then Y then hand off to Z	HR, Legal
Risk mitigation	Every week	Link to process document	None
SSO implementation	Done only once	No process	Devteam, Design team
Policy reviews	Annually	First we do X then Y then hand off to Z	HR, Legal
Pen testing	Every 6 months	Link to process document	None
Compliance gap reviews	Every week	No process	Dev team
Access reviews	Daily	First we do X then Y then hand off to Z	HR, Legal
Budget planning	Annually	Link to process document	Dev team, HR, Legal, People team
Disaster recovery planning	Every 6 months	No process	Dev team
Backup verification	Twice a week	First we do X then Y then hand off to Z	HR, Legal
Phishing simulation	Every quarter	Link to process document	None

Step 2: Identify which processes need updating

Now you'll assess each of your processes and prioritize them. This step will help you identify which ones to transform and decide which to update first based on their potential impact. This impact will be determined by time saved, potential risk, and reduced cross-functional complexity.

Consider the following questions as you look at each task you've listed:

- How much time is spent on this task?
- How often is it repeated?
- How does this task impact your organization's risk?
- How would increasing the recurrence of a process impact your organization's security posture?
- How many other teams contribute to this task?

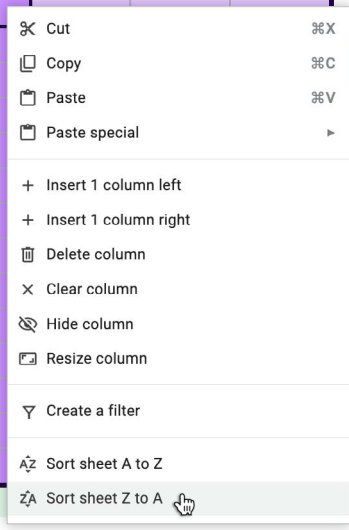
Use this scoring rubric to help guide your prioritization exercise:

Effort score How much time is spent on a task?	**1** Takes less than 30 minutes to complete	**2** Takes 1-2 hours to complete	**3** Takes several hours to complete	**4** Takes a full day (8 hrs) to complete	**5** Takes multiple days to complete
Cadence score How often is the task repeated?	**1** Performed only once	**2** Performed infrequently	**3** Performed 1-2 times a year	**4** Performed on a monthly basis	**5** Performed more than once a month
Risk score How does this task impact your organization's risk?	**1** Does not reduce risk	**2** Marginally reduces risk	**3** Moderately reduces risk	**4** Significantly reduces risk	**5** Critically reduces risk
Contributor score How many other teams contribute to this task?	**1** Does not require other teams to contribute to project	**2** Requires 1 external team to contribute toward part of project	**3** Requires 2-3 external teams to contribute toward part of project	**4** Requires 2-3 external teams to contribute toward major portions of project	**5** Requires 4 or more external teams to contribute toward major portions of project

ACTION: Score your security tasks

- [ ] Using the template you just created, give each of the tasks you listed a score based on the scoring rubric listed above.
- [ ] The sheet will calculate the average score for each of your security tasks.
- [ ] Right click on the column with the average score and sort from Z to A to see the tasks with the highest score listed first. Updating these tasks will have the biggest impact.
- [ ] With this score in mind, identify which tasks to update. Indicate which you will update and which you won't by using the dropdown in the "Update?" column.

Effort score	Cadence score	Risk score	Contributor score	Average score
1	5	3	1	2.5
5	3	4	2	3.5
4	3	5	3	3.75
3	5	1	1	2.5
5	1	2	4	3
4	4	3	3	3.5
4	3	4	1	3
1	5	5	2	3.25
2	5	1	4	3
2	3	2	5	3
3	3	3	2	2.75
2	5	4	3	3.5
4	4	5	1	3.5



Step 3: Make the needed changes

Now that you've identified which of your security processes to update, it's time to take action and improve them. Looking at the high-impact tasks you've identified, consider how you can centralize them, integrate them into existing workflows, and automate them.

Ask yourself the following questions:

→ **Can you make your security processes more centralized?**

- Can you group together similar tasks and workflows?
- Can you connect your tools and vendors to a centralized platform?
- Can you conduct your monitoring tasks all in one place?
- Can you create a centralized repository for your security documentation?

→ **Can you make your security processes more integrated?**

- Can you set up a template or process for repeated tasks?
- Can you pull information from your tool into a centralized view or report?
- Can you take action from the place where you monitor your risks?
- Can you set up workflows that notify collaborators in the tools they use?

→ **Can you automate any of your security processes?**

- Can you set up alerts and automatic reminders?
- Can you set up automatic SLAs and deadlines?
- Can you establish triggers and events that keep workflows moving?
- Can you eliminate your copy and paste tasks?

You'll likely need a trust management platform to help you centralize, integrate, and automate your security program. If you do not already have a platform to help you manage your security, find a platform that streamlines the process and workflows you identified as most impactful.

> "We centralized our security questionnaire function by implementing a database of common questions and answers. This has dramatically increased our speed and efficiency, improved our accuracy, and reduced follow-up questions. As a result, we've absorbed double the volume of questionnaires without adding headcount."
>
> **Vicky Levay, Sr. Director, Compliance, Risk, & Information Security**
> FloQast

ACTION: Find solutions

- [ ] Use the questions above to help you identify areas of opportunity within the security processes in your tracker. Are there any commonalities you notice? Are there steps that are repeated throughout multiple processes? Are there similar tasks that could be consolidated?
- [ ] Identify some of the top areas of opportunity for your current processes and create solutions. This will be unique based on how your organization is the setup of your organization and the tasks that you've identified as most impactful. Possible solutions could be creating a template for repeated tasks, onboarding to a platform that centralizes your security, or finding tools that enable you to automate the heavily-manual steps in your processes.
- [ ] Consider finding a platform that offers centralization, integration, and automation for a majority of the processes you've identified. This will enable you to streamline your program and limit the number of tools you use to manage your security.

Step 4: Influence your team to change

Next, align with your cross-functional stakeholders and co-create workflows with them. Your goal is to find a solution that's mutually beneficial and creates a better working model for both teams, enabling them to execute in their existing workflows and systems while moving projects forward.

Tailor your approach to the team you're collaborating with and the tasks you need to accomplish with them. For example, if you're talking to HR about hiring policies for SOC 2 compliance, make your communications relevant to their contributions, like bringing in quality candidates through background checks and creating appropriate policies for hiring. If you're talking to the dev team, explain how mitigating code errors in a timely manner protects the organization and how vulnerability management processes can reduce defect recurrence, saving them time and effort.

It's also important to share how this new process will benefit them. Some examples include preventing them from veering from their day-to-day processes, reducing last-minute requests, and more automation and alerts for deadlines, etc.

In your initial communications with these teams, get an understanding of their tools, processes, and pain points. Ask questions about how they manage their tasks, which systems they use, and how they stay on top of deadlines. Share your security processes with them and identify opportunities to integrate your workflows. Leverage the integration capabilities of your security platform to create automated workflows directly into the systems they use.

> "Communication and training is key when rolling out new processes. Create training programs and guides to educate staff on process changes. Do small pilot tests of new processes before rolling out organization-wide. And audit your new processes regularly to catch any post-implementation issues.
>
> **Anne Simpson, Head of Privacy, Security, and Compliance, IT**
> Databook

ACTION: Collaborate on new workflows

- [ ] Using the stakeholder column you filled out in your tracker, identify the teams you need to work with to co-create workflows for your security tasks.
- [ ] There may be multiple tasks associated with one cross-functional team. Collect all of the processes you identify per team so that you understand the full scope of your collaboration with each team. Note which portion of the task or process you need their help with.
- [ ] Discuss the following with the cross-functional teams you've identified:
  - The importance of these new workflows and how they're mutually beneficial.
  - Share the task or list of tasks you need their assistance with.
  - Ask questions about the way they manage their tasks, which systems they use, and how they stay on top of deadlines.
- [ ] In collaboration with this team, come up with a plan to update your cross-functional processes and determine the benefits of doing so. Here are some considerations:
  - How can you connect your processes with their existing workflows?
  - Is there a way to create automated alerts about new tasks assigned to their team?
  - Can you trigger security tasks to populate into their systems based on the cadence these tasks need to be done on?
- [ ] Create any templates, automations, or integrations necessary to execute on this plan.
- [ ] Establish a communication channel with this team for ongoing updates to the process or ad-hoc questions.

Step 5: Adapt as your organization grows

The final step is to monitor your processes, integrations, and automations over time to ensure they're scaling with your business. This step will be ongoing and done on a regular cadence.

Establish a reporting procedure and cadence that monitors the impact and value of your security program. Communicate the insights across your leadership and cross-functional teams. Monitor and improve the overall operations of your program and scale your processes as your organization grows.

ACTION: Establish reporting and review cadence

- [ ] In your security platform, set up a report that covers the most impactful metrics to your organization.
- [ ] Communicate these metrics to your leadership team to show the value of your security program on a regular cadence.
- [ ] Set up a quarterly or yearly task in your platform to review your security processes using this same method.
- [ ] Adapt your processes as needed based on your organization's new needs to ensure your security program is scaling as your business grows.

Scale your security with Vanta

Security leaders around the globe trust Vanta as a single solution to scale their security program with automations and integrations, centralize their efforts, and streamline their security reviews.

Centralize your security program
Use Vanta to bring together all of your siloed tools and systems and create a holistic view of your organization's risk.

Integrate your tools and workflows
Connect with security tools across your tech stack to surface risks and connect your workflows with Vanta's 300+ pre-built integrations.

Automate and take action
Get an end-to-end solution for managing your organization's security program where you can set up workflows, trigger alerts, and actions all in one place.

Leverage in-product tools and workflows
Complete risk assessments, access reviews, and vendor security assessments using Vanta's purpose-built platform.

Promote trust and reduce friction
Use Trust Centers to demonstrate your security posture and easily share key artifacts with customers and prospects.

Learn more about Vanta

Get a demo of the Vanta platform
See how you can build an automated, scalable security and compliance program with Vanta.

Request a demo ›

Register for an upcoming webinar
Every month we host webinars with updates about our products, innovations in the industry, and give you the opportunity to ask questions to our team.

View upcoming webinars ›

The State of Trust Report
We surveyed business and IT leaders globally to uncover the top trends in security and compliance. See what's shaping the future of trust in our report.

Download now ›

Vanta

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. Thousands of companies, including Atlassian, Chili Piper, Flo Health and Quora, 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