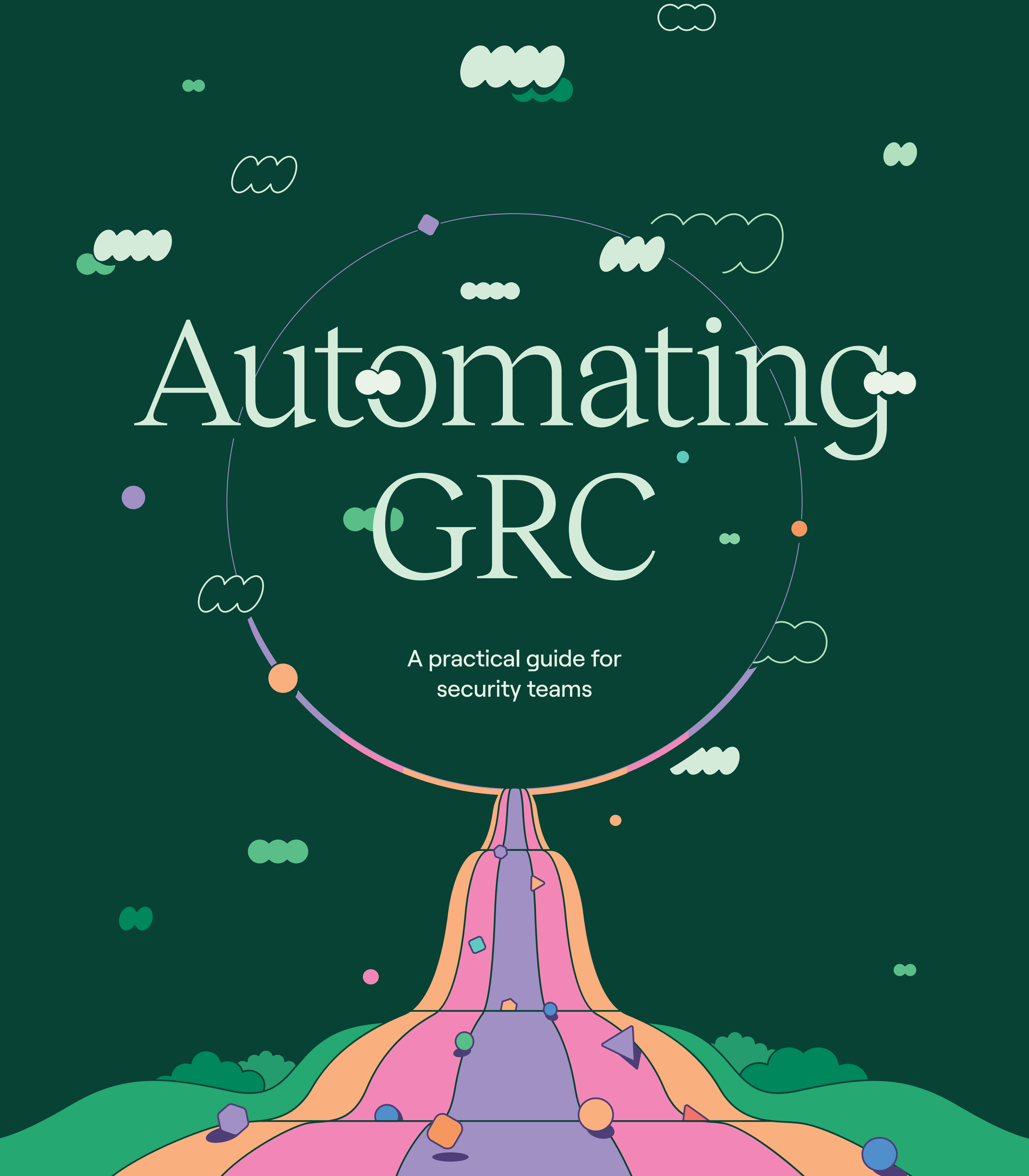
Essential Guide

Automating GRC

A practical guide for
security teams



Contents

Foreword
Matt Muller
Field CISO, Tines

With regulatory demands rising and security teams stretched thin, it's no surprise that many organizations are rethinking how they approach governance, risk, and compliance (GRC). Even well-resourced teams struggle to balance regulatory obligations with broader goals around improving security posture.

GRC isn't optional – it's foundational. It plays a critical role in identifying and managing enterprise risk and meeting regulatory demands. But the traditional approach is no longer fit for purpose. Too many teams are stuck with siloed systems and manual processes that can't scale to meet the complexity of modern enterprises.

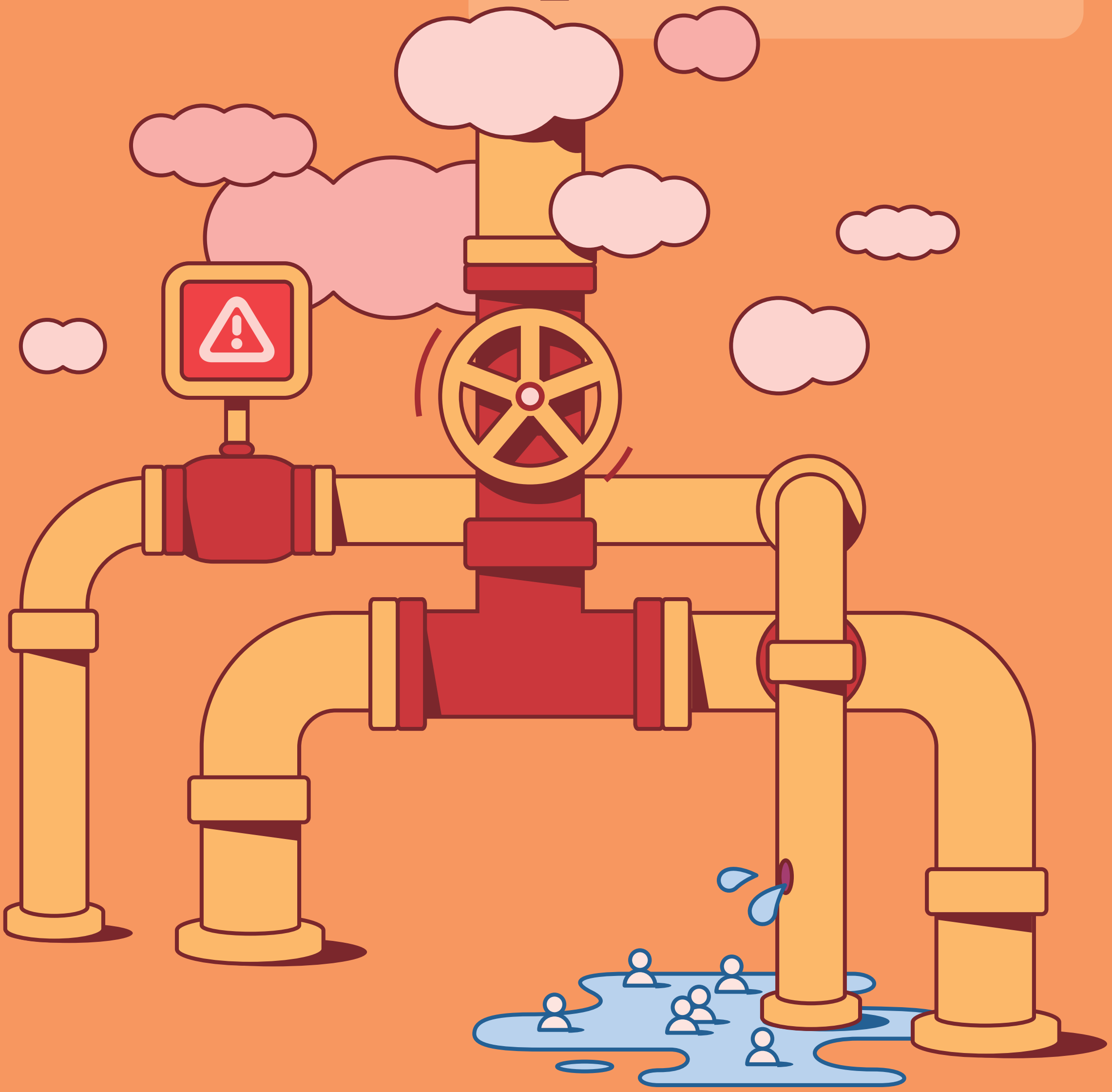
And it's only getting harder. Regulations are multiplying as governments race to catch up with cloud, AI, and emerging cyber threats. At the same time, threats are evolving. The attack surface is broader. Third-party dependencies are growing. And security teams are being asked to do more with less.

No wonder nearly half (46%) of security leaders say spiraling regulatory complexity keeps them up at night. Our research reveals nearly two-thirds (63%) of security practitioners and leaders are experiencing some level of burnout. The status quo simply isn't sustainable.

But there's a better way. A third of security leaders view compliance and reporting as a top-three challenge that could be solved with the right automation. By replacing fragmented, manual processes with unified, end-to-end workflows, teams can stay ahead of evolving standards and regulatory requirements – while reducing burnout and risk.

Done right, GRC is more than a requirement – it's a strategic advantage. According to Drata, 98% of organizations already view it as a business driver. With the right workflow orchestration and automation, GRC becomes a foundation for resilience, agility, and smarter security. This guide will help you move beyond checkbox compliance – and turn GRC into a source of strength.

The problem



Why GRC is harder than ever

GRC today is more complex, more visible, and more critical to get right – yet harder than ever to manage. As regulatory demands grow and cyber threats intensify, security and compliance teams are facing pressure on multiple fronts:

A shifting regulatory landscape

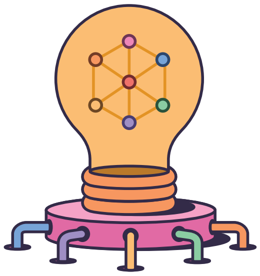
Nearly a third (30%) of organizations rank compliance as a top-three challenge, according to our Voice of the SOC research. Meanwhile, separate research from Drata showed nearly half (48%) of GRC teams struggle to keep pace with updates to existing frameworks – and identify areas requiring attention.

New legal jeopardy

Emerging regulations like Europe's NIS2 and DORA introduce personal liability for security leaders in the event of serious incidents. In the U.S., the SEC has also shown a growing willingness to bring charges against CISOs for GRC failures.

Data management and privacy concerns

Teams must ensure data accuracy, integrity, and security while complying with data protection and privacy laws like GDPR. That requires strong data classification, encryption, and access controls – often across siloed systems.



Mounting cyber threats and vulnerabilities

As digital transformation increases the size of the typical corporate attack surface, threat actors are ready to exploit this. According to one estimate, the total number of vulnerabilities discovered in 2024 rose 61% annually. Regular risk assessments and continuous monitoring are required to mitigate such risks.

Time and resource constraints

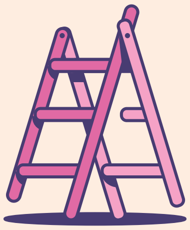
Limited staff and resources hamper your ability to keep GRC efforts effective and current. Over half (51%) of GRC leaders admit they are exhausted identifying and integrating new frameworks into GRC programs.

Siloed ownership

GRC requires cross-functional collaboration and alignment – but many teams still operate in silos. Legal, security, IT, and finance may have different priorities, or view compliance as a box-checking exercise rather than a strategic function. Shared visibility and ownership are essential.

Competing priorities

GRC doesn't exist in a vacuum. Security teams still need to deliver on broader goals – improving detection and response, managing vulnerabilities, or reducing tech debt. Without workflow orchestration and automation, GRC pulls resources from those critical initiatives.



"Part of what we suffer from is data silos – too many different systems that don't talk to each other. It's more of a checklist-based approach to security. Instead ask yourself: 'What threats am I trying to protect against? How do I put together a couple of well-architected platforms so that I can solve this problem end-to-end with the least amount of overhead, maintenance, and opportunity for error?'"

TRAVIS HOWERTON, CO-FOUNDER AND CEO OF REGSCALE

The opportunity

Workflow automation and orchestration

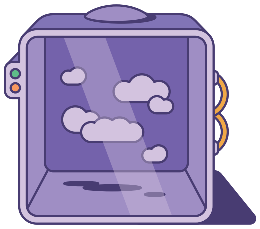
Manual processes and disconnected tools make GRC feel like a burden. But with the right workflows, security teams can automate manual tasks, orchestrate across systems, and turn GRC into a business enabler.

Here are four areas where GRC teams have leveraged orchestration and automation to make an immediate impact – with example workflows for each:

Streamline compliance processes

Routine tasks like evidence collection, policy management, and audit prep are repetitive and time-consuming. Automation handles the manual steps – data collection, analysis, reporting – so your team can move faster, reduce errors, and focus on strategic priorities.

→ Example: Automatically collect vulnerability or asset scan data from your security systems and upload it to your compliance dashboard – keeping data accurate and up to date without manual work.



Enhance risk management

Staying ahead of risk is difficult when signals are fragmented across tools, spreadsheets, and systems. Automation helps by aggregating data from internal sources, external databases, and threat intelligence feeds. With consistent, real-time scoring and analysis, teams can prioritize more effectively and mitigate risks sooner.

→ Example: Trigger a risk assessment when onboarding a new vendor, automatically calculate severity based on impact and likelihood, and log the results in a dynamic risk register.

Improve policy enforcement and monitoring

Enforcing policies and tracking employee compliance manually doesn't scale. Automation ensures policies are delivered on schedule, acknowledgments are tracked, and violations are flagged early. Alerts and notifications enable teams to respond quickly to compliance gaps before they escalate.

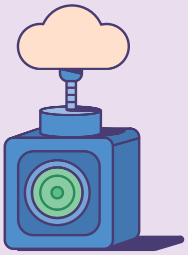
→ Example: Automatically monitor compliance across your environment, flag policy violations, and send reminders to ensure timely resolutions.

Accelerate audit processes

Audit season doesn't have to mean stress and scramble. Automated audit trails and reports give auditors comprehensive insight into controls, processes, and compliance status, helping teams complete audit cycles more efficiently and meet regulatory requirements.

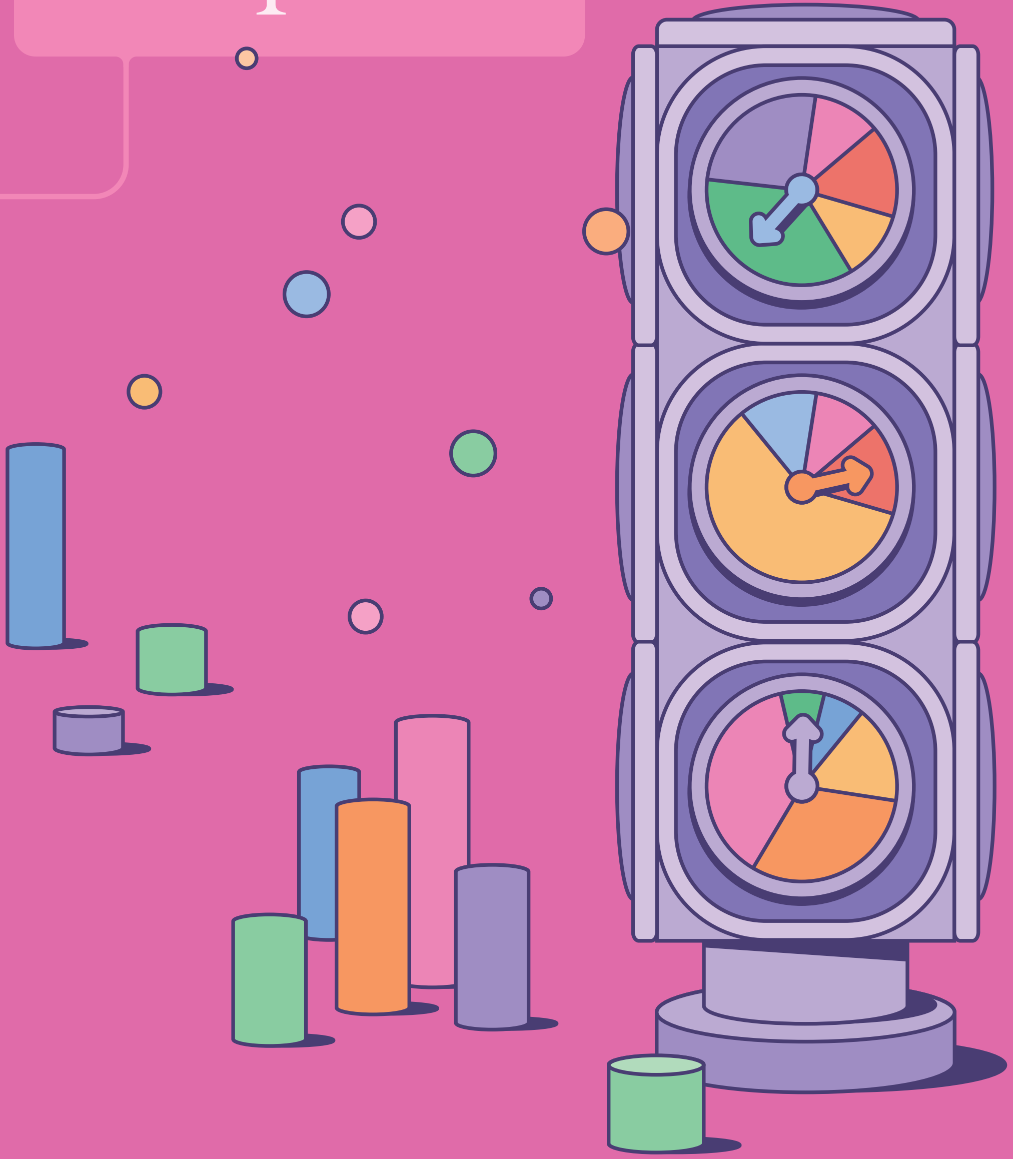
→ Example: Ingest audit logs on a schedule, store them securely for long-term retention, and ensure activity trails are always accessible for audits or internal reviews.

"I've never been able to get anyone excited about compliance... How we got people excited was by saying, 'Just don't do it anymore. Let automation do that for you. Lock down your systems. Focus on operational excellence in cyber. Let us give you all the risk and compliance checkboxes for free.'"



TRAVIS HOWERTON, CO-FOUNDER AND CEO OF REGSCALE

The impact

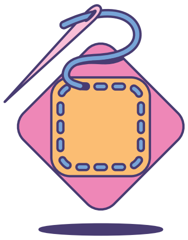


From bureaucracy to business enabler

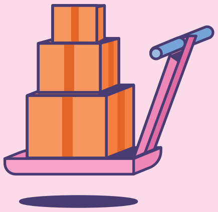
GRC used to be viewed as a cost of doing business – a checkbox to satisfy regulators and avoid fines. But that's changing. Today's executives increasingly see it as a strategic function that strengthens decision-making, increases accountability, and drives agility across the business.

By orchestrating and automating GRC workflows, your organization can:

- **Improve efficiency** by reducing duplication, automating manual tasks, and standardizing key processes.
- **Accelerate compliance** with fewer errors through continuous monitoring, automated reporting, and proactive gap remediation.
- **Reduce audit fatigue** by mapping internal controls to multiple regulatory frameworks.
- **Gain real-time visibility into controls** through dashboards, reporting, real-time alerts, and more.
- **Strengthen cross-team collaboration** and accountability by breaking down silos and creating shared ownership of risk and compliance.



- **Protect brand reputation** by building trust and preventing major breaches. Half (51%) of organizations report brand damage due to compliance failures.
- **Exceed compliance** by strengthening security beyond regulatory baselines. Almost half (49%) of organizations have suffered security/data breaches due to poor GRC, according to Drata.
- **Enable better decision-making** by surfacing timely, actionable insight on risk and other critical data.
- **Increase agility and resilience** by continuously identifying, assessing, and prioritizing risk, and adapting to regulatory changes.



“Compliance is a fundamental baseline for many organizations but doesn’t guarantee security. While there is some overlap, today’s security leaders must recognize the need to go beyond what compliance frameworks call for to achieve an extra layer of protection and peace of mind against potentially devastating breaches.”

BRANDON MAXWELL, HEAD OF IT OPERATIONS AND INFORMATION SECURITY AT TINES

What *good* looks like

All of this sounds great in theory, but what does it look like in practice? Some of the fastest-moving companies are using Tines to automate and orchestrate GRC. Here's how:

PathAI

Case study
Path AI

Automating onboarding and offboarding for compliance at scale

> "Before, no matter what, something would go wrong and break. Now, it's all automated. It's given me a source of truth to expand on and made us seem way more organized - honestly because we are. We just get to enter a form, and it's done!"

IT DEPARTMENT TEAM MEMBER, PATHAI

BEFORE TINES

- PathAI faced a high risk of non-compliance due to inconsistent, manual onboarding and offboarding processes.
- YAML + Python setup was fragile, error-prone, and lacked reporting or audit logs.

AFTER TINES

- Rapid, compliant onboarding and offboarding
- Improved repeatability and audibility
- Enhanced reporting and error logging
- Saved 45 minutes per onboarding request

Key workflow

PathAI replaced a fragile YAML + Python setup with a compliance-driven onboarding workflow built in Tines. The process starts with a Tines form behind SSO, validates the new hire, assigns the right access, logs actions in Jira, and creates audit-ready records. The same approach now powers offboarding – enabling scheduled access revocation across departments, even during mass layoffs or urgent exits.

→ Read the full case study: tines.com/case-studies/pathai druva

Case study
Druva

Scaling security operations with automation

> “To have workflows that stitch all our tools together, that became a force multiplier.”

ALLAN SWANEPOEL, PRINCIPAL SECURITY ARCHITECT, DRUVA

BEFORE TINES

- Druva’s security analysts were overwhelmed with manual tasks – ranging from Jira queries to compliance checks and data enrichment.
- Repetitive processes slowed innovation and made it hard to scale.

AFTER TINES

- Fully automated workflows
- Unified interface to manage detection and response
- Removed barriers to innovation, scalability, and compliance
- Saved 1–2 hours per analyst per week

Key workflow

Using Tines, Druva automated key workflows across vulnerability management, compliance, enrichment, and customer sales requests. Without relying on heavy engineering resources, the team automated Jira reporting, email alerts, security data enrichment, credential management, and API integrations – all from a single interface.

→ Find out more about how Druva is using Tines: tines.com/case-studies/druva tines

Case study
Tines at Tines

Achieving SOC 2 compliance in record time

> “We were able to pull all of this information together ourselves. Our engineers could continue with their regular operations – they weren’t even aware it was happening.”

BRANDON MAXWELL, HEAD OF IT OPERATIONS AND INFORMATION SECURITY, TINES

THE CHALLENGE

- Manual evidence collection and reporting for SOC 2 audits threatened to consume over 250 hours of IT and engineering time.

THE SOLUTION

- Automated evidence collection with Tines and Drata
- No engineering involvement required
- SOC 2 compliance achieved in just four months
- Saved 250+ hours of manual work

What we automated

The Tines team automated two high-effort audit areas:

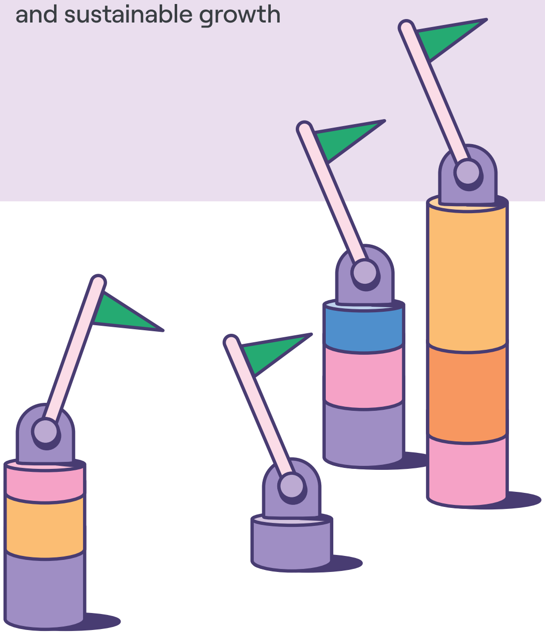
- Endpoint compliance evidence collection using Drata and Tines integrations—even without direct vendor support
- GitHub production change tracking, surfacing 7,000+ code merges in an organized, audit-ready format – without custom scripts or engineering effort

→ Find out more about how Tines used Tines to achieve SOC 2 compliance: tines.com/blog/soc-2/

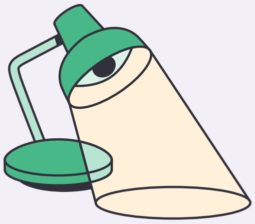
Ready to automate and orchestrate GRC? A checklist:

If you're ready to transform your GRC program through automation and orchestration, use this checklist to get started:

- Assess your current workflows and maturity to identify gaps, inefficiencies, and automation opportunities
- Set clear objectives to align stakeholders and tie efforts to business goals
- Choose tools that integrate easily with your existing stack to accelerate time to value
- Prioritize high-impact use cases for automation to prove value quickly and build momentum
- Build and test automated workflows to validate assumptions and refine processes early
- Collaborate across teams to reduce resistance, get buy-in, and ensure shared ownership
- Enable adoption from day one through clear communication, training, and support
- Monitor, iterate, and scale to drive continuous improvement and sustainable growth



Why security teams choose Tines for GRC automation



Reduces human error

By standardizing evidence collection and task execution, Tines minimizes the risk of mistakes like pulling the wrong data.

Improves visibility and trust

Tines makes it easier to confirm tasks are done correctly, increasing confidence across audits, teams, and stakeholders.

Accessible for the whole team

Anyone on your team can build and run workflows – no engineering support or custom scripting required.

Secure by design

Built by security practitioners, Tines helps every team operate with the highest standards of privacy and protection.

Designed for modern frameworks

Tines helps automate a wide range of compliance processes across frameworks like SOC 1, SOC 2, GDPR, CCPA, PCI, ISO 27001, NIST, and CIS/SANS controls.

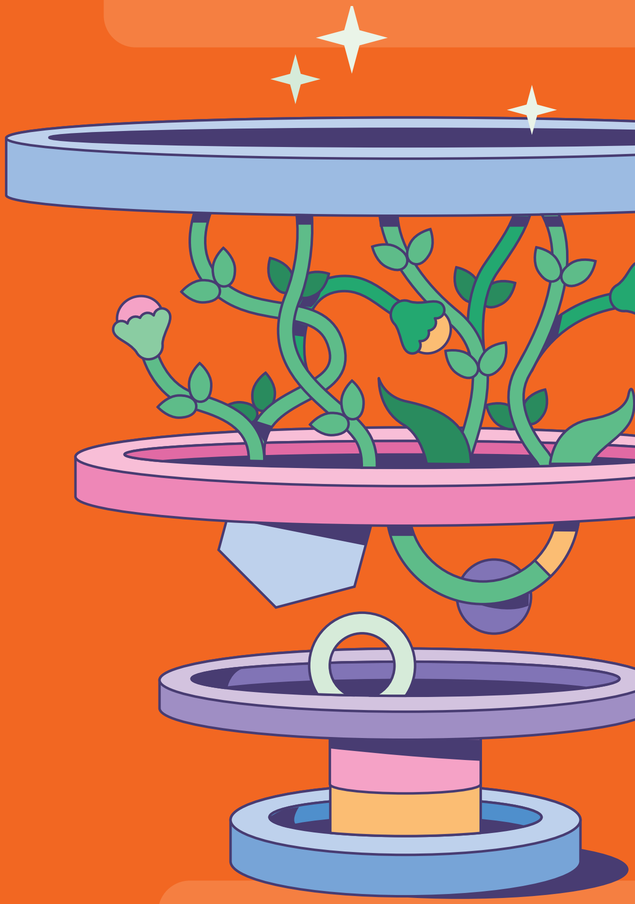
Connects the dots across your tech stack

Tines integrates with the tools you already use to embed GRC into your broader security automation strategy.

Simplifies compliance procedures

Automating manual GRC tasks with Tines saves time and resources, while ensuring a consistent, systematic approach.

Popular technologies and workflows



GRC tools commonly used with Tines

Tines connects to any tool with an API – but some tools are particularly popular for GRC:

Drata

Threat intelligence cloud platform enabling organizations to identify and mitigate threats across cyber, supply-chain, physical, and fraud domains.

→ Explore Tines' pre-built workflows for Drata

RegScale

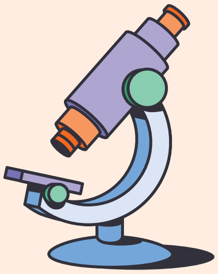
A modern compliance platform purpose-built for real-time compliance and continuous controls monitoring. Utilizing Tines with RegScale streamlines regulatory processes and enhances operational efficiency.

→ Explore Tines' pre-built workflows for RegScale

Vanta

A leading automated security and compliance platform that helps companies achieve and maintain compliance standards. Leveraging Tines with Vanta streamlines security workflows, enhances threat detection, and ensures continuous audit readiness.

→ Explore Tines' pre-built workflows for Vanta



Pre-built workflows

The Tines Library offers over 1,000 pre-built workflows with over 60 built to suit your unique GRC requirements. These stories help teams automate common tasks like:

Send automated reminders for employee training

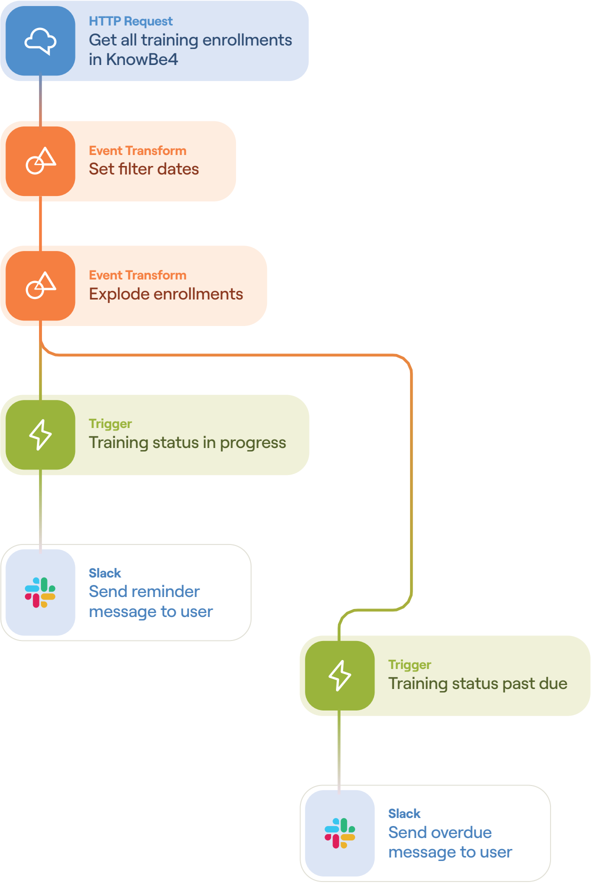
Automatically check for overdue or upcoming security training and send reminders on a schedule that works for your team. Choose daily, weekly, or any cadence you need.

TOOLS

KnowBe4, Slack

USE THIS FLOW

tines.com/zqrsl



HTTP Request
Get all training enrollments in KnowBe4

Event Transform
Set filter dates

Event Transform
Explode enrollments

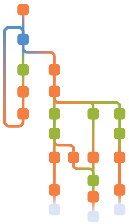
Trigger
Training status in progress

Slack
Send reminder message to user

Trigger
Training status past due

Slack
Send overdue message to user

FULL WORKFLOW MAP



Run asset vulnerability scans & add evidence to compliance system

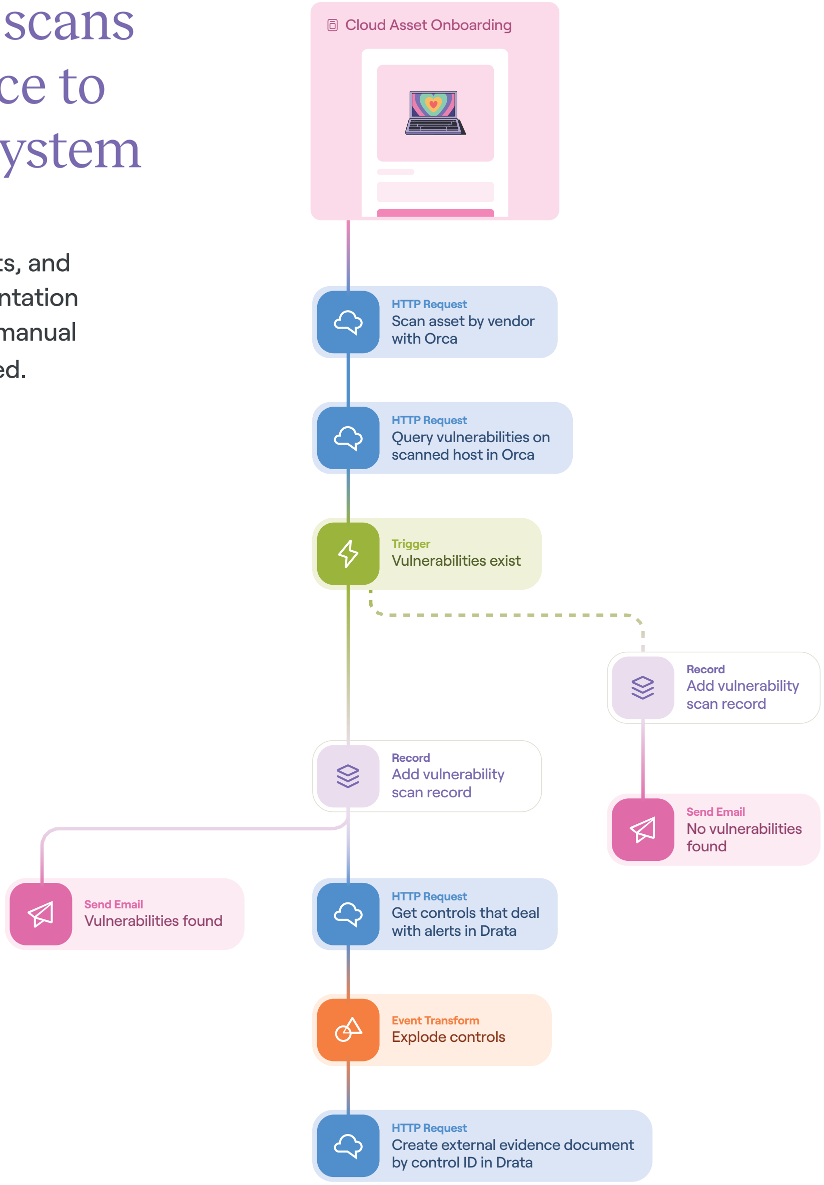
Trigger scans, collect results, and upload supporting documentation to platforms like Drata. No manual steps or extra logins required.

TOOLS

Drata, Orca Security

USE THIS FLOW

tines.com/zplga



Cloud Asset Onboarding

HTTP Request
Scan asset by vendor with Orca

HTTP Request
Query vulnerabilities on scanned host in Orca

Trigger
Vulnerabilities exist

Record
Add vulnerability scan record

Send Email
No vulnerabilities found

Record
Add vulnerability scan record

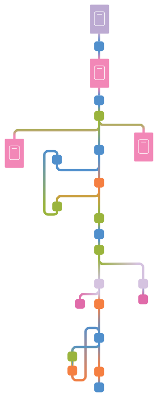
Send Email
Vulnerabilities found

HTTP Request
Get controls that deal with alerts in Drata

Event Transform
Explode controls

HTTP Request
Create external evidence document by control ID in Drata

FULL WORKFLOW MAP



→ Test drive the **full library** for free by signing up today for **Tines Community Edition.**

Getting started

As digital transformation accelerates, regulatory complexity is becoming a major obstacle. Over **77% of global organizations** say compliance challenges have negatively impacted them – and in 2024 alone, more than 1.3 billion breach notifications were issued in the US.

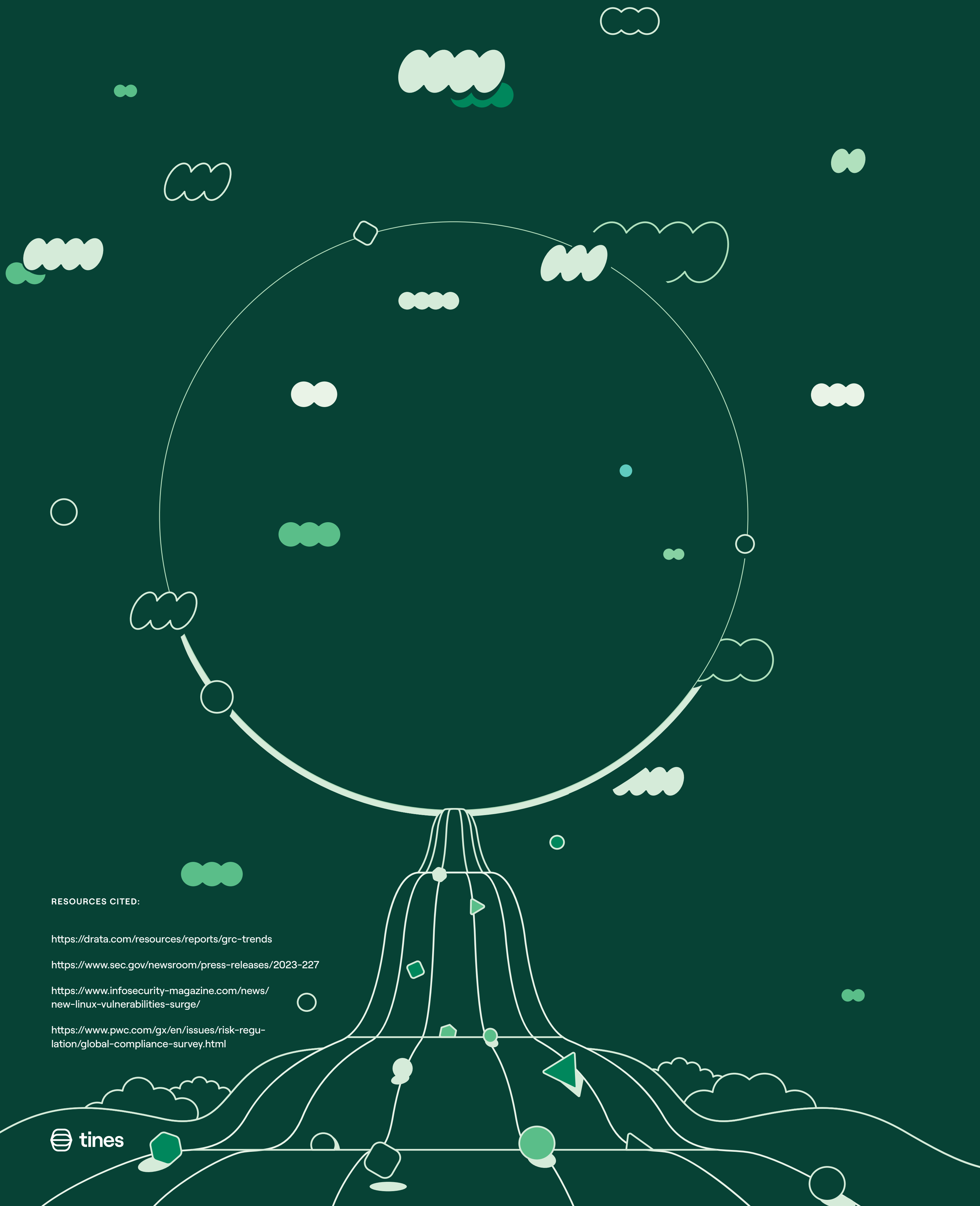
Despite the high stakes, most GRC programs still lag behind. Fewer than two in five organizations consider theirs close to maturity.

Tines offers a better way forward. By orchestrating and automating manual processes, security teams can strengthen risk management, streamline compliance, and free up time for higher-impact work – all without burning out your team or adding headcount.

Whether you're building from scratch or scaling what's already working, Tines helps you move faster, stay compliant, and reduce risk.

→ Sign up for the always-free Community Edition of Tines: **tines.com/community-edition**

→ Learn more about Tines for GRC: **tines.com/solutions/security/governance-risk-and-compliance**



RESOURCES CITED:

https://drata.com/resources/reports/grc-trends

https://www.sec.gov/newsroom/press-releases/2023-227

https://www.infosecurity-magazine.com/news/new-linux-vulnerabilities-surge/

https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html

tines