

# Features

Onboarding (Quick Start)

Dashboard

Audit Center / Task

Compliance (Framework / Controls / Policies / Evidence/ Audit)

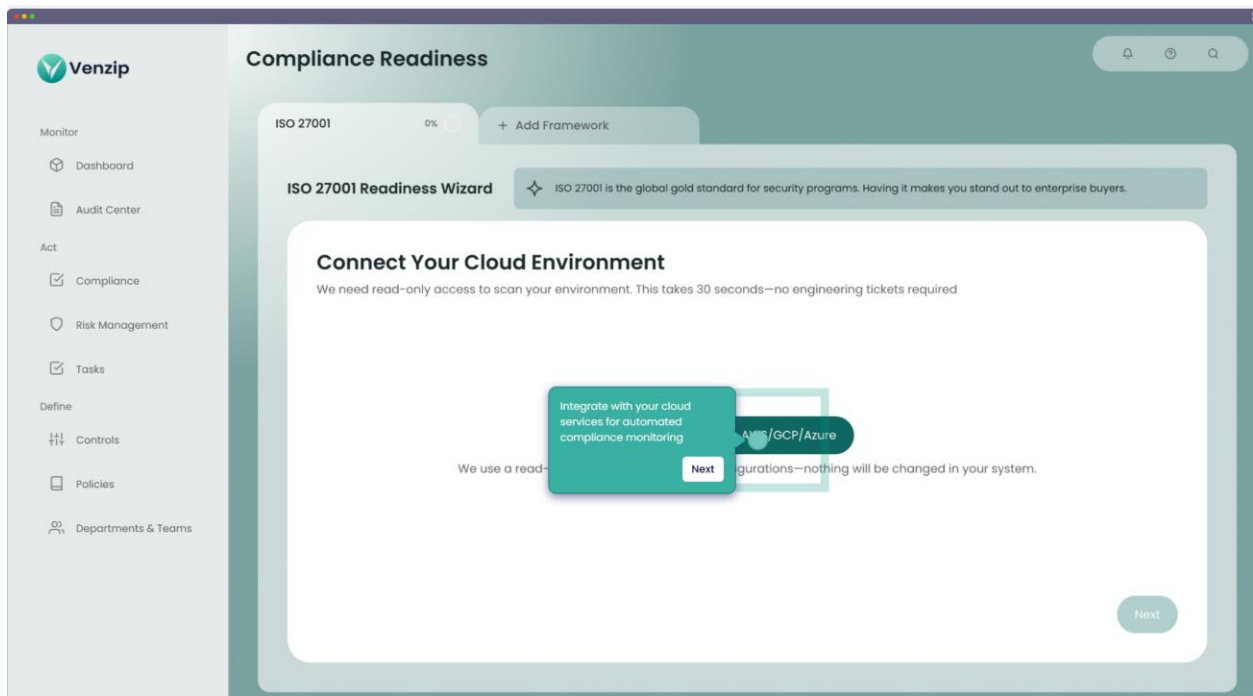
Risk Management

Automation (API Integrations / Test/ Automation etc)

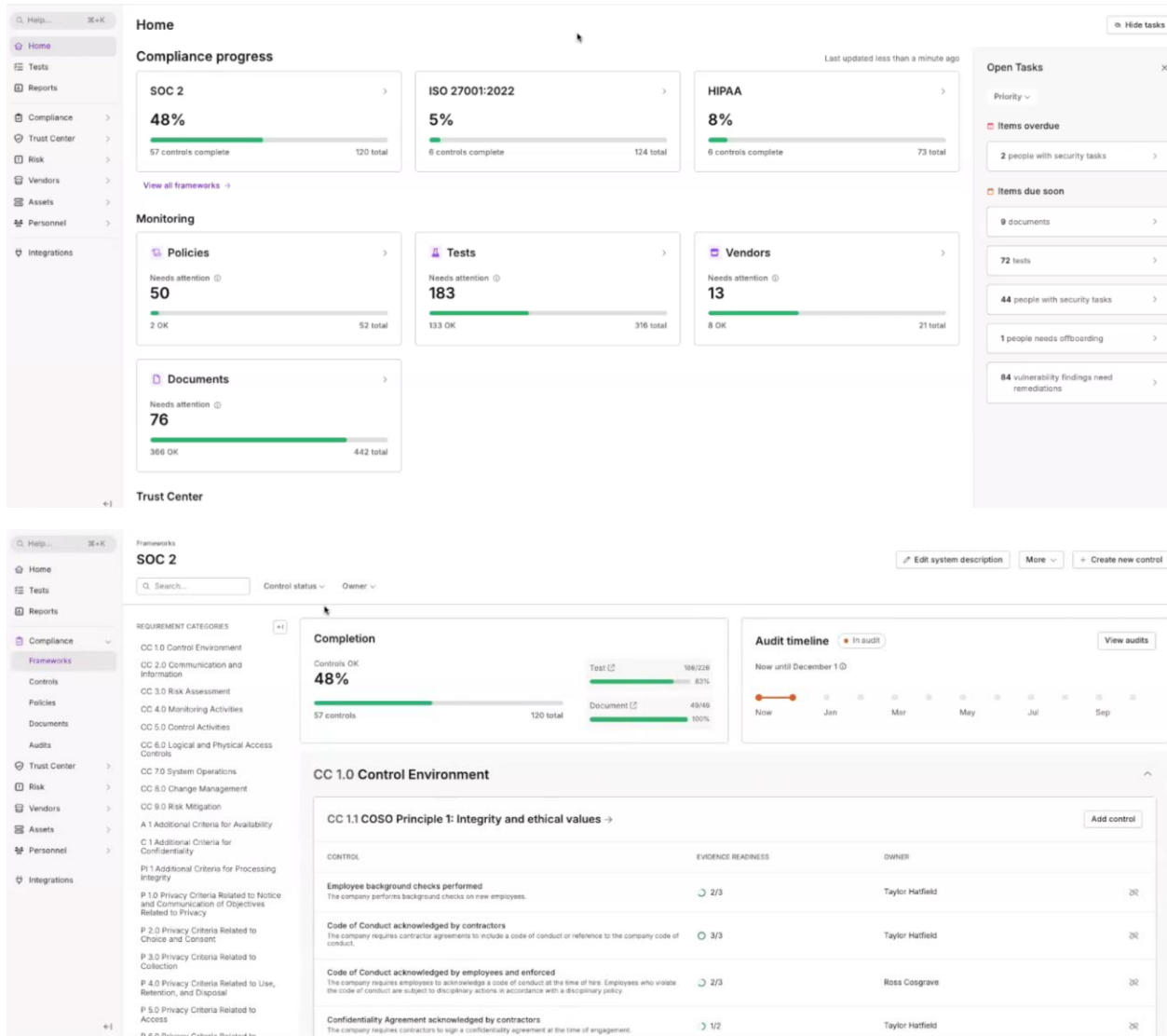
## Sample System Walkthrough – Watch Demo from 12 mins

[cdn.embedly.com/widgets/media.html?src=https%3A%2F%2Fplayer.vimeo.com%2Fvideo%2F1027480289%3Fh%3D0476f32983%26app\\_id%3D122963&dntp=1&display\\_name=Vimeo&url=https%3A%2F%2Fvimeo.com%2F1027480289%2F0476f32983&image=https%3A%2F%2Fi.vimeocdn.com%2Fvideo%2F1947459476-9d10791cc381a56bf7da6e2b5fd2dc5cef4b0afc5af2e9605e265dac829b87a8-d\\_1280&key=96f1f04c5f4143bcb0f2e68c87d65feb&type=text%2Fhtml&schema=vimeo](https://cdn.embedly.com/widgets/media.html?src=https%3A%2F%2Fplayer.vimeo.com%2Fvideo%2F1027480289%3Fh%3D0476f32983%26app_id%3D122963&dntp=1&display_name=Vimeo&url=https%3A%2F%2Fvimeo.com%2F1027480289%2F0476f32983&image=https%3A%2F%2Fi.vimeocdn.com%2Fvideo%2F1947459476-9d10791cc381a56bf7da6e2b5fd2dc5cef4b0afc5af2e9605e265dac829b87a8-d_1280&key=96f1f04c5f4143bcb0f2e68c87d65feb&type=text%2Fhtml&schema=vimeo)

## Layout Samples



# Dashboard



## Onboarding?

Quick Start – attached details / info questions separately

DRATA

SettingsConnections

100%100%

Data Ventures P...

DashboardTasks

COMPLIANCEControlsFrameworksMonitoringEvent TrackingEvidence LibraryAudit Hub

TRUSTTrust Center

RISKRisk ManagementVendorsAssetsVulnerabilities

Connections

Andreas Van N...

All ConnectionsActive connectionsAvailable connectionsSearch connections

Types

Automation Tools

Background Checks

Codebase

Communication

CSPM

Custom

Customer Relation Management

Cyber Insurance

Digital Signature

EDR

Enterprise Single Sign-On

External Policy Management

HRIS

Identity

Infrastructure

MDM

AUTOMATION TOOLS

Set up an automation tool to build your own workflow.

Swift

Set up

Times

Set up

Torg

Set up

Tray.io

Set up

BACKGROUND CHECKS

LIMIT OF 1 CONNECTION

Connecting your background check provider to Drata allows for new hires to conduct their background checks via Drata's onboarding at a preferred partner rate, and to automatically pull in background checks conducted outside of Drata.

Okta

Connect

OneLogin

Connect

Observability

Security Reviews

Security Training

Ticketing

User Access Review

Version Control

DRATA

Quick Start

100%100%

Data Ventures P...

DashboardTasks

COMPLIANCEControlsFrameworksMonitoringEvent TrackingEvidence LibraryAudit Hub

TRUSTTrust Center

RISKRisk ManagementVendorsAssetsVulnerabilities

Connections

Andreas Van N...

Provide Basic Info

Share basic details about your company.

1/1 completed

Enter your company info

Enter basic info about your company to satisfy common compliance requirements.

Enter detailsCompleted

Make connections to power automation

Set up connections to continuously monitor controls, collect evidence and more.

4/4 completed

Establish continuous compliance for your frameworks

Review framework requirements and work with your team to establish continuous compliance.

3/3 completed

Ensure your personnel stays compliant

Set up and review your personnel security procedures to establish compliance.

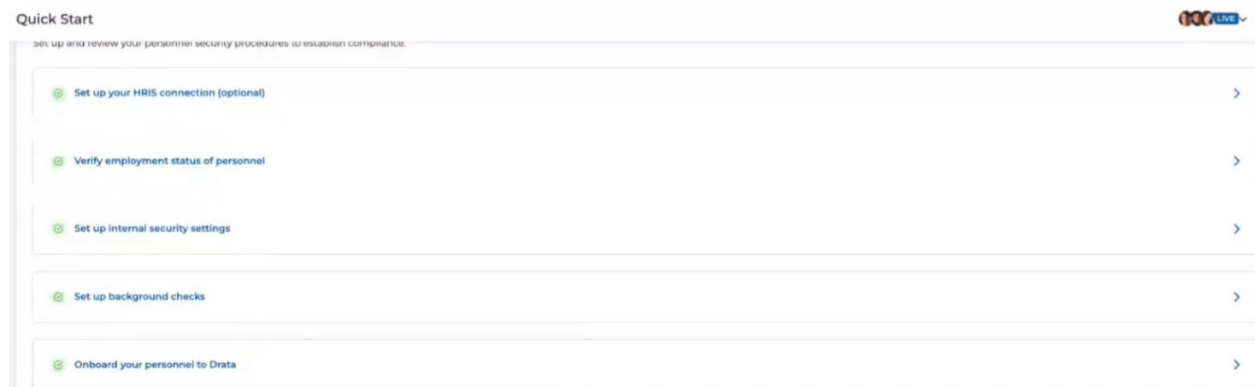
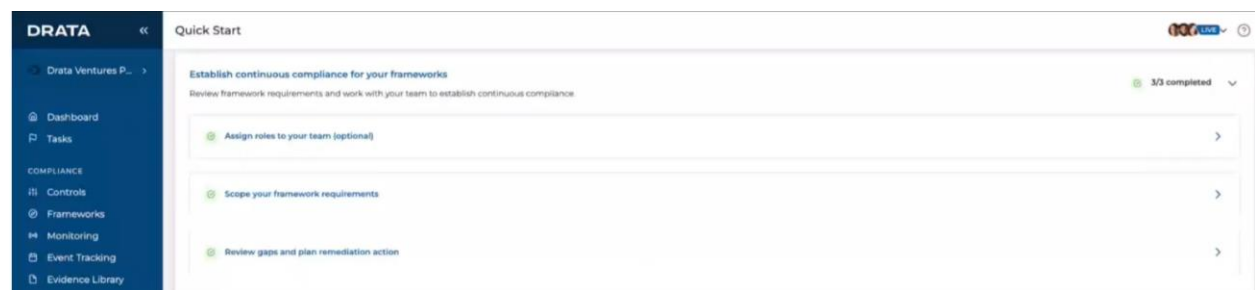
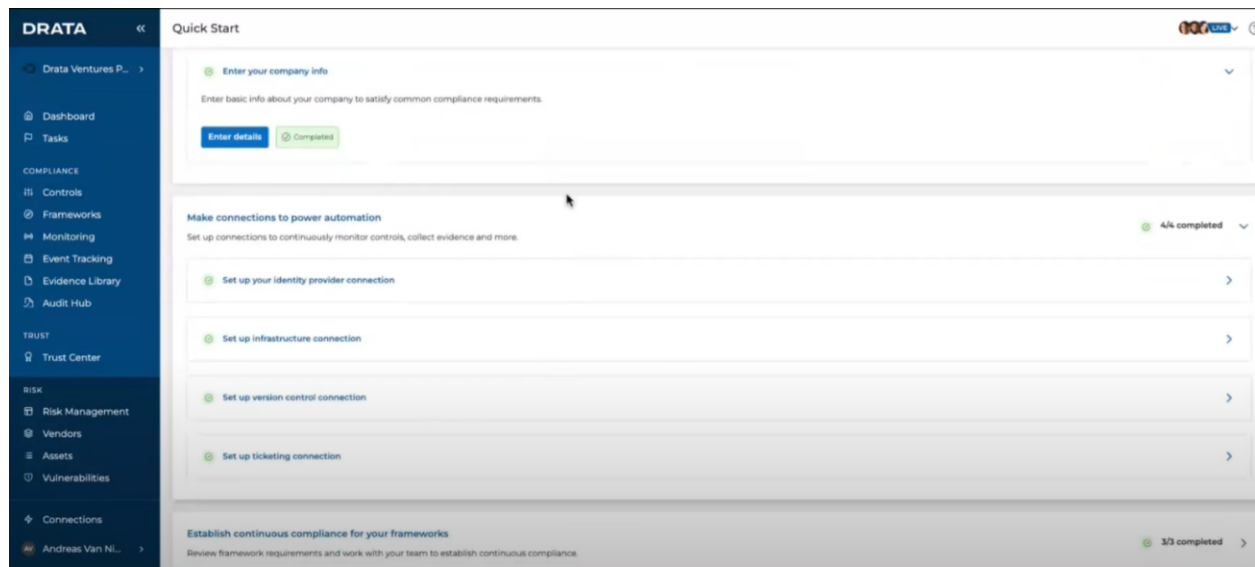
5/5 completed

Set up your policies

Create policies using our templates or import existing ones that fit your organization's needs.

39/44 completed

What's next



## Frameworks

ISO27001 , HIPPA, SOC 2, GDPR and Vendor Risk Management

Priority

- ISO27001
- SOC 2
- Vendor Risk Management

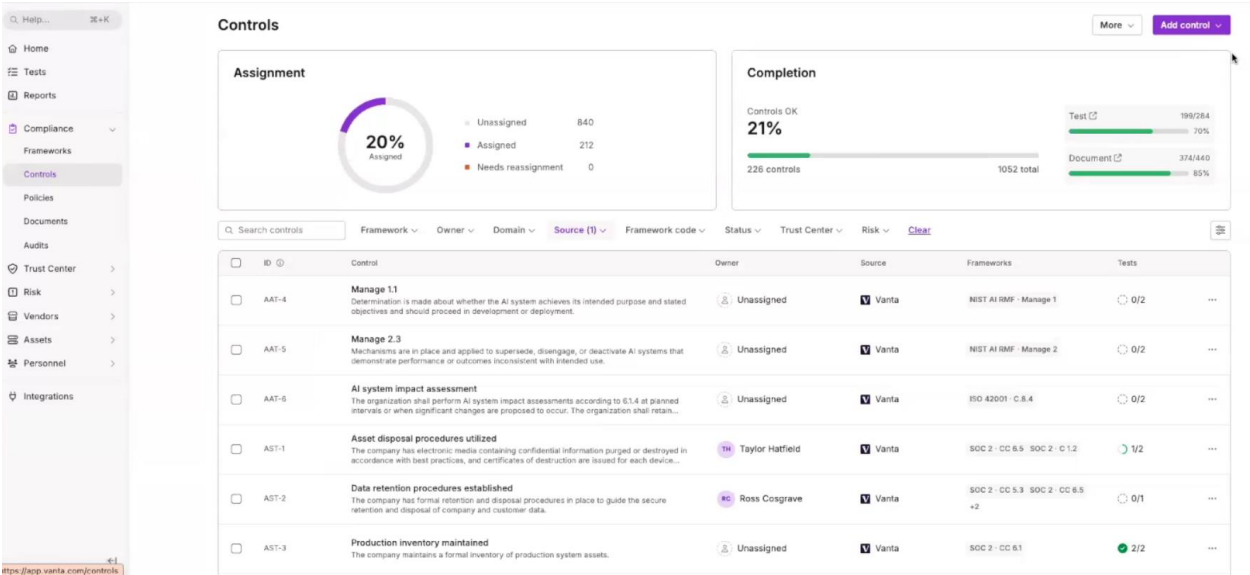
Compliance progress

Last updated less than a minute ago

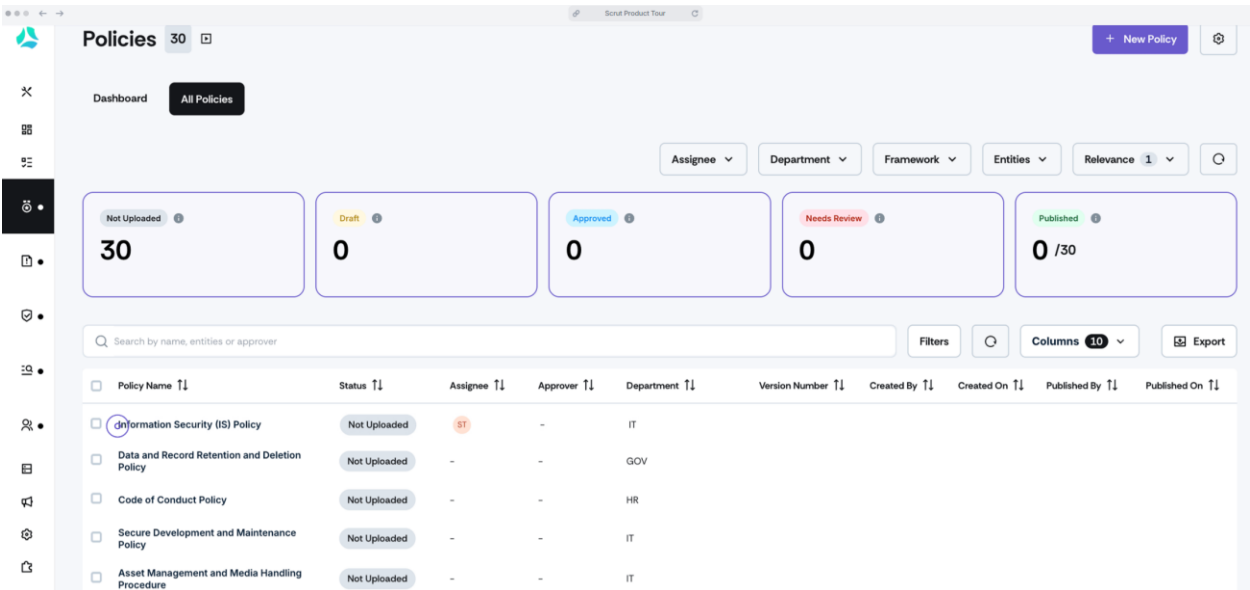


[View all frameworks →](#)

Controls



Policies



## Policy / Control Templates

**Goal:** Start strong with vetted policies mapped to controls.

1. Library Curation
  - Provide versioned, legally reviewed templates (InfoSec, Access, BYOD, SDLC, BCP/DR, Incident, Vendor, Privacy).
2. Parameterization
  - Variables (company, roles, RTO/RPO, data classes); guided Q&A to tailor.
3. Cross-Mapping
  - Each clause maps to control IDs across frameworks (SOC 2, ISO, HIPAA, PCI, GDPR, ISO 42001).
4. Review & Approval
  - Redline workflow, legal/privacy review, e-sign, publication date & next review date.
5. Attestations & Training
  - Collect employee attestations; assign training modules; track completion.

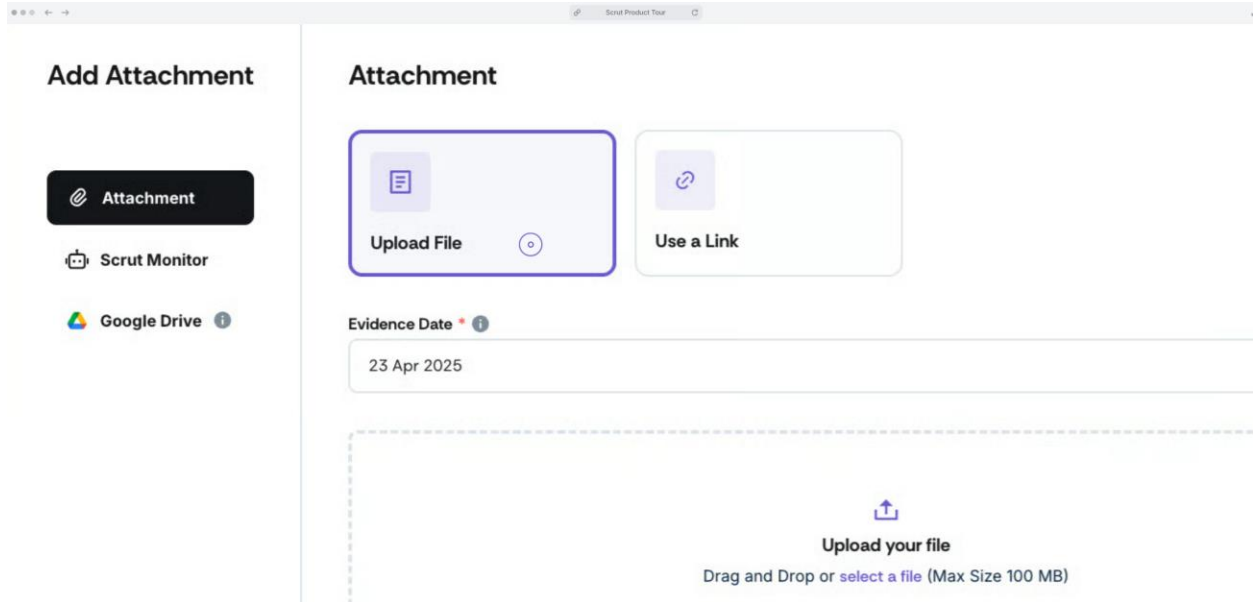
**Automations:** Renewal reminders, change-impact analysis (which controls evidence needs updating when a policy changes).

**Audit-Ready DoD:** All required policies approved, published, and attested; mappings visible; reviews current.

## Evidence tab

The screenshot displays the 'Evidence Tasks' dashboard. At the top, there's a header with 'Evidence Tasks' and a count of '50'. A sidebar on the left contains navigation icons. The main area features a dashboard with four status-based cards: 'Not Uploaded' (44), 'Draft' (0), 'Needs Attention' (0), and 'Uploaded' (6/50). Below these cards is a search bar and a table of evidence items. The table has columns for 'Evidence Name', 'Status', 'Assignee', and 'Department'. The first four items are 'Not Uploaded', and the last one is 'Uploaded'.

| Evidence Name   | Status       | Assignee | Department |
|---|--------------|----------|------------|
| Business Continuity Plan and Disaster recovery plan - Testing Results | Not Uploaded | G        | IT         |
| Code Review Results and Action Items                                  | Not Uploaded | G        | IT         |
| Documented Asset Inventory and Review Dates                           | Not Uploaded | G        | IT         |
| Documented Organizational Chart with Reporting Lines                  | Not Uploaded | G        | HR         |
| Enabled Multi-Factor Authentication                                   | Uploaded     | G        | IT         |



## Evidence Collection & Documentation

**Goal:** Gather, version, and prove controls with trustworthy artifacts.

1. Evidence Model
  - Define types (policy, log, screenshot, config export, code scan, attestation), retention, and freshness rules.
2. Evidence Requests
  - Per control, auto-create requests with examples & redaction tips; map to owners.
3. Integrations & Pulls
  - Connect cloud, CI/CD, ticketing, IdP, scanners; pull evidence on schedule.
4. Manual Uploads & Attestations
  - Drag-and-drop with guidance; templated attestations (e.g., quarterly access reviews).
5. Versioning & Chain of Custody
  - Immutable versions, timestamps, collector identity, hash; link evidence → control(s).
6. Quality Gates
  - Automated checks (date freshness, file type, redaction, control fit).
  - Human QA for narratives and diagrams.
7. System Description & Narratives
  - Generate/edit system description, data flows (DPIA where needed), policies, and SoA (ISO).

## 8. Auditor Package

- One-click export by control, with evidence index and narratives.

**Automations:** Scheduled collectors, freshness alerts, “evidence completeness” meters, auto-indexing by control.

**Audit-Ready DoD:** All required evidence present, fresh, QA-passed; system description and narratives finalized; export validated.

## API Integrations

The screenshot displays the 'Integrations Library' interface. On the left, a sidebar lists categories: Cloud Providers, Identity Providers, Version Control, Project Management Platforms, Human Resource Information Systems, Background Check, Mobile Device Management Tools, Policy Management, Threat Intelligence, Vulnerability Scanners, Miscellaneous, Web Security & CDN, and Capacity & Usage. The main area is divided into two sections: 'Cloud Providers' and 'Identity Providers'. Under 'Cloud Providers', there are cards for Amazon Web Services, Microsoft Azure, Google Cloud, Digital Ocean, Heroku, and Vercel. Each card shows 'Automated Evidence' and 'Access Review' status, along with an 'Integrate' button. Under 'Identity Providers', there are cards for Google Workspace, Microsoft Entra (Azure AD), and Okta (IDP). A search bar at the top right allows searching by name.

The bottom part of the image shows a detailed view of the 'Integrations' page. It includes a 'Description' section for the AWS integration, stating: 'The AWS integration allows Scrut to monitor IAM policies, user roles, and cloud resource configurations. It tracks privileged users, validates secure configurations for critical resources, and ensures compliance with cloud security best practices.' Below this, the 'Scopes and Permissions Required' section lists: 'Read Only Access: Permissions to retrieve cloud resource details, including inventory of services like S3 buckets, EC2 instances, and RDS databases.' and 'Security Audit: Permissions to access audit logs and security configurations, including IAM policies, user roles, and security findings from AWS services like Security Hub and GuardDuty.' At the bottom, there are three expandable sections: 'Automated Tests' (153), 'Automated Controls' (94), and 'Automated Evidences via Scrut Monitor' (20).

## Integrations



**Goal:** Pull the right evidence & signals automatically.

1. System Discovery

- Guided catalog: cloud accounts, IdP, code repos, ticketing, SIEM, EDR, HRIS, MDM, vulnerability scanners.

2. Connector Setup

- OAuth/service accounts; least-privilege scopes; secrets in vault.

3. Data Mapping

- Normalize into a common schema (assets, users, configs, events, findings).

4. Sync Policies

- Set frequencies, backfill windows, retention, masking rules.

5. Health & DQ

- Connector health dashboard, retries, lag alerts, sample-based validation.

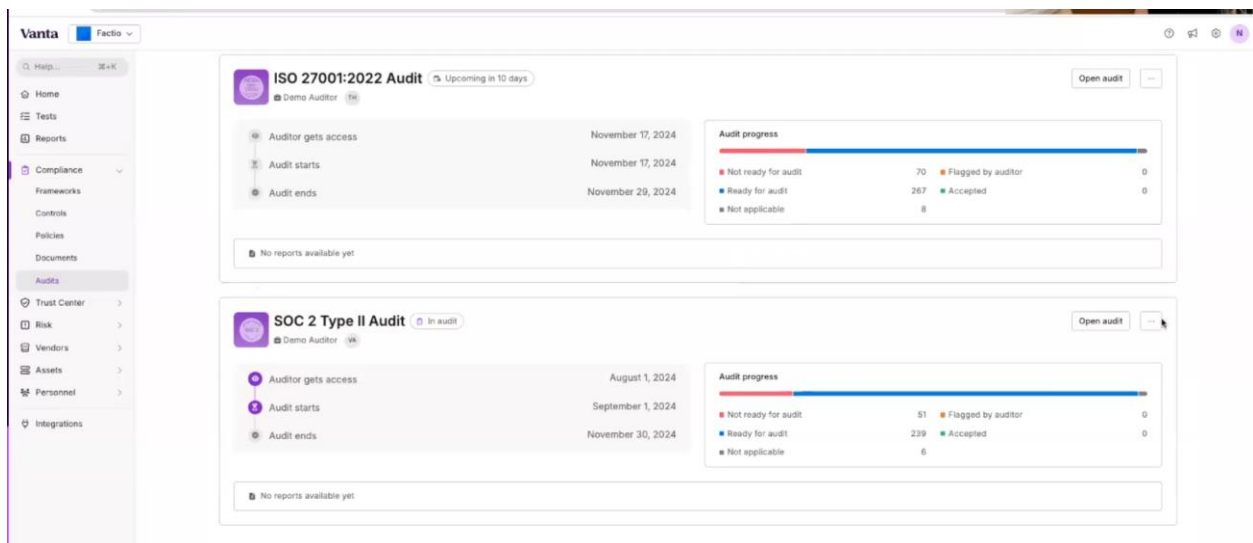
6. Sandbox→Prod

- Test connectors before production; change control for scopes/permissions.

**Automations:** Auto-suggest connectors based on selected controls; connector-health alerts.

**Audit-Ready DoD:** All mandatory connectors healthy; data freshness within SLA; least-privilege reviewed.

## Audit Centre



Scrut Automation

Compliance

Frameworks

Controls

Policies

Evidence Tasks

Cloud

Vault

Risk

Trust

Audit

Audit Center

Corrective Action

People

SOC 2 Audit

Mark Audit Complete

Export Audit Report

Owner: Gautam

Audit Date: 1 Oct 2025

Audit Type: External

Status: In Progress

Audit Team: A

Framework: SOC 2

Entities: Organization Wide

Observation Period: 1 Sept 2025-1 Oct 2025

Audit Readiness: 98%

Policies: 97%

Automated Tests: 100%

Evidences: 100%

Requirements

Controls

Requests

Findings

Corrective Actions

Audit logs

Search by finding name, audit name

Filters

Create Findings

Export

Columns

| Finding Name        | Assignee | Nature of Findings | Actions |
|---------------------|----------|--------------------|---------|
| Code Review Process | Open     | Scrut Team         | Minor   |
| VAPT                | Closed   | Gautam             | Minor   |

1

1-2/2

Show

5

rows per page

SOC 2 Audit

Mark Audit Complete

Export Audit Report

Owner: Gautam

Audit Date: 1 Oct 2025

Audit Type: Internal

Status: In Progress

Audit Team: +

Framework: SOC 2

Entities: Organization Wide

Observation Period: N/A

Audit Readiness: 100%

Policies: 100%

Automated Tests: 100%

Evidences: 100%

Requirements

Controls

Requests

Findings

Corrective Actions

Audit logs

CC1.0-Common Criteria for Confidentiality, Availability and Security

CC2.0-Common Criteria for Confidentiality, Availability and Security

CC3.0-Common Criteria for Confidentiality, Availability and Security