DRUMMOND

DRATA

Securing Trust:

Cybersecurity and Compliance Automation for Health IT Vendors

Speakers

Gretel Witt
Senior Compliance Analyst
Drata Inc.

Michael Zgourovski
Risk Assessor
Drummond Group, LLC

MODERATOR

Michael Henry
VP, Growth Strategy
Drummond Group, LLC

DRUMMOND

- Drummond & Drata Partnership
- Cybersecurity Regulations in Health IT
- Scaling Compliance with Automation
- Q&A

DRUMMOND

Cybersecurity Regulations in Health IT

Cybersecurity Regulations Impacting Health IT

- Title 21 Part 11
- HIPAA Security, Privacy, and Breach Notification Requirements
- HITECH / HITRUST
- State specific requirements
- International Standards

4th Party Risk

- Organizations Need to Focus on Third-Parties
  - Have contracts in place
  - Assess risks associated with subcontractors
  - Know where data is held and who has access
- Organizations Shifting Back to Hybrid Cloud & On-Premise
  - Greater ownership and control of data
  - Tighter control over licensing, access, and vendor lock in

Changing Regulations

- Maryland COMAR HIE Requirements
  - New annual audit rules
  - Business impacts
  - How to prepare
- HIPAA Security Rule
  - Pending updates
  - Significant impact to small and mid-sized organizations

Increased Opportunity vs Increased Risk

- Market and Geographic Growth / Reach
  - Often results in new regulation/compliance obligations

- Delaying Compliance Comes with Financial Risk
  - Non-Compliance fines and sanctions
  - Reduced market trust, reputational damage, and lost customers
  - Business interruptions

ONC Health IT Certification ≠ HIPAA Compliance

DRUMMOND

- Where They Overlap
  - Some shared controls
  - Both are important to protect health data and privacy
  - HIPAA applies broadly to anyone handling PHI (not just to health IT developers)

- What's Required
  - ONC Health IT Certification alone is not enough
  - Ongoing monitoring for, and active maintenance of, HIPAA compliance is mandatory
  - Drummond provides compliance services for both programs

State AI Security Regulations

DRUMMOND

- What Regulators Expect
  - Limit and monitor sharing of health data with third parties
  - Maintain control over your data through BAAs and vendor contracts
  - Manage AI systems with the same policies and safeguards as other applications handling sensitive data
- Practical Approaches
  - Use virtual desktop infrastructure (VDI) with rented GPUs to isolate workloads
  - Keep sensitive data on locally hosted, partitioned drives for stronger control

SOC2, ISO 27001, and NIST Conformance

- Achieving Conformance
  - Internal control testing
  - Gap assessments to identify weaknesses
  - Independent audits for verification

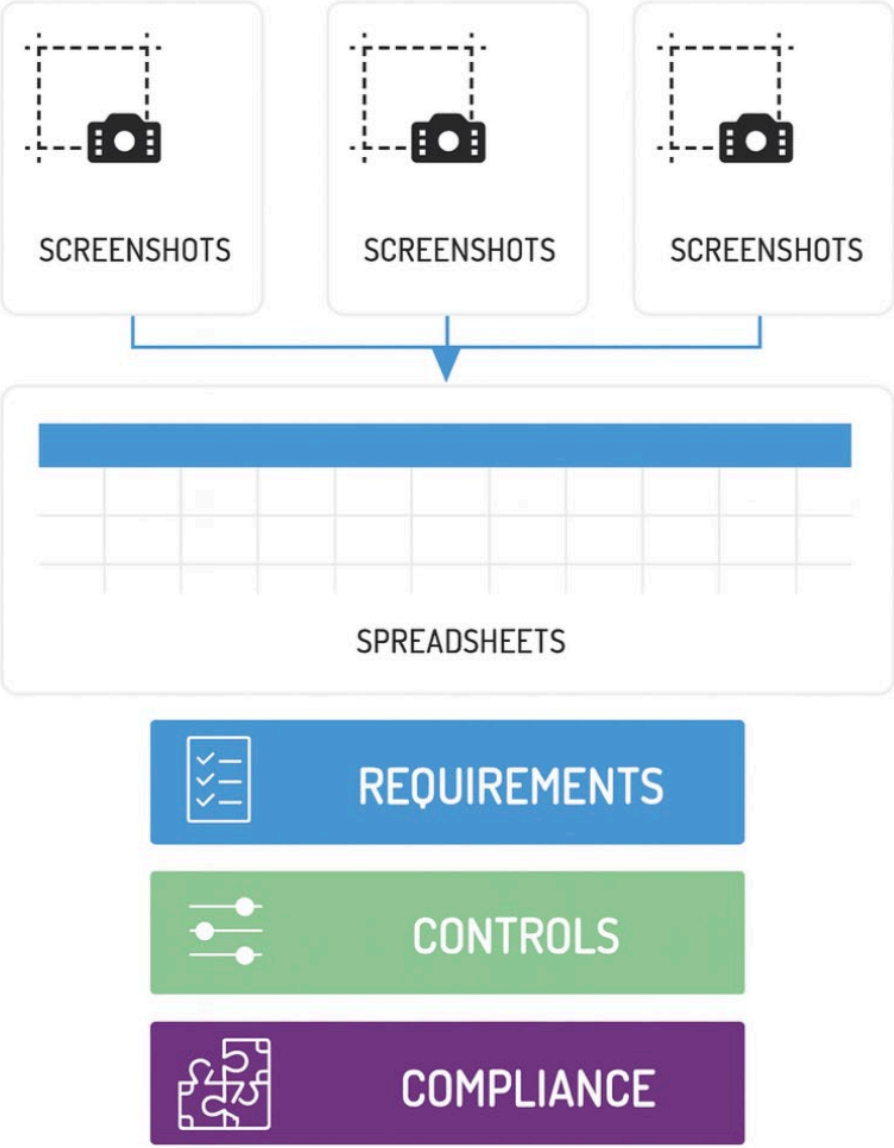
- Business Benefits
  - Builds market trust and credibility for your product/service
  - Demonstrates value and justifies cost of your product/service

DRATA

Scaling Compliance with Automation

Compliance Today

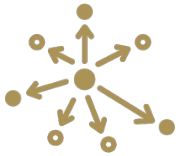
DRATA



The Case for Automation

DRATA

Reactive



Scattered

Manual

Burden

The Case for Automation

DRATA

Reactive → Continuous Monitoring

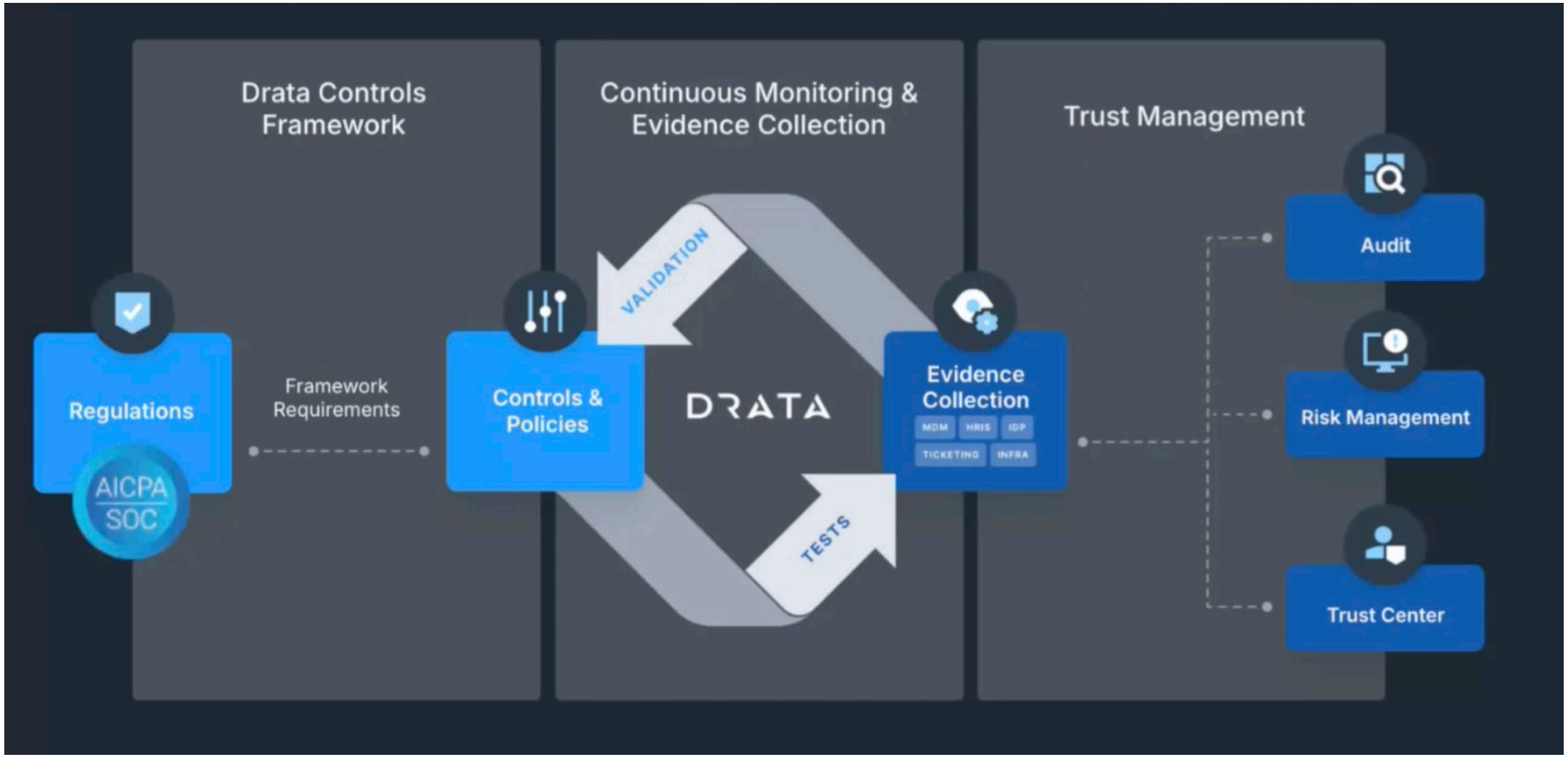
Scattered → Centralized

Manual → Automated

Burden → Business Enabler

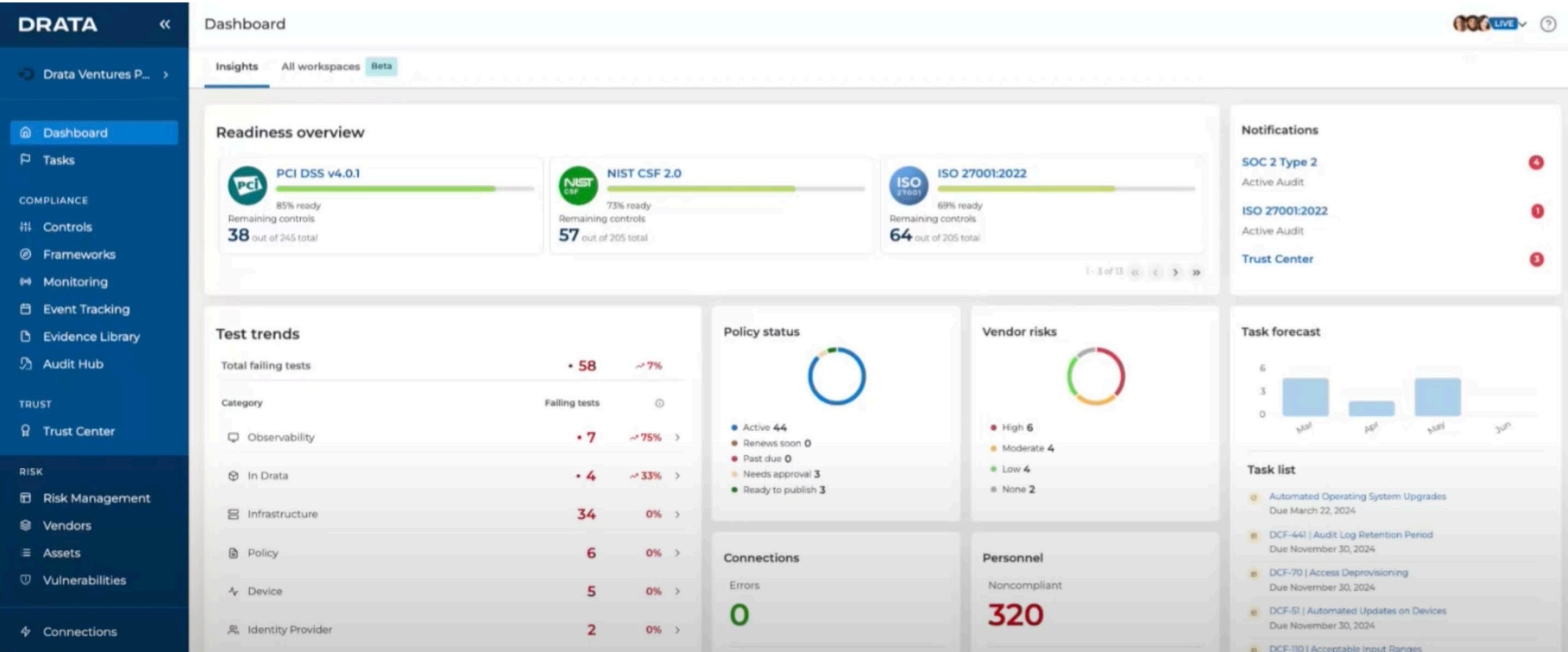
How Drata Works

DRATA



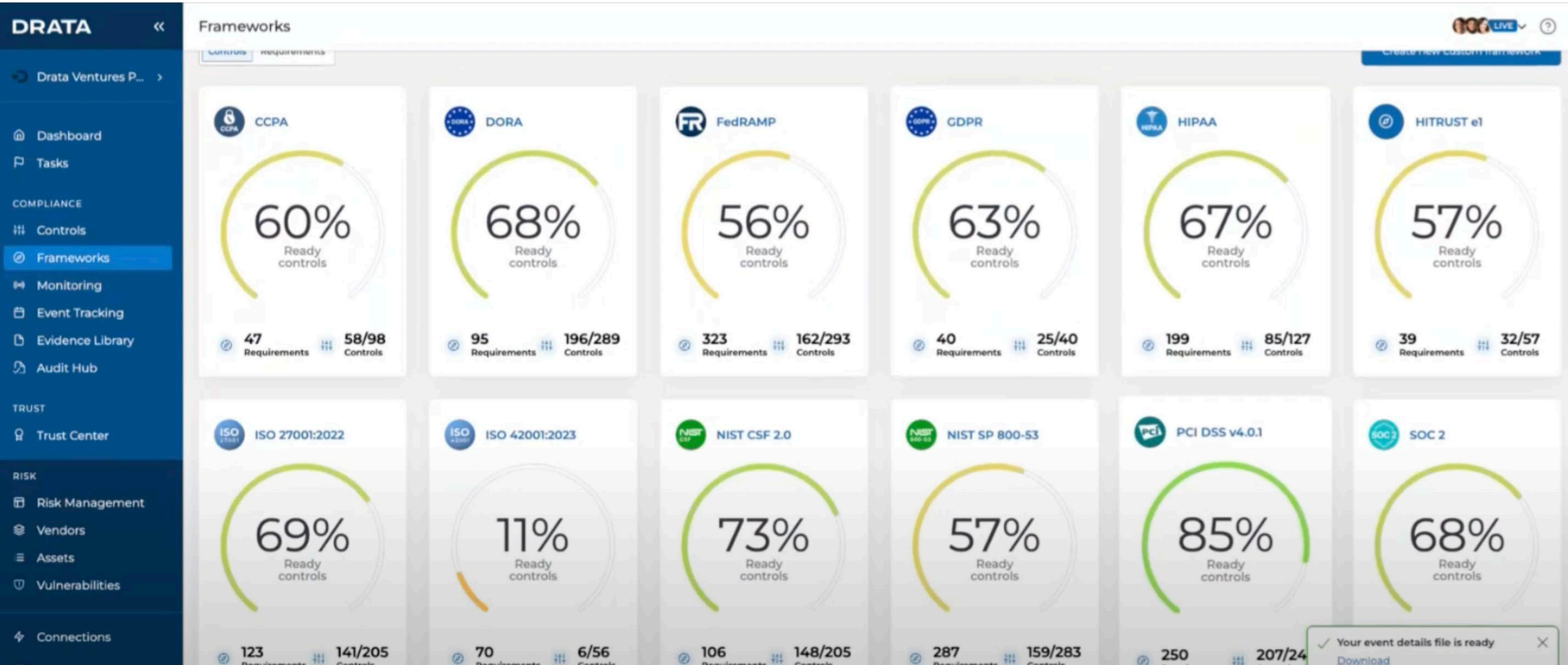
Drata in Action

DRATA



Frameworks

DRATA



Continuous Monitoring

DRATA

74%
Of Tests Passed

25
Failed Tests

74
Passed Tests

Create test

Filters (2)

Search

Name	Result	Findings	Status	Category	Active Connections	
Security Awareness Training Completed	Failed	216		In Drata	-	Fix failure
Production Code Changes Restricted	Failed	111		Version Control	GitHub	Fix failure
Storage Data Versioned or Retained	Failed	80		Infrastructure	aws	Fix failure
Cloud Data Storage Exposure	Failed	2		Infrastructure	aws	Fix failure
Public SSH Denied	Failed	7		Infrastructure	aws	Fix failure
MFA on Infrastructure Console	Failed	-		Infrastructure	aws + 1 more	Fix failure

Policy Center

DRATA

Policy Center

LIVE

Active policies | Archived or replaced policies

Policies have renewal dates to make it easier to prepare for compliance goals
It's a best practice to have personnel acknowledge policies at least once a year and many frameworks require it. Tasks and tests are automated based on renewal dates to help you stay on top of your goals. Default renewal dates are 1 year from the last approval or creation date, but you can change them as needed.

Policy overview

Renews soon	Renewal past due	Needs approval	Ready to publish
10	8	15	0

All policy statuses | All renewal statuses | Search by owner | Search by name... | Download all | Create custom policy

Policy name	Version	Status	Creation date	Approved date	Published date	Renewal date	Owner
Acceptable Use Policy	V3	Published	6 months ago Uploaded custom	Jul 14, 2024	Jul 14, 2024	May 31, 2025	

Vendor Risk Management

DRATA

Vendors › Current

LIVE

Current | Prospective | Risks | Insights | Settings

323 new vendor suggestions from Connections
Review suggestions

All Types | All Subprocessors | Status is Active | Impact Level is Critical | All Risks | All Security Reviews Statuses | All Next Review Deadlines | All Scheduled Questionnaires | All Business Units | Search by name... | Download | Add vendor

Search by security owner | Reset Filters

Vendor	Security review status	Next review deadline	Last review date	Risk	Risk associated	Impact Level	Subprocessor	Status	Security owner	Type
1Password Administrative	In progress	Jun 13 2026	Aug 25 2025	High	0	Critical	No	Active	[redacted]	Vendor
Abnormal Security Engineering	In progress	Due soon: Oct 01 2025	Jun 30 2025	High	0	Critical	No	Active	[redacted]	Vendor
AdPoll										

Vendors › Current › 1Password › Security reviews

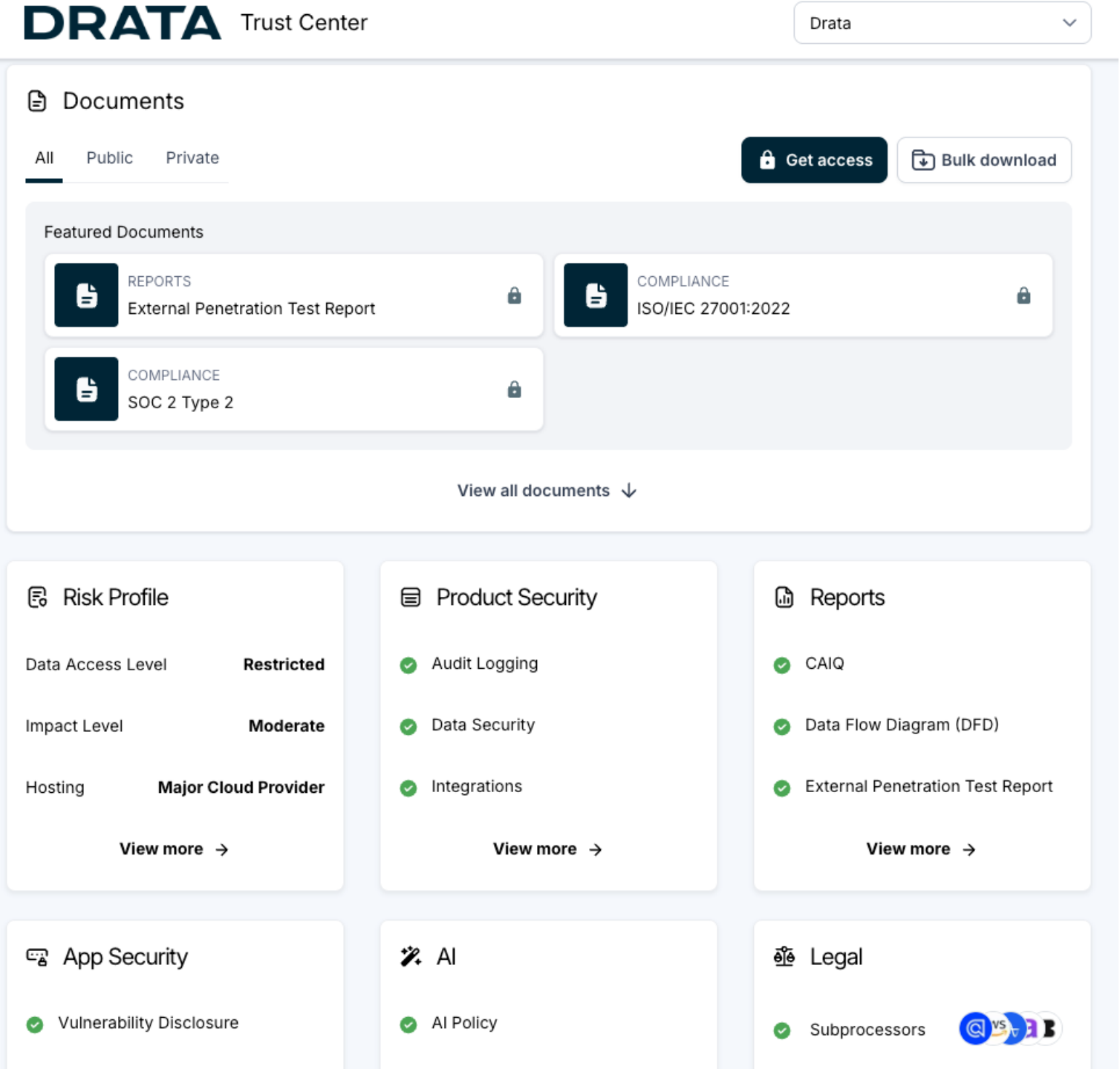
Active

1Password

Overview | Risks | Security reviews | Reports and documents

June 2025 SOC 2 Type 2 report review
Completed Reviewer: [redacted] Completion date: Jun 11 2025

June 2024 SOC report review
Completed Reviewer: [redacted] Completion date: Jun 25 2024



DRATA

SafeBase Trust Center

DRATA

SAFEBASE by DRATA

- Dashboard
- Accounts

Trust Library

- Trust Center Editor
- Knowledge Base (FAQ)
- Documents
- Trust Center Updates
- Subscribers
- Trust Library Search

Trust Inquiries

- Questionnaires
- Conversations

Questionnaires 68 of 68 Approved

Filters | Assignee | Approval | Answer Status

#	Question	Answer/Comment	Approval
64	Do you follow secure coding principles (SAST, DAST scans, OWASP Checklist etc.) while developing software used to process client information?	Yes	
65	Does your organization define and implement security testing processes in the development life cycle	Yes	
66	Does your organization separate and secure development, testing, and production environment ?	Yes	
67	Does your organization follow a documented Change management procedure for changes to the production environment impacting Client data ?	Yes	

SafeBase AI Questionnaire Assistance (AIQA)

The Future of Compliance Automation

DRATA

- Agentic AI is here
  - Static automation → intelligent, autonomous workflows
  - Example: VRM Agent
    - Auto-collects evidence, evaluates vendor risk in real time, and drafts follow-ups

DRUMMOND

DRATA

Q & A