A Quick-Start Guide to Compliance for Startups (Open Sourcing Datavant’s Compliance Policies)

Holly May Follow
Mar 24, 2019 · 12 min read

We are sharing this “quick start guide” for leaders of early stage data companies trying to build a compliance program while retaining a culture of nimbleness and empowerment. It’s everything we wish we knew a year ago.

Datavant’s vision is to connect the world’s health data. This puts us in the epicenter of privacy, security, compliance and regulation. We take that responsibility seriously. As a result, building a secure system, establishing regulatory compliance, and handling customer audits is a routine part of our business.

Over the past 12 months, we’ve spent over $500,000 and several thousand person-hours to complete a SOC 2 audit (required by many large enterprises), establish GxP/CFR Part 11 compliance (required by anyone submitting data to the FDA), handle Fortune 500 audits, establish HIPAA compliance (required by all of our customers in healthcare), and hired a Chief Privacy Officer (not to mention developing compliance programs around GDPR, HITRUST, CCPA, and many others). Moreover, building secure systems and a culture of privacy is critical for our long-term success.

This is a steep price of admission into an industry for a startup, but important for a company with broad ambitions in a highly-regulated sector. We took these steps very early in the lifecycle of our business — a decision I’m glad we made. For context, at our CEO’s last startup, they built similar programs only as they were crossing $100 mm in revenue — which is more industry standard.

The goal of this post is to create the how-to guide for CEOs thinking about compliance. While compliance is not a one-size-fits-all topic, we are open-sourcing our compliance templates, and walking through our thought process on a variety of compliance-related topics. I hope that this saves the next startup hundreds of hours of time, hundreds of thousands of dollars, and helps companies build compliance into their framework.

This post includes:

- Building compliance into your culture (preserving nimbleness and avoiding a check-the-box mentality)
- Why starting early matters
- How to start — what to keep in mind
- Where to start — getting tactical
- Lessons learned from what went well for Datavant
- Lessons learned from our challenges
- Appendix 1: External Resources
- Appendix 2: Datavant’s Policy Templates

Avoid ″Check the Box″ Culture (aka ″Compliance In Name Only″)

At first glance, building data security compliance into your company DNA from the ground up may seem contradictory to a culture that prizes fast action, autonomy and nimble experimentation, but at Datavant we do just that.

The classic mantra for Silicon Valley startups is to move rapidly, try unconventional ideas, and fail fast. This disruptive spirit often draws founders and employees to the fast pace of boundary-breaking companies.

The culture you create around compliance, security, and privacy matters. Tone comes from the top. Inside early stage companies, leaders can conflate boundary-breaking and rule-breaking, resulting in hazardous short cuts. Alternatively, they create a “check the box” culture around compliance. Compliance in name only might look like this: new hires join your company and receive a 100 page employee handbook with rules and policies; they are asked to sign it acknowledging they have received and read the contents and pledge to abide by the rules, and yet it's an open secret that very few employees *actually* read the SOPs and policies. This is a hallmark of check-the-box-compliance: doing it in name only.

Datavant, like many startups, has a cultural value of autonomy that we articulate as: "more responsibility and fewer rules". We give lots of autonomy to every employee. We don't have policies on expenses and we give unlimited paid time off. We trust employees to self manage and deliver at a high level. We believe highly talented and highly motivated teammates rise to the expectations set for them. Yet, we complement this independence with a very compliance-forward approach for employment, privacy, and security topics.

Here's what it looks like:

- Employees at Datavant review and pledge to standards of behavior and ethics every quarter on a 2 page document with simple explanations of their commitments. This keeps the commitments top of mind. This is in contrast to signing a lengthy, legalese employee handbook once, on a frenetic first day. You can see our model in Appendix 2.
- We defined privacy principles in our first 9 months. See Appendix 2.
- One of our first 10 hires was a leader to own privacy and data ethics. These principles have guided our product development and client engagement.
- From day 1, we tried to maximize technical ease of compliance and traceability. Invest up front in ways to build automated and technical compliance methods, rather than administrative and manual controls. Although it's more effort/cost upfront, it feels lighter. The invisible forces of compliance are baked into technology, not meetings, policies, processes and administrative systems that *feel* "compliancy".

Starting early matters — here's why

It may seem non-obvious, but making compliance and security core to your company from the early days is far easier than adding it in later.

- **Reason #1 to start early: Starting matters.** When it comes to security and compliance, something is better than nothing. Don't let perfect get in the way of good enough. There will always be more you can do; that feeling never fades.

- **Reason #2 to start early: Build the right habits from the ground up.** As the company scales, systems and patterns of behavior form regardless of whether they were consciously designed. It's hard to get these patterns right when you're small, but it only gets harder if you wait. If you wait until you're mature, there will be more time spent aligning, more time spent justifying priorities, more time spent planning the roll-out of controls, processes and tools to ensure minimal disruption across a much larger organization. It's like rebuilding your house's foundation while living in it: much easier if you get it right (or close to right) at the beginning.

- **Reason #3 to start early: Create credibility from the early days.** A functional compliance program gives a small company the look-and-feel of a bigger company, allowing it to punch above its weight class, especially in deals with enterprise customers. We were audited by a leading, large multinational company in our sector and the auditor privately described our quality approach as an "innovative strength of the organization" despite the fact that 4 pizzas would feed our whole team.

How to start — what to keep in mind

You'll crawl before you walk; you'll walk before you run. It takes a while to decipher the jargon, so a brief vocabulary lesson first:

- **Policies** capture the rationale and frameworks (i.e., what you are doing and why)

- **Procedures** document the process and requirements (i.e., the how)

- **Technical controls** are security controls that a computer system executes (e.g., user authentication (login) and logical access controls, antivirus software, firewalls)

- **Physical controls**, like locks and badge readers, maintain the security of the physical environment

- **Procedural controls,** like management oversight and approval, incident response processes, and security awareness training, ensure human judgement is in the loop

- **Cybersecurity framework:** You'll want to choose an established framework like ISO 27002 or NIST 800–53 as the foundation of security program, rather than reinventing the wheel. Your choice will depend on the compliance requirements of your business and industry, but the NIST 800–53 controls are a good starting point.
- **Security Program** includes all of the above things, collectively

Here are some key mindsets and philosophies we developed along the way. These may be helpful as you start your journey.

- Write your policies and procedures with the **expectation of scaling.** In your v1.0 of these documents, remember to explain the logic behind the current approach and the timeline for reevaluation.
- **Be consistent: walk the walk.** The policies and procedures you define must match what your organization actually does. Elaborate procedures that are followed inconsistently — or worse, that no one knows — are far *worse* than having no defined policies. Having policies and procedures that you don't follow is toxic. Not only does it breed a culture that says we don't do what we say and that's okay, you also will not get any of the benefits of having a rigorous system in place.
- **Share overlapping accountability, rather than silo responsibility.** Share security and compliance obligations across multiple roles when possible while you're small. Multiple functions co-own security and compliance: Engineering, Privacy, and Operations all engaged with overlapping scopes intentionally. This demonstrates that complying with our controls is the duty of everyone, not a single role. Organizationally, having camaraderie while designing and implementing a security program or preparing for an audit also helps a lot.
- **Start with procedures that describe what you already do**, and then write more visionary policies to frame them. Doing it this way helps avoid the "where do I start?" or writer's block when looking at a blank page. It's easy to slip into writing aspirational policies, which tend to be overly burdensome and unrealistic for small companies. Starting with concrete procedures grounds the policies.
- **Resist administrative processes as much as possible, but keep humans in the loop as appropriate.** Early stage companies will likely rely more heavily on

administrative processes for compliance (e.g., have a sign-off process and monthly review meetings), but should attempt to implement technical processes as early and as often as possible. Technical process should be one of the priorities of every policy review and revision, since it's the best way to maximize compliance (incentivizing employees to follow the rules by automating them) and reducing risk without creating friction or long-term compliance debt. Remember that supervision and judgement from the humans you hire is important too. All technical controls you implement will require validation (documentation and evidence that it does what you expect).

Where to start — let's get tactical

When you start Googling the first time or you call your first strategy session to brainstorm about building a security program or compliance program, the immediate first thought for most entrepreneurs is "Oh my goodness, there are so many policies and procedures to document".

This felt daunting for us. And it likely will for you too. It helps to remember that a compliance program evolves over time — don't let perfect get in the way of good enough.

Here's our suggestion for where to start as you develop your program:

1. **Frameworks and principles for a Quality Management System (QMS)**

Definition: QMS is a system that documents processes, procedures, and responsibilities for achieving your company's objectives to meet customer needs and regulatory requirements and improve its effectiveness and efficiency on a continuous basis.

2. Software Development Lifecycle

Definition: Process used by the software industry to plan, design, develop, test, deploy and maintain high quality software that meets or exceeds customer expectations and regulatory requirements.

3. Incident Response Policy

Definition: A policy that explains the appropriate way to address security incidents, including detection, analysis, containment, eradication, recovery, and post-incident activities.

4. Password Management Procedure

Definition: Policy designed to enhance computer security by encouraging users to employ strong passwords and use them properly.

5. Privacy Principles

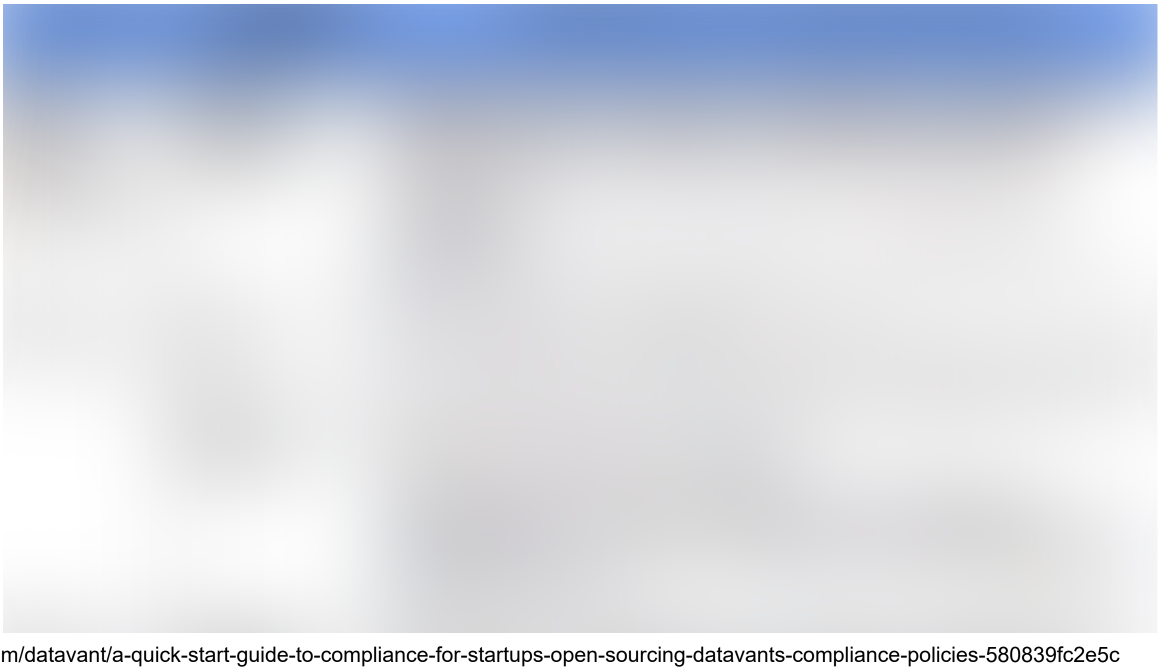
Definition: A policy that discloses some or all of the ways an organization gathers, uses, discloses, and manages a customer or client’s data

6. Data Management Policy

Definition: A set of rules defining the responsibilities and methods to appropriately use and safeguard any data.

These are by no means a full set of policies and procedures — we have two dozen today. Right-size your approach to your company. If you have nothing in place, getting started matters.

In preparing this post, I asked our Head of Engineering what he wished he knew a year ago when we started this journey. Here are the key items he identified.



Lessons Learned From What Worked Well

- **Focus your sights on a single target**: we started initially with SOC 2 as our core focus. This was a strong foundation for all other data security and compliance regulations. We have sequenced a roadmap of additional security program milestones.

- **Automate key controls as early as possible** to ensure compliance and minimize employees' desire to work outside the lines — it's harder to be allergic to controls when they run automatically in the background.

- **Able to invest:** as a well-capitalized company, we had the ability to spend money on developing templates, on getting readiness assessments, on working with Big 4 firms

- **Compliance ownership as cross-functional**: the opportunities and burden of compliance rest jointly on the shoulders of 3 individuals: Head of Engineering, Head of Privacy, and Head of People & Operations. Our Compliance Trio dedicated time to these topics on a regular cadence, setting aside an hour meeting on Tuesday nights, called SOCTuesdays.

> **Quick note** — *There is definitely an opportunity cost to this approach and part of why our staff investment was so high. The compliance trio was very often hunched over documents or debating choices together. We felt it was a worthwhile trade-off because it ensured multiple team members understand the compliance frameworks and tradeoffs that are now the operational infrastructure for the whole company. And they passed on their knowledge and points of view to their respective teams.*

- **Cultural support and executive buy-in:** our CEO routinely emphasized this as a priority, spotlighted the progress, and ensured that no one brushed aside "oh, it's just some compliance obligation". Support your team.

- **Stay realistic.** Don't be aspirational. It is better to have a limited set of controls that you follow 100%, than a stronger set of controls you can't fully comply with.

- We have a **strong networ**k of investors, advisors, and partners, and we talked to everyone we could to educate ourselves.

Lessons Learned From Our Challenges

- **Resist the temptation of "simple" administrative controls.** Administrative controls are easiest to create and document. Yet, they are the hardest to support consistently. Examples of administrative controls are: you have to file paperwork signed by specific people, or you have to call a meeting to review and approve something. As much as possible, automate these or use a technical method that scales.

- **One size doesn't fit all.** Defining the set of relevant regulations or criteria to follow takes time. The structure, scale and sequence of your compliance program will depend on many factors, including: the kind of data your business touches; whether you store it or not, whether its identified or aggregated. And the target changes over time. As you serve new types of customers, they will place new expectations and requirements and your compliance program will scale as a result. For instance, if your initial clients are similarly fast-moving, small startups doing data analytics they may spotlight security and compliance less than large pharmaceutical companies regulated by the Food & Drug Administration (FDA).

- **The work of a compliance program is never done.** Policies require ongoing implementation and monitoring. Certifications and audit periods expire or require regular renewal. Regulations change. You adapt over time as business changes. New customer segments mean new requirements.
- **Preparing for audits is a demanding assignment.** We had a lot of the right raw ingredients, mindsets, controls, and documentation, but we did not have a singular tool to track compliance, to schedule frequent tasks (e.g., policy reviews, approval meetings, audit log reviews) or to store key documents (artifacts). We spent much more staff time preparing for our first audit — gathering and printing files, searching emails for attachments, screenshotting records in Gsuite or github — than our auditor spent onsite.
- **Compliance done well takes time and money…that you cannot use for other priorities.** If you commit, you have to invest here.

Of course, companies vary. Your approach will change based on your industry and customers, your physical setting, your financial resources, and your prior experience.

We're trying to help, by open-sourcing some of our lessons and documents — see below for a list of some of our own policies and procedures as well as useful resources.

Appendix 1: External Resources

These resources may be helpful.

NIST's Special Publication 800–53 v4 is a great framework for preparing for SOC2 in any industry and can be downloaded for free here: https://nvd.nist.gov/800-53

If you're a healthcare company or working with healthcare data, you'll likely want **HITRUST** certification at some point. You can download the Framework via the website, here: https://hitrustalliance.net. You'll need to sign a license agreement to receive it, but the download is free. HITRUST also offers a self-assessment certification option, which is less expensive than the third-party certification.

If you're a software or data solution involved in healthcare and your end users are subject to **FDA regulation**, expect them to hold you to the same high standards. Relevant resources:

- ISPE GAMP 5: Compliant GxP Computerized Systems
- ISPE GAMP Good Practice Guide: Validation and Compliance of Computerized GCP Systems and Data (Good eClinical Practice)
- General Principles of Software Validation: Final Guidance for Industry and FDA Staff

Google's Governance, Risk Management, and Compliance (GGRC) project provides an open source solution for managing some of the common problems and workflows in this space.

Appendix 2: Open Sourcing Datavant Content

Datavant is offering some of our templates. These are not recommendations. Nor are we offering consulting services on this topic. These templates may not be right for you. These should help spur your team's brainstorming. The policies and procedures you establish should reflect your organization today. Feel free to email me directly if interested in any of these templates — holly (at) datavant.com

- Privacy Principles — https://datavant.com/privacy/
- Quarterly Employee Ethics Pledge
- Cultural Values
- Quality Management System (QMS) — table of contents
- Software development lifecycle
- Password Policy
- Incident Response Policy
- Data Management Procedure

Datavant's Cultural Values

First page of our ethics pledge — employees read and sign this quarterly

List of all procedures and policies we have in place today

Many thanks to Aneesh Kulkarni, Patsy Bailin, Eric Chin, and Bob Borek who helped craft and revise this piece, and to Travis May for encouraging these efforts.

Cybersecurity Compliance Privacy Data Culture