GROWTH CREATES THE RECORD

How a Prosecutor Reads a Founder's Record — and What to Build Before They Do

The Gap Between Compliant and Defensible Is Where Prosecutors Work

Shan Potts

Attorney · Criminal Defense · Appellate Advocacy · Trial Counsel · U.S. Immigration · Crisis & Regulated-Risk Advisory

In Regulated Markets, Growth Creates a Record

After more than two decades practicing law — in courtrooms, before appellate courts, inside criminal defense, and across regulated-risk advisory work — one lesson has repeated itself with enough consistency that I can now state it plainly:

> ***Companies are rarely judged only by what their founders believed they were doing at the time. They are judged by the record they created.***

That record may include investor decks, emails, board updates, customer communications, financial controls, compliance decisions, data practices, legal warnings, product claims, and the way leadership responded when risk became visible.

In the moment, those things feel ordinary. A founder is moving quickly. A company is raising capital. A team is trying to satisfy customers. The market rewards speed. Everyone is trying to prove the company can grow.

But when a company operates in a regulated market, growth does not remain just a business objective.

Growth behavior becomes a legal record.

And when that record is later reviewed by a prosecutor, regulator, plaintiff attorney, investor, acquirer, judge, or jury, the question may no longer be what the founder meant. The question becomes what the record can be made to mean.

> ***In regulated markets, growth creates a record.***

Control Architecture exists to help founders, investors, and boards identify that exposure early, build preventive controls, and create a record of responsible growth before someone else defines the story.

The Problem Is Not Only Bad Actors

Many founders do not begin with bad intent. They begin with pressure.

- Pressure to raise the next round.
- Pressure to show traction.
- Pressure to enter the U.S. market.
- Pressure to satisfy investors.

- Pressure to sign enterprise customers.
- Pressure to move faster than competitors.
- Pressure to explain risk with confidence before the company has fully built the controls to manage it.

Investors face their own pressures. They want to find category winners before the opportunity is gone. They want to believe in strong founders. They want diligence to confirm the growth story, not destroy it.

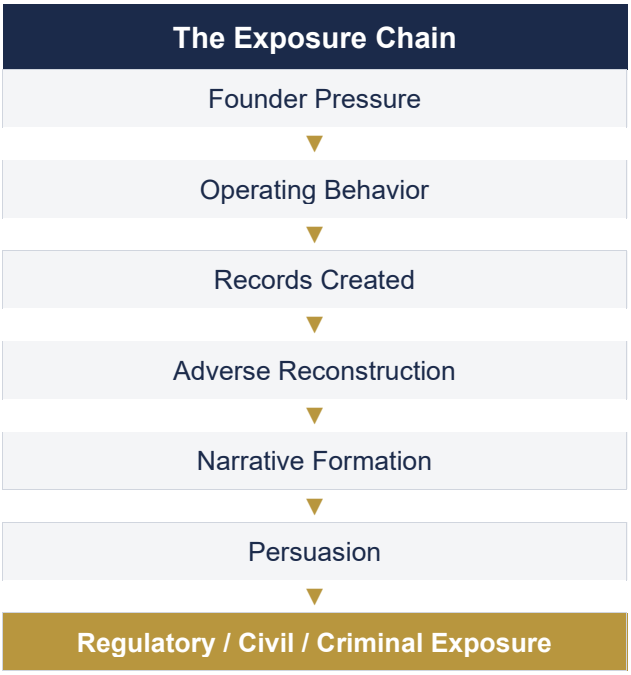
None of that is inherently wrongful. But in regulated industries — fintech, AI, cybersecurity, digital identity, health tech, crypto, payments, data privacy, and enterprise compliance — pressure without Control Architecture can become dangerous.

How it feels inside the company	How it can later be reconstructed
A founder sees speed.	A prosecutor argues recklessness.
A founder sees optimism.	A plaintiff attorney argues misrepresentation.
An investor sees traction.	A regulator sees weak controls and consumer harm.
A company sees incomplete systems.	A jury is asked to see knowledge, concealment, or intent.

> ***The issue is not what the founder meant. The issue is what the record can be made to mean.***

Diagram 1: The Exposure Chain

The following diagram shows how ordinary founder behavior — driven by pressure — passes through the company's record and becomes legal exposure.



Why Good Faith Is Not Enough — And Why the Lens Matters

This is where founders and investors often stop asking the right question.

They hire outside counsel. They engage a compliance firm. They build a GRC program. They subscribe to cybersecurity and data-governance platforms. They feel covered.

They are not wrong to do any of that. Those functions matter. But they do not answer the question that a founder with genuine good faith most needs answered:

> ***If I am acting in good faith, why do I need something beyond outside counsel and a compliance firm?***

The answer is specific, and it comes directly from the courtroom.

What Outside Counsel and Compliance Firms Actually Do

Outside counsel are trained to answer legal questions. They review contracts, assess regulatory requirements, draft disclosures, advise on employment issues, and respond to specific legal problems. When something goes wrong, they help the company respond.

Compliance firms are trained to build programs. They map regulations, create policies, implement procedures, train employees, and help companies demonstrate that requirements are being followed.

Both functions are essential. Neither is sufficient on its own. And both share a critical limitation:

> ***They are generally looking at what the law requires today. They are not looking at how today's operating record will be reconstructed by a prosecutor or plaintiff attorney tomorrow.***

The Appellate and Criminal Defense Lens

Appellate work teaches a discipline that most legal practice does not require: you learn to read a record the way an adversary will.

In appellate work, the record is largely fixed. The facts have been organized. The exhibits have been admitted or excluded. The jury instructions have been given. The sentencing record has been built. The arguments have been made. By the time an appellate court reviews the case, the story has already been told.

At that stage, the only question is: what does the record support? Not what the founder intended. Not what the executive believed. Not what the investor understood. What the record can support.

That discipline — reading a record the way a hostile court, prosecutor, or plaintiff attorney will read it — is exactly what most founders and investors have never had applied to their company's growth model while they still have time to change it.

Criminal defense deepens that discipline further. In criminal defense, you learn how the government builds a theory from ordinary facts. You learn how internal communications become evidence of knowledge. How missing controls become evidence of recklessness. How fund movements become evidence of fraud. How optimistic investor statements become evidence of misrepresentation. How a licensed professional's participation can be reconstructed as legal cover for a criminal enterprise.

> ***Control Architecture brings the criminal defense and appellate lens to the company's growth record before that record is tested — while founders and investors still have the ability to shape what it says.***

Why Appellate Thinking Belongs Before the Crisis

- By the time a case reaches appeal, the record is fixed. What should have been documented, preserved, or clarified can no longer be changed.
- Appellate courts do not retry facts. They review what was built and preserved below.
- The arguments available on appeal depend entirely on what was built into the record during operations and at trial.
- Control Architecture applies this discipline at the front end: before the record is tested, while there is still time to shape what it says.
- The best time to think about appeal is before the record is created.

The Function Comparison

Function	What It Does Well	What It Cannot Do Alone
Outside Counsel	Answers specific legal questions. Responds to problems. Advises on compliance requirements.	Does not apply a criminal defense or appellate reconstruction lens to the growth record in real time.
Compliance Firm	Builds programs, maps regulations, creates policies, demonstrates adherence.	Does not assess whether the operating record can defend the company when facts are reconstructed adversarially.
GRC / Cyber / AI Platforms	Monitor systems, collect evidence, automate compliance, track risk workflows.	Do not interpret the legal meaning of control gaps or assess how gaps become enforcement or prosecution narratives.

Function	What It Does Well	What It Cannot Do Alone
White-Collar Defense Counsel	Responds after allegations arise. Positions the record for defense.	By the time engaged, the record may already be weak. Prevention is no longer available.
Appellate Defense	Reviews the fixed record. Identifies preserved arguments.	Cannot change what was built during operations. The record is closed.
Control Architecture	Applies the criminal defense and appellate lens before the record is fixed. Builds defensibility into the growth model.	Does not replace any of the above. Connects and interprets what they produce.

Diagram 2: The Diligence Gap

Three types of diligence are available to founders and investors. Most companies perform the first. Many perform the second. Almost none have had the third applied before growth becomes a legal record.

Traditional Diligence	Regulatory Diligence	Exposure Diligence
Can the company grow?	***What rules apply?***	***Can the record defend how it grew?***
Market, cap table, contracts, financials, IP, regulatory obligations.	License requirements, enforcement history, pending obligations.	Adverse reconstruction, prosecutor narrative, good-faith proof — the missing layer.

> ***Traditional diligence asks whether the company can grow. Exposure diligence asks whether the company can defend how it grew.***

Who This White Paper Is For

I am writing this for founders, investors, boards, and advisors operating in markets where growth is also a legal question.

That is especially true for companies building in fintech, AI, cybersecurity, digital identity, data privacy, health tech, crypto, payments, remittances, enterprise compliance, and other regulated or high-trust environments.

If you are building in one of these spaces, the issue is not only whether your company can grow. The issue is whether your company can defend the way it grew if that growth is later examined by someone who does not share your assumptions, your urgency, your optimism, or your version of events.

What Founders Often Underestimate

- Good faith is not self-proving. It must be documented, escalated, and built into the record in real time.
- The operating files that feel ordinary today — emails, Slack messages, board updates, investor decks — may become exhibits.
- A prosecutor does not need malicious intent. Recklessness, willfulness, or knowledge inferred from the record is sufficient.
- U.S. market entry is not only a commercial event. It may be a jurisdictional exposure event requiring mapped controls before launch.
- Compliance programs demonstrate adherence to rules. They do not, by themselves, prove good faith when facts are adversarially reconstructed.

What Investors Miss

- Traditional diligence confirms market opportunity, cap table, financials, IP, and regulatory framework.
- It often does not ask: can this company defend the legal meaning of how it is actually growing?
- A company may be building enterprise value and legal exposure at the same time.
- Board participation creates oversight responsibility. Silence and failure to require controls may become part of the record.
- The investor's real question is not whether the company has compliance software. It is whether the company is building defensible growth or accumulating unresolved exposure.

The Liability Formation Model

Legal exposure does not usually appear all at once. It forms. It forms through ordinary decisions, repeated communications, missing controls, unverified claims, deferred warnings, and the records that companies create while trying to grow.

> ***Facts become records. Records become narratives. Narratives become persuasion. Persuasion becomes exposure.***

A fact by itself may look ordinary: a customer complaint, a board update, a missing disclosure, a data-access issue, a weak control, an optimistic metric, an internal warning, a legal memo no one implemented, a founder decision made under pressure.

But when those facts are preserved in the company's record, they become available for reconstruction. A prosecutor can organize them into a theory. A regulator can organize them into an enforcement narrative. A plaintiff attorney can organize them into negligence or misrepresentation. An investor can organize them into reliance or loss.

This is why Control Architecture is not just about compliance. It is about controlling the meaning of the record before someone else does.

Table 1: Operator Intent vs. Prosecutor Interpretation

Business Behavior	Founder / Operator View	Prosecutor / Plaintiff Interpretation
Moving fast before controls are mature	"We are still building the company."	The company prioritized growth over legal obligations. Reckless disregard.
Strong investor claims before proof	"We need to tell the growth story."	Knowing or reckless misrepresentation to investors.
Compliance deferred post-funding	"We will fix this after the next round."	The company knew controls were inadequate and continued anyway.
Legal advises but cannot stop operations	"We had lawyers involved."	Legal was symbolic. It had no real authority. Advice was ignored.
Aggressive customer or investor metrics	"These are reasonable internal numbers."	Metrics were false, inflated, or not independently verified.
U.S. expansion without exposure review	"We are testing demand."	The company entered a regulated jurisdiction without adequate controls.
Sensitive data without runtime controls	"Engineering is managing it."	The company exposed private or regulated data without governance.

Business Behavior	Founder / Operator View	Prosecutor / Plaintiff Interpretation
Customer funds without segregation	"Finance had a process."	Misuse, commingling, or concealment of customer funds.
Internal warnings minimized	"We were busy and would address it later."	Leadership had knowledge and failed to act. Evidence of intent.
Founder judgment over institutional controls	"The founder knows the business best."	Founder control overrode governance. Board oversight failed.

> ***Controls are not merely operational tools. They are evidence.***

Case Studies: From Founder Perspective to Exposure Narrative

The following case studies are not included to suggest that every founder is a bad actor. They are included to show how the same operating behavior can be understood very differently depending on who is reconstructing the record.

Defense-side and company-side statements are included because they show how founders, operators, executives, or companies may understand or explain their conduct. Allegations are distinguished from convictions. The citation discipline follows DOJ, CFTC, CFPB, and court sources; Reuters and Financial Times are cited only for facts not available in government sources.

Case Study 1: FTX — Financial Controls, Customer Funds, and Founder Authority

United States v. Bankman-Fried, No. 1:22-cr-00673-LAK (S.D.N.Y.) | DOJ Press Release, Dec. 13, 2022

The DOJ alleged that Samuel Bankman-Fried defrauded customers of FTX and investors in FTX by misappropriating customer deposits, making false statements, and concealing the diversion of customer funds to Alameda Research. On November 2, 2023, Bankman-Fried was convicted after trial on all counts, including wire fraud, securities fraud, and conspiracy charges. Sentencing followed in March 2024.

Founder perspective: Managing liquidity, supporting the ecosystem, moving quickly in a volatile market. Business judgments made under pressure. Financial structures complex, not criminal.

Defense framing: "Sam Bankman-Fried doesn't make decisions with malice in his heart. He makes decisions with math in his head." — Marc Mukasey, defense counsel, at sentencing.

Control Architecture failure: FTX lacked financial-control architecture capable of proving that customer assets were protected from related-party use, founder discretion, and misleading investor representations. Customer-fund movement became not an operational question but the center of the criminal narrative.

Appellate lens applied early would have asked: Were customer funds segregated? Who could authorize related-party transfers? Were founder decisions constrained by governance? Did investor statements match internal financial reality?

Source: DOJ Press Release, Dec. 13, 2022; Superseding Indictment, U.S. v. Bankman-Fried, No. 1:22-cr-00673-LAK.

Case Study 2: BitMEX — Cross-Border Structure, AML/KYC, and U.S. Touchpoints

United States v. Hayes et al., No. 1:20-cr-00500-JGK (S.D.N.Y.) | CFTC v. HDR Global Trading Ltd., No. 1:20-cv-08132 (S.D.N.Y.)

The DOJ charged Arthur Hayes, Benjamin Delo, Samuel Reed, and Gregory Dwyer with willfully failing to establish, implement, and maintain an adequate anti-money laundering program, as required by the Bank Secrecy Act. Hayes, Delo, and Reed each pleaded guilty. The CFTC also

charged BitMEX's operating entities with operating an unregistered trading platform and failing to implement required KYC and AML programs.

Founder perspective: Building a global platform, offshore and international. Restrictions in place. Users responsible for their own access. New and unsettled industry.

Defense framing: "He wishes he had had better controls and keep US persons off the platform. The controls were not a meaningless scam." — Reported defense counsel statement at sentencing.

Control Architecture failure: Treating offshore structure and partial user restrictions as sufficient. Without tested customer-access controls, documented legal analysis, and evidence that U.S. touchpoints were actively governed, cross-border complexity became part of the exposure narrative rather than a shield.

Appellate lens applied early would have asked: Where were the U.S. touchpoints? Were U.S. users meaningfully blocked and monitored? Were AML/KYC obligations mapped to actual operations? Could leadership prove U.S. exposure was identified, escalated, and controlled?

Source: DOJ Press Release, Oct. 1, 2020; CFTC Release No. 8270-20, Oct. 1, 2020; Guilty Plea, U.S. v. Hayes, No. 1:20-cr-00500-JGK.

Case Study 3: Wise — U.S. Market Entry and Consumer-Finance Disclosures

In re Wise US Inc., CFPB Administrative Proceeding, File No. 2025-CFPB-0004

The CFPB found that Wise US Inc. violated the Electronic Fund Transfer Act, the Remittance Transfer Rule, and the Consumer Financial Protection Act. The CFPB's order stated that Wise failed to accurately disclose fees and exchange rates to U.S. consumers, failed to properly resolve errors, and failed to meet refund and cancellation requirements. Wise agreed to pay a civil money penalty and provide redress to affected consumers. Wise stated it disagreed with the CFPB's characterization and that in limited cases some U.S. customers saw slightly incorrect fees.

Regulator narrative: Fee advertising, exchange-rate disclosures, refund practices, timing, and whether Wise complied with U.S. consumer-finance rules. The issue was not innovation — it was whether customer-facing representations and processes satisfied U.S. legal requirements.

Control Architecture failure: Treating U.S. customer-facing communications and remittance processes as operational matters rather than regulated representations requiring precise control. What looked like product communication became a consumer-protection record.

Appellate lens applied early would have asked: What claims are being made to U.S. customers? Are fee and exchange-rate disclosures accurate and tested? Do customer communications match operational reality? Can the company prove compliance across U.S. jurisdictions?

Source: CFPB Consent Order, In re Wise US Inc., File No. 2025-CFPB-0004; CFPB Press Release, 2025.

Case Study 4: Frank — Growth Metrics, Data Rooms, and Acquisition Representations

United States v. Javice et al., No. 1:23-cr-00251-AKH (S.D.N.Y.) | DOJ Press Release, Apr. 4, 2023

The DOJ alleged that Charlie Javice, founder of Frank, and Olivier Amar conspired to commit wire fraud and bank fraud in connection with JPMorgan Chase's approximately $175 million acquisition of Frank. The DOJ alleged that Javice falsely represented that Frank had approximately 4.25 million student users when it allegedly had fewer than 300,000 legitimate accounts, and that she

paid a data science professor to fabricate a synthetic customer list to support the representations. Javice was convicted after trial.

Founder perspective: Communicating market potential. Showing traction. Preparing a data room under deal pressure. Numbers reflected the growth story.

Defense framing: "This case was a 28-year-old versus 300 investment bankers from the largest bank in the world that did due diligence in 22 business days. We would never ask you to punish JPMorgan Chase's stupidity." — Ronald S. Sullivan Jr., defense counsel, at sentencing.

Control Architecture failure: Treating growth metrics as storytelling rather than transaction-level legal representations. Without verified user metrics, documented data lineage, and source-of-truth evidence, the growth story became the fraud theory.

Appellate lens applied early would have asked: What is the source of truth for user metrics? Are customer lists verified? Do data-room materials match internal systems? Are assumptions separated from facts?

Source: DOJ Press Release, Apr. 4, 2023; Superseding Indictment, U.S. v. Javice et al., No. 1:23-cr-00251-AKH.

Case Study 5: Done — Regulated Activity, Professional Judgment, and Platform Scale

United States v. He et al., No. 3:24-cr-00329-CRB (N.D. Cal.) | DOJ Press Release, June 2024

The DOJ alleged that Ruthia He, co-founder of Done, and David Brody, Done's chief medical officer, conspired to unlawfully distribute controlled substances and to commit health care fraud and wire fraud through Done's telehealth platform. The government alleged that Done prescribed ADHD medications without legitimate medical examinations, that prescribers faced pressure to approve prescriptions quickly, and that the platform's revenue model distorted clinical judgment. Both He and Brody were convicted after trial.

Founder perspective: Improving access to care. Licensed professionals involved. Technology making care more efficient. Responding to patient demand.

Defense framing: "Dr. Brody dedicated his life to his patients and his goal of expanding access for treatment of ADHD. He did not intend to do anything unlawful and unfortunately became a scapegoat." — Valery Nechay, attorney for David Brody, post-verdict.

Control Architecture failure: Treating the presence of licensed professionals as sufficient control architecture. Without structural independence, documented clinical decisions, and board visibility into regulated conduct, licensed participation was reconstructable as legal cover for scale.

Appellate lens applied early would have asked: Was professional judgment structurally independent? Could licensed professionals say no? Did compensation distort judgment? Were prescribing patterns monitored? Could the company prove that scale did not overtake professional independence?

Source: DOJ Press Release, June 2024; Indictment, U.S. v. He et al., No. 3:24-cr-00329-CRB.

Table 2: Case Study Comparison

Case	Core Control Failure	Governing Legal Theory
FTX / Bankman-Fried	No financial segregation. Founder discretion over customer funds. Board oversight absent.	Wire fraud, securities fraud, conspiracy (convicted after trial).
BitMEX / Hayes et al.	Offshore structure treated as AML/KYC substitute. U.S. touchpoints uncontrolled.	BSA violations — failure to maintain AML program (guilty pleas).
Wise / Wise US Inc.	U.S. customer-facing disclosures and remittance processes not governed as regulated representations.	EFTA, Remittance Transfer Rule, CFPA violations (CFPB consent order).
Frank / Javice	Growth metrics used as storytelling. No source-of-truth verification. Fabricated customer list.	Wire fraud, bank fraud, conspiracy (convicted after trial).
Done / He & Brody	Licensed professionals present but not structurally independent. Revenue model distorted clinical judgment.	Conspiracy to distribute controlled substances, health care fraud, wire fraud (convicted after trial).

What Prosecutors Look For

- What did leadership know, and when did they know it?
- Were internal warnings documented, escalated, and acted upon — or ignored?
- Were controls real and operating, or merely stated in a policy document?
- Were customer funds, regulated professionals, or sensitive data governed or exposed?
- Did the company continue operating after risk became visible?
- Can intent — or willful blindness — be inferred from the record?
- Was legal authority symbolic, or did legal and compliance functions have the power to stop conduct?

Preventive Controls: Building the Record Before Someone Else Defines It

Control Architecture identifies where exposure can form. Preventive controls build the record that prevents someone else from defining it.

In regulated markets, the legal fight is often not only about what happened. It is about what the record can be made to mean. Founders and investors may believe they acted in good faith — but belief is not proof. A company can survive weak controls for a long time while exposure quietly accumulates underneath the growth.

> ***Preventive advisory protects good-faith operators from building records that can later be argued as bad faith.***

Preventive controls create contemporaneous evidence that the company identified risk, escalated warnings, verified claims, protected customers, governed data, documented decisions, corrected weaknesses, and acted responsibly while scaling.

Without that record, plaintiffs, regulators, prosecutors, or adverse investors can fill the gap with their own narrative of negligence, recklessness, concealment, misrepresentation, or intent.

Diagram 3: Control Architecture

Control Architecture is not a checklist. It is a system of interdependent controls that together produce a single output: a growth record that can be defended when tested by a hostile audience.

Control Architecture Components		
Financial Controls	Data Controls	AI Runtime Controls
Legal Authority	Board Reporting	Metric Verification
Documentation	Crisis Protocol	Founder Mobility
Professional Independence	U.S. Market-Entry Analysis	Compliance Escalation

▼ All components feed into:

Defensible Growth Record

Why AI Runtime Controls Matter

- AI systems may process sensitive customer data, financial information, health records, or regulated content at runtime — often without governance that matches the exposure.
- When AI is deployed before data-governance architecture matures, the gap between what the system can access and what it should access becomes a legal and regulatory exposure.
- Investor and customer claims about AI safety, privacy, and data handling are regulated representations in many jurisdictions. They must match what the system actually does.
- A breach, a regulator inquiry, or a plaintiff complaint may focus on what data the AI accessed, who authorized that access, what protections were in place, and whether leadership knew the exposure existed.
- AI runtime controls are not back-office tools. They are part of the company's legal record.

Table 3: Preventive Controls Checklist

Control Area	The Record Question
Representations	Are investor, customer, partner, and market-facing claims verified and documented?
Warnings	Have legal, compliance, customer, employee, or technical warnings been escalated and addressed?
Financial Controls	Are customer funds segregated, related-party transfers restricted, and financial representations auditable?
Data and AI Governance	Are sensitive data flows, AI usage, access rights, and runtime exposures governed?
Legal Authority	Do legal and compliance functions have real authority to stop conduct, or are they advisory only?
Regulated Professional Judgment	If licensed professionals are involved, is their judgment structurally independent from the revenue model?
Metric Verification	Are user counts, customer lists, growth claims, and diligence materials supported by source-of-truth evidence?
Board Reporting	Does the board receive meaningful risk reporting — not only growth reporting?
U.S. Market Entry	Have jurisdictional touchpoints, disclosure obligations, and enforcement risks been mapped before launch?
Crisis Protocol	Is there a documented response protocol for regulatory inquiry, subpoena, or government contact?
Founder Mobility	Have immigration consequences of criminal or regulatory exposure been analyzed for key founders?
Adverse Narrative Test	How would a prosecutor, regulator, plaintiff attorney, investor, acquirer, judge, or appellate court read the record?

> ***The best time to think about appeal is before the record is created.***

The Market Has Control Tools. What It Still Needs Is Exposure Architecture.

The market already understands part of this problem. The growth of cyber, AI-governance, data-protection, compliance-automation, runtime monitoring, and GRC platforms shows that enterprise buyers understand something fundamental: unmanaged control environments create enterprise risk.

Platforms such as Privaclave, Nightfall AI, Cyera, BigID, Protect AI, Vanta, Drata, and Hyperproof reflect a market that already recognizes the importance of control infrastructure. But they also reveal a gap.

Most existing platforms help companies monitor, secure, automate, govern, or document controls. None of them answer the investor's deeper question:

> ***Is this company building enterprise value, or is it building legal exposure that has not yet surfaced?***

That is not a software question. It is an advisory question.

It requires legal judgment, litigation perspective, governance analysis, regulatory awareness, founder-risk interpretation, and an understanding of how narratives are built after failure.

Investor Moment	The Exposure Question Control Architecture Answers
Pre-investment diligence	Is the company's growth model creating hidden legal exposure?
Follow-on financing	Has the company's risk profile changed as it has scaled?
Board participation	What oversight risks could attach to the board or lead investor?
Portfolio monitoring	Which companies are accumulating unresolved legal or regulatory exposure?
Acquisition or exit preparation	What hidden exposure could impair valuation or kill a transaction?
Regulated-market expansion	Is the company entering a market where weak controls could become enforcement risk?
AI deployment	Are AI tools being deployed faster than governance and control maturity?
Crisis prevention	What facts would be damaging if regulators, plaintiffs, prosecutors, or journalists reviewed them now?

When Prevention Fails: Investigation, Defense, Sentencing, and Appeal

More than two decades of appellate work has taught me that the record is not created when litigation begins. It is created in the ordinary course of growth. By the time a case reaches appeal, the facts have already been organized. The exhibits have been admitted or excluded. The jury instructions have been given. The sentencing record has been built. The story has already been told.

At that stage, the question is no longer what the founder, executive, investor, or company meant to do in real time. The question is what the record can support.

> ***The purpose of control architecture is not to slow growth. It is to make growth defensible.***

This perspective is not theoretical. I am currently involved in advisory work connected to a federal telehealth prosecution now in the sentencing phase. I will not identify the matter here because confidentiality and professional responsibility require care. But the issues in that matter are instructive for regulated-scale companies: platform growth, telehealth operations, professional judgment, controlled-substance prescribing, revenue incentives, founder conduct, internal controls, sentencing exposure, and criminal narrative formation.

Advisory: What the Record Is Becoming

In advisory work, I look for the facts that could become dangerous before anyone calls them dangerous. The question is not simply whether the company is compliant today. The deeper question is whether the company is creating a record that can defend its growth tomorrow.

I look for gaps between what the company says externally and what it knows internally. I look for claims that have not been verified. I look for controls that exist on paper but not in operation. I look for warnings raised but not escalated. I look for legal or compliance functions that advise but cannot stop conduct.

Defense: How the Record Can Be Positioned

In defense work, the record is no longer hypothetical. It is being reviewed by someone adverse. At that point, the question becomes how the record can be positioned toward a defensible narrative. Where does it show good faith? Legal advice sought? Uncertainty rather than intent? Warnings addressed? Controls that existed and operated?

Defense is often a fight over meaning. The prosecutor may argue knowledge; the defense may argue ambiguity. The prosecutor may argue concealment; the defense may argue incomplete systems, not intent. But those arguments are only as strong as the record supporting them.

Sentencing and Appeal: The Record's Final Function

At sentencing, the court evaluates what the conduct means: was it predatory, reckless, negligent, or confused? Was there remediation? Evidence of good faith? These questions depend on the record built during operations — not at trial.

Appellate work teaches discipline because the record is largely fixed. What should have been built, preserved, objected to, documented, or clarified earlier is often what appellate counsel wishes they had. More evidence of good faith. More documentation of warnings addressed. More contemporaneous explanation of why decisions were made.

That is why appellate thinking belongs at the front end of advisory work. Founders and investors should not wait until the record is fixed to ask what the record should have shown.

Conclusion: Making Growth Defensible

After years of criminal defense, appellate work, and regulated-risk analysis, I have learned that legal exposure rarely begins the way it is later described.

Inside the company, the story may feel like growth: speed, pressure, fundraising, customer demand, product execution, market entry, imperfect systems catching up to ambition. But in a regulated market, that same conduct becomes a record. And once that record is in the hands of a prosecutor, regulator, plaintiff attorney, adverse investor, acquirer, judge, or jury, the question may no longer be what the founder believed.

The question becomes what the record can be made to mean.

FTX was not simply a story about financial complexity — it became a story about customer funds, related-party transfers, founder authority, and investor representations. BitMEX was not simply a story about an offshore platform — it became a story about U.S. touchpoints and whether restrictions were real. Wise was not simply a story about fintech expansion — it became a story about what U.S. consumers were told. Frank was not simply a story about startup metrics — it became a story about whether numbers in a transaction were true and defensible. Done was not simply a story about telehealth access — it became a story about whether regulated activity was protected from the business model.

Different industries. Different legal theories. Same structural lesson.

> ***When growth outpaces Control Architecture, the company may lose control over the meaning of its own record.***

The reason the advisory layer is missing is specific: it requires the criminal defense and appellate lens applied to the company's growth record in real time — while there is still the opportunity to shape what that record says. Control Architecture is that lens.

For founders: you may know your intent. But if the record does not support it, someone else may define it.

For investors: a company may be building enterprise value while also building legal exposure. Traditional diligence may not reveal that unless someone is specifically asking how the company's conduct could later be reconstructed.

For boards: oversight is not passive. If risk is not reported, escalated, documented, and addressed, the absence of that record may later become part of the story.

> ***Growth creates the record. Control Architecture determines whether that record can be defended.***

REQUEST A CONTROL ARCHITECTURE REVIEW

For founders, investors, and boards operating in fintech, AI, cybersecurity, health tech,
crypto, payments, data privacy, and other regulated-scale environments.

https://www.shanpotts.com/booking-calendar/founder-vc