axiom
corestream grc

Practical guide to implementing value-based compliance for cultural change

Introduction

This is a practical guide to implementing **value-based compliance** for real cultural change. Not the “annual training and hope for the best” version. The kind where people make the right call when no one is watching, and you can prove it without a spreadsheet scavenger hunt.

Compliance is the discipline of meeting your legal, regulatory, and internal obligations consistently, and being able to show the evidence.

Value-based compliance goes one step further. It turns compliance from a set of documents into a shared standard for how work gets done across the whole organization, including leaders, employees, and the extended enterprise (suppliers, contractors, and outsourced service providers).

Why culture is the make-or-break factor

A lot of compliance work is “binary.” Either you did the thing or you did not. But plenty of it is judgment-driven, and that is where culture decides outcomes.
So what do we mean by culture in this context?

Gartner defines culture as “the unstated ethical and compliance expectations that employees feel from their colleagues.” Put more plainly, culture is the pressure (often subtle) people feel about what is really expected, especially when the rulebook is not enough.

As one long-time compliance leader told Harvard Law, the culture compliance should foster is one where employees “are placing the welfare of clients and customers first.”

This is important, as when pressure hits, the job is not just knowing the standard, it is having the instincts, backbone and will to enforce it

> *“Compliance cannot be about just doing the minimum or not getting caught. It has to be how each and every employee acts, no exceptions. There can be no shortcuts, no looking the other way.”*
>
> Judy Perry Martinez, a former vice president and CCO in conversation with Harvard Law

If your culture does not actively surface concerns, people stay quiet. And when issues emerge late, the cost is high:

- IBM’s 2025 Cost of a Data Breach report puts the global **average breach cost at about $4.4M.**
- The ACFE’s 2024 Report to the Nations found **43% of occupational fraud cases were detected by a tip.**
- Gartner found **87% of employees faced situations in the last 12 months where they did not know how to comply.**

So, if people do not understand what “good” looks like, don’t align with the company's values or they do not feel safe raising a hand, you are running blind.

The CoreStream GRC philosophy: what we mean by value-based compliance

Value-based compliance **aligns compliance to outcomes**, not just avoiding penalties. It treats compliance as a way to **protect results, speed up decisions, and build trust,** not slow the business down.

In practice, it is built on:

- **Trust**: people believe the controls and reporting because they match reality
- **Integrity**: people do the right thing even when it is inconvenient
- **Clarity**: people know what's expected and what to do when it is unclear
- **Proactivity**: issues are surfaced early, not buried until audit season
- **Responsibility**: compliance is owned by everyone, with clear roles and follow-through

This is where "compliance" starts to look like "**integrity**." A compliance-only mindset can produce silence, box-ticking, and workarounds. An integrity-led mindset **makes speaking up normal, makes decisions defensible, and makes accountability real.**

.

A culture of integrity is essential for effective compliance. Compliance cannot be isolated; it must be a shared responsibility across the organization, integrated into decision-making, performance management, and third-party relationships.

Michael Rasmussen
Founder and Pundit

De-bunking common objections to re-building a compliance culture

“This will slow us down.”

It slows you down if it is over-designed. Value-based compliance speeds up decisions because it **increases confidence and reduces rework.**

“We already have policies.”

Policies are not culture. **Culture must be embedded** into your company. It dictates what happens when nobody is watching.

“We can’t overhaul everything.”

You do not need to. Start with **2-3 use cases**, prove value, then scale.

“My teams are too busy.”

That is exactly why you **build proof into the workflow.** Otherwise, you tax them later with audit archaeology and expensive clean-up.

5 things the best compliance cultures have in common

When CoreStream GRC consults our expert community, we have found that the strongest programs all have 5 defining traits show up again and again.

1) A real grip on obligations, and employees who can explain the "why"

The best organizations take a clear, **structured approach to their obligations**. They define them, assess the risk behind them, catalogue them in a way people can actually use, and check adherence over time. And they do it whether the obligation comes from a regulator, an industry standard, or an internal policy.

Think about the reality most teams are juggling: **SOX** expectations around controls, the **UK Corporate Governance Code**'s stronger focus on internal controls, **GDPR**, sector rules (like **FCA** expectations or healthcare requirements), plus internal policies and standards. They are not operating from one rulebook.

That mix is genuinely hard to navigate.

The cultural difference is what happens inside that complexity. **In strong programs, employees understand why the obligation matters and they aim to meet it even when it is inconvenient, and self-report when they cannot.** That is the gap between a proactive team that offers visibility early, and a team that is worn down by the process and lets things slip, or waits for someone else to pick it up.

Our client, UNT Health is a good example. They treat integrity as an everyday expectation, not a slogan, and they back it up with clear leadership, including a Chief Integrity and Privacy Officer who helps teams make the right call and speak up early when something feels off.

This has worked well for us. It's a nice moment in time to reflect on how the tool has helped us live our values.

Desiree Ramirez
Chief Integrity and
Privacy Officer

UNT Health
FORT WORTH

2) Assurance is not a sea of green, and issues are culturally acceptable (if owned and fixed)

Strong compliance cultures do not pretend everything is fine. They surface gaps early, report them honestly, and treat remediation as a delivery commitment, not a hope.

This is where **trust is built internally**. Leadership is never left guessing because the organization is willing to admit the truth, then prove it improved.

It is also where incentives matter.

Some practical ways to apply this without turning it into a performance-review circus:

- Put **1–2 integrity behaviors into performance reviews** (role-specific, not generic)
- **Reward early escalation and quality documentation**, not just outcomes
- Stop celebrating "hero fixes" that bypass process and create evidence debt

> *"Make integrity, ethics and compliance part of the promotion, compensation and evaluation processes as well. For at the end of the day, the most effective way to communicate that "doing the right thing" is a priority, is to reward it."*
>
> Stephen M. Cutler, EX- SEC Director of Enforcement

3) People handle grey situations with shared principles and a consistent "consult" reflex

Gartner's data study conducted of over 1,000 employees, found that;

- Uncertainty is the **most common** driver of **noncompliance**.
- **Over 87%** of the respondents had said they faced situations where they **didn't know how to comply** in the last 12 months.

Policies will never cover everything. The best cultures give people simple guiding principles and the confidence to escalate.

Keep principles short enough that people can actually use them.

Examples could be;

- If it cannot be evidenced, it did not happen.
- **Escalation is professional**, not political.
- **Exceptions are allowed**, but never hidden.
- **Ownership is named**, not implied.
- Then back it up with "**consult paths**" that are fast and non-punitive.

So yes, **culture matters**. But it has to be paired and reinforced with clarity people can actually use.

4) Ownership is named, escalation is fast, and third parties are part of the model

I**n strong cultures, responsibility is clear.** People know who owns the decision, who approves it, and who needs to be pulled in when it gets messy. Escalation is treated as professional, not political.

This also applies to the extended enterprise. If suppliers, contractors, or outsourced providers create risk or handle sensitive work, the culture has to reach them too. The **best programs make third-party accountability real, not a once-a-year questionnaire.**

Done right, training can be a useful tool here, but only if done right.

This means that, training is scenario-based and role-specific. Policies are succinct and written to be used, not admired. **People can find what they need in the moment of decision.**

A simple fix is i**ntegrating your policy management solution with your HR system.** This enables triggered automation: new starters get the right policies assigned on day one (by role and location), with attestations tracked automatically.

One of our clients, Pets at Home has benefited from this exact use case of joined-up policy and controls work in CoreStream GRC, then adding automation through their own GenAI integration to **cut manual drafting and speed review.**

5) Processes are right-sized so teams stay engaged

A strong compliance culture avoids over-design, or “death by a thousand forms”. It **asks for the information needed to make a decision defensible, and no more**. It streamlines. It automates where it should. You don’t want to capitalize people’s time on things that aren’t relevant for the business, a mountain of paperwork will not help relations between compliance and other employees.

Chyono Flynn at Rolls Royce calls this out as a key reminder to fellow GRC professionals in the Risk is Our Business podcast:

“Don't slavishly following a process without a focus on an outcome e.g. asking for information for information’s sake. Don't forget the people filling this in aren't GRC professionals, you need a workflow/process that is simple and easy to follow.”

What breaks in the real world when culture is weak

Weak compliance cultures rarely fail because people are bad. They fail because the organization teaches people, quietly, that compliance is someone else's job.

A) Compliance becomes abstract, so people default to habit

Well-written policies do not matter if they are hard to find, written for lawyers, or disconnected from real workflows. People default to "how we have always done it."

B) Reporting becomes theater

Dashboards look perfect. Risks look green. Everyone knows it is not real.

C) Evidence lives in inboxes and spreadsheets

Even if compliance is followed, an efficient compliance culture does not exist if proof is rebuilt after the fact. Audits become archaeology.

D) "Compliance" gets branded as bureaucracy

Once teams believe compliance slows them down, they work around it. That is the start of unmanaged risk.

How to start a value-based operating model: breaking down the core tenants

You can build a value-based operating model for compliance without a huge transformation program. You just need a simple operating model and the discipline to keep it real.

The goal is straightforward: **turn compliance obligations into consistent decisions, clear ownership, and provable execution.**

Step 1: Link compliance to business reality

Identify the obligations that drive your operations, then connect each one to the exact processes where it creates requirements or constraints.

For example, regulations/frameworks like these

- SOX and internal controls
- UK Corporate Governance Code expectations around internal controls and board oversight
- UK GDPR / EU GDPR
- FCA conduct expectations
- UK Bribery Act
- AML and sanctions
- NIS2 / DORA (for regulated or critical infrastructure environments)
- HIPAA / Open Payments
- ISO 31000

The point is not to create a library. It's to answer one question per obligation:

- Where does this show up in real work, and who is accountable for the outcome?

If you need a board-level anchor, the UK Corporate Governance Code is useful because it pushes boards to monitor and review the effectiveness of risk management and internal controls, not just sign off on documentation.

Step 2: Define “values for decisions,” not just policies for reference

This is where value-based compliance becomes real.

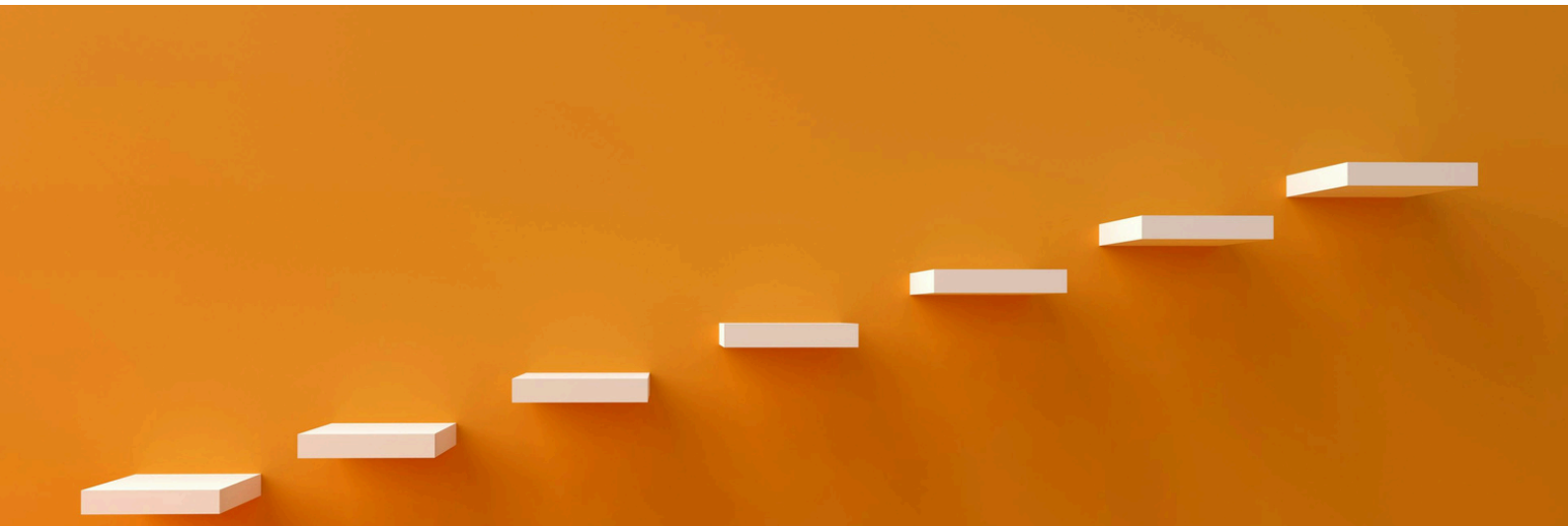
Policies are necessary, but under pressure people do not open a PDF and calmly interpret it. They make judgement calls. Therefore, you need a small set of **principles** that guide decisions when the policy is not enough.

This is also where ISO 37301 is a strong credibility reference if you want one. It frames an effective compliance management system around building, maintaining, and improving compliance in a structured way, not just publishing rules.

Step 3: Build role-based enablement so people can actually comply

This is the “training and usability” layer but tied into the operating model.

- Training is **scenario-based and role-specific.**
- Policies are **searchable, relevant, and assigned based** on role and location.
- People can **find the right answer in the moment** of decision.



Step 4: Make accountability in compliance unavoidable

For every “high-regret” compliance decision (the ones that create regulatory exposure), hard-code:

- **Owner** (who is responsible)
- **Approver** (who signs off)
- **Escalation path** (who gets pulled in when it is unclear)
- **Decision record** (what was decided and why)

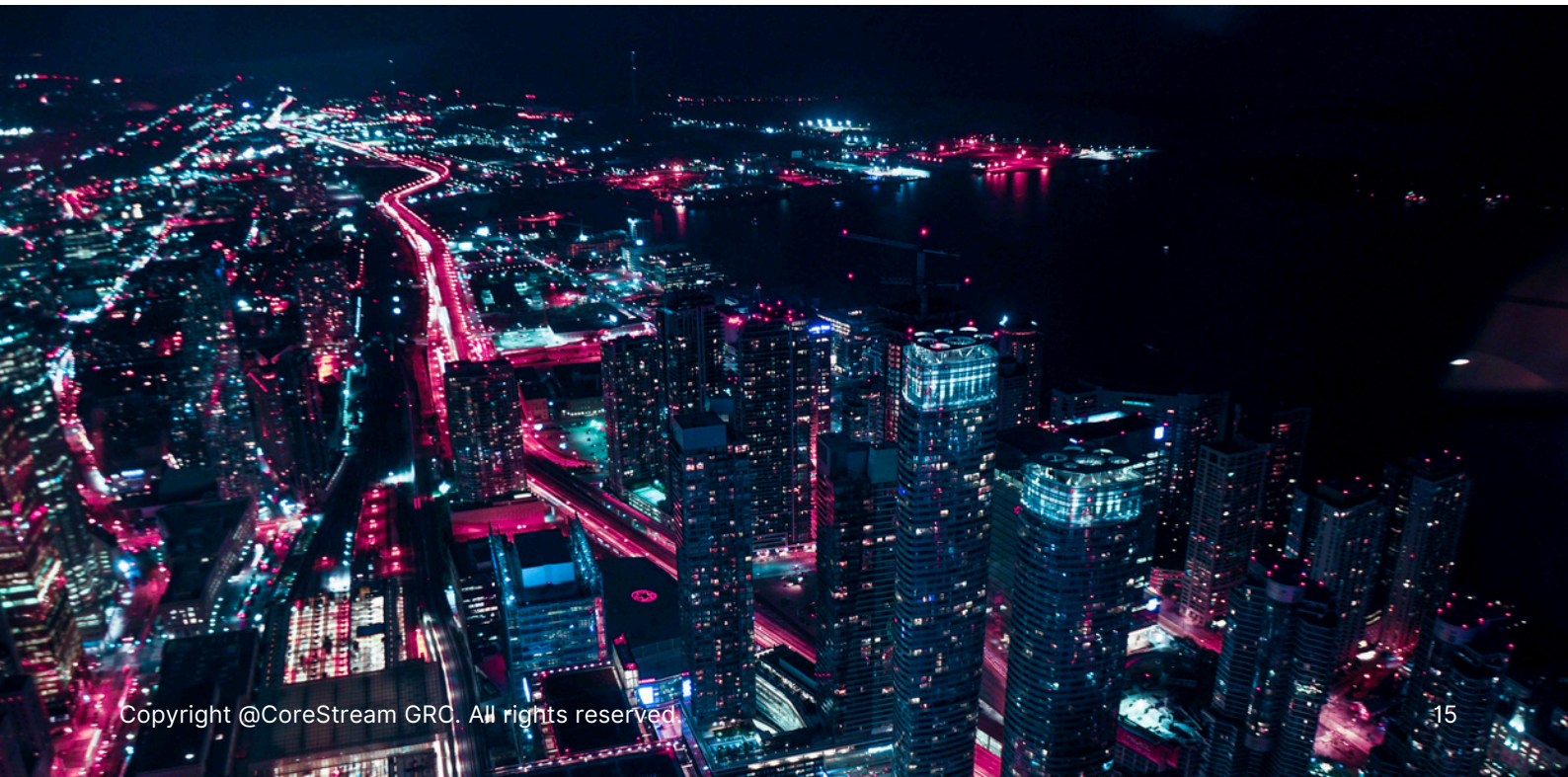
This is where trust is built internally. Leadership stops guessing because the accountability chain is visible.

Step 5: Build proof into the workflow

For compliance, “proof” is evidence that holds up to internal audit, external audit, regulators, and sometimes litigation.

This looks like;

- **Attestations**: policy acknowledgement, code of conduct, conflicts of interest
- **Control evidence**: access reviews, change approvals, reconciliations, monitoring logs
- **Third-party evidence**: due diligence, screening results, contract clauses, ongoing monitoring
- **Incident evidence**: timeline, decisions, containment actions, notifications, root cause analysis
- **Investigation evidence:** case notes, triage decisions, outcomes, remediation actions



Step 6: Run the operating rhythm

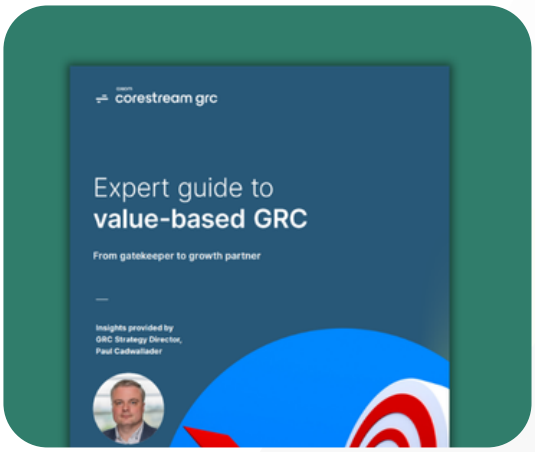
This is what keeps it from becoming a dusty “program.”

A lightweight rhythm (example):

Monthly:
- Top compliance risks and trending issues
- Exceptions and approvals (volume, reasons, repeat areas)
- Overdue attestations and training gaps by function/region
- Open investigations and remediation status (high level, sensitive)
- Third-party onboarding and monitoring status

Quarterly:
- Repeat findings and control failures (and whether fixes stuck)
- Speak-up metrics and retaliation risk indicators
- Policy lifecycle updates (what changed, why, adoption)
- Regulatory change intake and implementation progress

Annually:
- Compliance program effectiveness review
- Control design and operating effectiveness review
- Evidence readiness test (how fast can you produce proof)
- Lessons learned from incidents and investigations



Read the value-based GRC guide

But most importantly…

“Start the conversation. It can be as simple as a sketch on a whiteboard.”

If you cannot sketch how compliance works in your organization, you cannot run it consistently.

Metrics that actually tell you if your culture of compliance is working

Avoid vanity metrics. Split what you measure into two buckets.

Execution and proof

- % of key controls with evidence on time (proof discipline)
- Time to produce an audit-ready evidence pack (evidence debt indicator)
- Exception volume and repeat exceptions (process clarity signal)
- Time to detect and time to resolve issues (how long problems stay hidden)

Confidence and trust

- Repeat findings trend (are fixes sticking)
- Escalation health (are people raising issues earlier)
- Retaliation risk indicators and trust pulse checks
- Leadership confidence in reporting (do they believe the “green”)

If you want one more external reality check: EY’s Global Integrity Report 2024 found **38% of respondents said they would be prepared to behave unethically in one or more ways to improve career progression.**

That is why **culture cannot be assumed. It has to be managed.**

axiom
corestream grc

For more information please contact:

Email us to book your demo:
demo@corestreamgrc.com

corestreamgrc.com

Book a demo

Learn more about CoreStream GRC's Compliance solution

Follow us on LinkedIn