



Compliance is Not a Department

Making Ethics and Safety Part of How
You Develop People

Table of Contents

- Why compliance needs to be part of your business strategy..... 2
- The strategic case for integration 3
- 5 components of an integrated compliance program 5
 - Strategic alignment
 - Cross-functional ownership
 - Defensible program design
 - Culture as infrastructure
 - Unified learning and measurement
- The opportunity for culture change 9
- How Skillsoft approaches integrated compliance 9

Why compliance needs to be part of your **business strategy**

Compliance isn't a legal problem. It's a people problem.

Yet many organizations treat compliance and talent development as fundamentally separate investments. Whether it lives with HR or legal, compliance training isn't always thought of as talent development in the same way that leadership or technical training are.

On paper, that may make sense. But in practice, it can create blind spots that increase risk.

The risks that compliance programs address – harassment, data privacy, corruption, workplace safety, ethical AI use – are not regulatory abstractions.

They are behavioral risks.

They arise from how people make decisions, how leaders set expectations, and how culture either reinforces or undermines the right behaviors. These are the same forces that leadership development, technical upskilling, and change management programs are designed to shape.

Yet in many organizations, the people responsible for building workforce capability and the people responsible for managing compliance risk never compare notes.

“You can’t upskill your people without making sure they’re protecting themselves and the organization.”

**Asha Palmer, JD, CCEP,
LPEC @ Skillsoft**





CHROs

Invests in training to teach managers how to drive performance.



CCOs

Invests in training to teach managers how to help team members feel safe.

Both are trying to shape the same behaviors – but neither sees the full picture.

Risk management must be embedded in professional development. Compliance shouldn't be treated as a standalone function or check-the-box requirement.

CHROs and their counterparts in legal must work together to weave it into how the organization develops people. Managing risk is a shared responsibility, so it's important for the talent development strategy to reflect that ownership.

It's long overdue. The organizations that bring these functions together will lower their risk, build more trusted, and position their workforce to grow.

The strategic case for **integration**

The argument for integrating compliance into broader talent and business strategy isn't theoretical. It's grounded in three tensions that compliance leaders and HR executives encounter every day – tensions that can only be resolved when compliance stops operating as an island.

Outside-in meets inside-out

Every compliance program faces pressure from two directions. From the outside in, regulators, auditors and enforcement agencies define what organizations must do to protect against misconduct. Anti-bribery statutes, data privacy regulations, workplace safety standards, harassment prevention mandates – the list grows every year, and the penalties for noncompliance grow with it.

From the inside out, organizations are asking a different question:

- What kind of company do we want to be?
- What values do we hold?
- What culture do we want to build?

The strongest compliance programs connect these forces. External requirements set the baseline. Internal values define the standard.

When those align, compliance stops being a constraint and becomes an expression of culture.

But that convergence doesn't happen by accident. It happens when compliance leaders and HR leaders work from the same playbook, aligned on the same priorities and measuring progress against the same outcomes.

Completion versus protection

Here's a hard ball question for compliance leaders: Is your organization at more or less risk today, than it was a year ago?

Most organizations can tell you who completed their training. They can report on course completions, policy acknowledgments, and audit-ready records. But those metrics say little about whether risk has actually decreased.

Completion is activity. Protection is outcome.

Without evidence of understanding and behavior change, completion rates are a poor proxy for risk. This is where many programs fall short – measuring what's easy instead of what matters.

Closing this gap requires a different kind of measurement – one that connects compliance learning to behavioral outcomes and organizational risk indicators. Are employees making better decisions? Are incidents decreasing? Are leaders reinforcing the right standards?

Until compliance is measured this way, organizations will struggle to understand their true risk exposure.

A fragmented view on performance

When compliance training lives on its own island – separate platform, separate vendor, separate reporting – L&D leaders lack the data and the narrative to make the case for integration.

The result is a fragmented view of the workforce.

L&D leaders can track leadership and skills development. Compliance teams can track training completion. But neither can answer the bigger question:

Are our people prepared to perform their roles effectively and responsibly?



That answer requires a unified view – one that connects compliance, capability, and performance.

Without it, organizations operate with blind spots in reporting, in development, in strategy.

With it, they gain the visibility needed to identify risk, target gaps, and build a workforce that's both capable and accountable.

5 components of an integrated compliance program

If compliance is going to function as a core business competency rather than a standalone obligation, organizations need more than good intentions. They need a framework.

The following five components represent what separates organizations that proactively lower their risk and bolster a culture of safety and ethics from those that simply check the box.

1. Strategic alignment

Compliance priorities should be derived from business strategy, not just regulatory requirements. Every major strategic move a company makes carries risk. Anti-corruption exposure increases with international expansion. Data privacy obligations multiply with new customer-facing technology. Safety requirements shift with changes to the physical work environment.

Yet, compliance programs are built around the regulatory calendar, not the strategic plan. Training is assigned because it's required, not because it addresses the specific risks the business is about to encounter.

Strategically aligned compliance programs start by asking: What are the three to five biggest priorities for the business this year, and what compliance risks do they carry? That question reframes compliance training from "things we're required to do" to "things that protect our ability to grow."

Where to start:

Identify your top 3–5 business priorities and map the compliance risks tied to each. This shifts compliance from reactive to strategic.



Lenovo, a global technology company with 75,000 employees across 180 markets, tailors compliance training to each employee's role, location, and language – mapping training not to a generic regulatory calendar but to the specific risks created by the company's global footprint. What began as 20 tailored courses has scaled to 40, all maintained in step with evolving local regulations.

[**READ THE STORY**](#)

2. Cross-functional ownership

Compliance is a team sport. But too often, it's treated as the chief compliance officer's problem. The CCO owns the program, HR helps deliver the training, and everyone else treats compliance as someone else's responsibility until something goes wrong.

This model was never adequate, and it's become untenable.

While it's important for software engineers to know secure programming principles, it's also important for everyone else to have basic security awareness while connected to the network.

The same could be said about safety, anti-corruption, harassment and so on. The compliance risks that matter most to an organization don't respect the boundaries of an org chart, and the programs designed to address them shouldn't either.

Cross-functional ownership doesn't mean diffusing accountability so broadly that nobody is responsible. It means establishing the CCO and CHRO as partners – not parallel players – and creating shared visibility into how compliance learning connects to every other development area.

Where to start:

Bring the CHRO and CCO together around a shared definition of workforce readiness. Use that to identify overlap between leadership development and compliance training.

3. Defensible program design

Most compliance programs are designed to prevent incidents. But the real test comes after an incident during an audit, an investigation or a lawsuit.

When regulators or opposing counsel examine your compliance program, they assess the training delivered, whether it addressed actual risks, whether it produced measurable outcomes, and whether the organization demonstrated improvement.

A defensible program is one that can withstand scrutiny.

It includes documented risk assessments that informed what training was developed and for whom. It includes evidence that training went beyond generic, one-size-fits-all content to address the specific risks faced by different roles and functions.

It includes outcome data – not just completion rates but assessments, behavioral indicators, and evidence that the program evolved over time based on what the data revealed.

Defensibility has legal and financial consequences. Whether the courts rule in your favor hinges on the rigor of the program and the actions of leaders.

Where to start:

Audit your current program against these elements. Where you can't demonstrate relevance or outcomes, you've identified your highest-risk gaps.

4. Culture as infrastructure

No compliance program succeeds in a culture that undermines it. An organization can have the most comprehensive training catalog in its industry and the most rigorous assignment and tracking processes, and it will still fail if people don't feel safe speaking up, if leaders don't model the expected behavior, or if incentive structures reward results at the expense of ethics.

The workplace's culture serves as the infrastructure that determines whether a compliance program works in practice or only on paper.

Building that culture is not a compliance-only exercise. It requires alignment between how an organization develops its leaders, how it defines performance expectations, and how it handles misconduct when it occurs.

When compliance and talent development are integrated, cultural alignment becomes a natural byproduct.

Where to start:

Look at how leaders are evaluated and rewarded. If ethics, safety, and accountability aren't part of performance expectations, compliance will remain theoretical.

Boyd Gaming, a national hospitality company, embedded safety into its operating model through property-level safety committees, executive-sponsored recognition programs, and standardized training across 28 locations. The result: incident rates well below industry averages and 83% of employees reporting they feel safe at work.

[READ THE STORY](#)



5. Unified learning and measurement

When compliance training lives on a separate platform from leadership development, technical upskilling and business skills training, organizations pay a price – and not just in vendor fees. They pay in fragmented data, duplicated administrative effort, and inconsistent learner experiences. It also makes it tougher to have a full picture of workforce readiness.

An L&D leader managing three or four platforms can tell you who completed what on each system. But they may not be able to answer more important questions like: Are our people equipped to perform their roles effectively and ethically?

That question requires connecting compliance outcomes to leadership capability to technical proficiency. That connection is a lot harder to make when the data isn't integrated.

Unifying all other areas of training with and compliance leads to several benefits that reinforce building a culture that values ethical behavior and safety. Most notably, it makes it easier to collatethe data, so organizations can identify patterns and improve how they target skill gaps.

It becomes a single source of truth that accounts for the full picture.

Where to start:

Map where compliance and L&D data currently live, then define a phased plan to bring them into a shared view – even if systems remain separate initially.



The opportunity

For too long, compliance has been treated as a tax on growth – a necessary cost, managed at arm’s length, measured by whether people completed their training on time. That model was never good enough, and it’s becoming untenable at a time when the pace of change, the complexity of regulation, and the expectations of employees, customers, and regulators are intensifying.

The organizations that will thrive are the ones that see compliance not as a separate obligation but as an integrated capability – a competency that makes leaders more effective, cultures more resilient, and growth more sustainable.

The shift doesn’t require a revolution. It requires a different way of thinking about what compliance is for and where it belongs in the organization. It requires the CHRO and the CCO to partner. It requires compliance learning to be connected to the broader development ecosystem. And it requires a willingness to measure what matters – not just completions, but outcomes.

The opportunity is to cement a culture that embraces high standards for ethics, privacy, and safety, while simultaneously supporting a workforce with meaningful skills development. Doing so creates a workplace in which employees feel comfortable and respected, which ultimately reflects outward to benefit the customers, patients, or patrons your organization hopes to serve.

Companies who are setting strategy, who want to go into new territories, create new products – all of that comes with risk,” says Palmer, with Skillsoft. “You can't just be making plans for the company to grow and expand without thinking about how you prepare the people you have for the risk you're about to encounter.”



How Skillsoft approaches integrated compliance

The Skillsoft Percipio Platform is the leading skills management platform for the AI era and one of the only platforms that brings compliance under the same umbrella as leadership, technical, and business skills development.

My To-Do List

- Encourage your team to try a CAISY simulation
- Keep your team's skills current by assigning content
- Check your team's learning activity
- Encourage your team to set a learning goal

Assessments
Create assessments that measure skill gaps and recommend relevant learning content.

Course Builder Pro
Create interactive, flexible courses for self-paced learning.

With 575+ compliance risk topics across legal and EHS domains, support for 45+ languages, AI-powered learning experiences and unified reporting that connects compliance outcomes to broader workforce readiness, Skillsoft helps organizations operationalize the integrated approach described here.

For organizations that already use Skillsoft for leadership and business content, extending to Skillsoft's Compliance Suite means no new vendor, no new platform and no new learning curve – just a more complete picture of how your people are developing and how your organization manages risk.

Ready to explore what integrated compliance looks like for your organization?

Take the [Skills Readiness Assessment](#) or request a demo at skillsoft.com