



Compliance and risk

– how to futureproof your business

A hands-on guide to reducing business risk by switching up your approach to compliance training, empowering your employees, and building a risk-aware culture.

Contents

Introduction	p.1
Chapter 1: Risk management 101	p.2
1.1 What is risk management?	p.3
1.2 The cost of poor risk management	p.4
Chapter 2: Building a risk-aware culture	p.5
2.1 Why compliance training fails	p.6
Chapter 3: Implementing a risk management program	p.8
3.1 How to empower learners	p.9
3.2 How to make compliance training engaging	p.11
3.3 How to amp up your L&D team	p.12
3.4 The right tools for the job	p.13
Conclusion	p.14
About the Authors	p.15
References	p.16

About Learn Amp

Learn Amp is an award-winning People Development Platform. Learning, employee engagement and performance management — all in one.

We're on a mission to make work life, work better. We make it easy to map out and deliver the best employee journey. Learn Amp combines learning, engagement and performance management tools in one seamless platform, driving better business results and higher employee retention.

Introduction

Business leaders know that **the future of their companies depends on compliance**. In today's increasingly regulated industries, the average company spends over \$160,000 per thousand employees on compliance training¹.

There's just one problem. **Standard compliance training is no longer fit for purpose**.

Now, more than ever, companies need risk management programs that prepare employees for the unexpected. **A top-down, "check-box" approach to compliance training cannot adjust to the realities of a post-pandemic world**, with its hybrid workforces and emerging business risks.

To create a risk management program that has a genuine impact on employee behaviour, we need to empower our employees with the **right learning tools** and **build a truly risk-aware culture**.

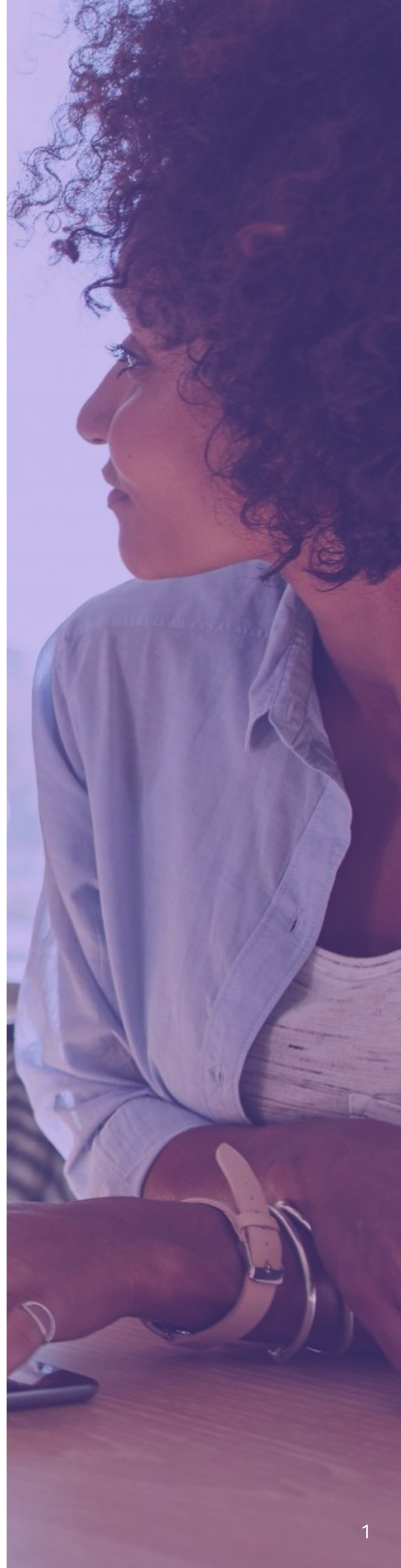
In this white paper, we'll show you how to transform your outdated compliance training into an **agile, employee-led and engaging risk management program** that will help to future-proof your business.



Alyson Thomson,

Regulatory Learning Manager, Paragon Bank

“When looking at cascading Regulatory learning we aim to make it more than just a tick box exercise. We strive to make it as engaging as possible whilst still providing the necessary learning and look for a means to check understanding. It is also crucial for us to have a means of evidencing the training/ understanding, facilitate line managers being able to see where there teams are in relation to completion of Regulatory learning and be able to produce Management Information (MI) for Senior Management and the Board.”



1. Risk management 101

When we hear the term “risk management”, too many of us fall into the trap of thinking of compliance training.

However, risk management is a far broader and more comprehensive agenda than simple regulatory compliance.

In this section, we'll explore:

- The difference between compliance and risk management;
- The consequences of poor risk management;
- How risk management can shift from a necessary evil to a strategic advantage.



1.1 What is risk management?

Risk management is the process of identifying possible risks, and then taking steps to mitigate, avoid, or plan for those risks.

For many companies, especially those in highly regulated industries, compliance is a major component of risk management. It's important to note, however, that compliance with legal and regulatory requirements is never the whole story.

Risk management involves addressing every area in which employees could potentially reduce or increase business risk. This includes:

- Operations
- Marketing
- Communication with customers
- Recruitment
- Data management
- IT and cybersecurity
- Business strategy
- Legal compliance
- Internal communications
- People management
- And much more!

Business risks can be grouped into three categories: preventable risk, strategic risk, and external risk².

Information is only valuable if it is put to use. Information is made up of units of data – it is knowledge that transforms that information into useful, practical conclusions.

For example, you may have the information that more customers are buying your products in December – but it takes market knowledge to relate that information to the fact that December is the month in which many of your customers are celebrating Christmas, and that your product is perceived as a good gift choice.

Information is easy to reproduce, whereas knowledge is unique, specific, and often tied to individual employees. Knowledge is the process of remembering, understanding, applying, analysing and evaluating information.

Risk management is far more than a set of policies and procedures.

Clearly, the process of managing business risk cannot be captured in an employee handbook or an annual compliance training session. In today's fast-paced business environment, change can be sudden and unpredictable, and employees may find themselves making decisions in situations not covered by the handbook or existing compliance guidelines.

Essentially, risk management needs to become an attitude and a behaviour, not a policy.

Employees need the capacity to evaluate risks, both predictable and unexpected, and then act in the best interests of the organisation and with a strong sense of ethics.

Compliance training, operational policies and procedural checklists are all helpful, but without an overall view of risk management as a fundamental component of business strategy and operations, they will fail to protect your business.

1.2 The cost of poor risk management

The consequences of an outdated or ineffective risk management strategy are no joke.

For starters, there are serious financial consequences. The numbers are alarming:

- The average cost of non-compliance is now \$14.82 million per organisation³;
- The cost of non-compliance has increased 45% since 2011⁴;
- Non-compliance costs businesses an average of over \$4 million in lost revenue.

These financial losses aren't just the result of government fines for failure to comply with regulations. In fact, penalties are often the least of your worries. The costliest consequence is the disruption to your business, as employees struggle to resolve the incident and return to compliance.

Of course, the cost of failing to properly manage risks isn't only financial.

Failing to implement an effective risk management plan can also have a major impact on your company brand. You may well lose customers, either because your business is no longer considered trustworthy, or because the disruption triggered by a compliance breach causes your customers too much inconvenience.

Nor is the financial fall-out short-lived. For instance, companies that experience a data breach as a result of non-compliant cybersecurity measures had share prices 13% lower than the NASDAQ index, even three years after the incident⁵. You might also find that you lose employees in the fall-out. Today's workers prefer to work for companies which align with and represent their values – and a serious breach of ethics by a senior staff member may send other employees out the door.

Companies spend a fortune on compliance measures – but these measures don't always address the root cause of non-compliance.

The average compliance cost for companies worldwide is \$5.47 million. Companies in highly regulated environments spend even more – for instance, the financial services industry spends an average of \$30.9 million⁶. While these huge expenditures reflect how seriously today's businesses take compliance, it's not clear if they're using their money in the most effective ways.

Companies typically spend the most on specialised technology to reduce cybersecurity issues, such as data non-compliance and data breaches⁷. This makes sense – automating cybersecurity compliance is extremely helpful, and can save businesses an average of \$1.55 million in the event of a data breach⁸.

However, risk management is really a people issue, not just a software issue.

Even in terms of cybersecurity, 48% of data breaches are caused by hackers and insiders⁹. Preventing hacking by training employees may be even more valuable than the latest expensive cybersecurity measures. For example, a corporate data security training program saves businesses an average of \$2.54 million – \$1 million more than an automated cybersecurity platform¹⁰.

In other words, when it comes to managing and reducing business risk, the right software is definitely helpful – but the right L&D strategy is vital.

\$4M

in lost revenue

\$2.5M

savings with
compliance training

2. Building a risk-aware culture

The business world moves fast. Regulations are on the increase in many industries. Maintaining compliance is becoming ever more challenging. Today's employees and companies are adjusting to the new realities of a post-pandemic workplace, with hybrid and remote work fast becoming the norm.

In this context, companies need to create a culture of risk awareness. In a risk-aware culture, employees are empowered to take responsibility for managing risk. They have the tools and training to identify risk when it comes up, and then to make the more compliant, more ethical and more risk-sensitive decision in the moment.

Here, we'll look at how to build a more risk-aware working culture.



2.1 Why compliance training fails

In 2012, Morgan Stanley employee Garth Peterson was charged with criminal misconduct for bribing a government official.

Peterson had received not one, but seven compliance training sessions, as well as 35 official reminders from the compliance department. The compliance training and notifications explicitly banned all employees from bribing government officials – and yet Peterson ignored them. In a subsequent interview, he commented, “They check the box that says, “He’s complied.” And then [I] just quietly hang up, or put my phone aside, and do [my] other work¹¹.”

In other words, this was not a failure of compliance training, per se. Peterson had certainly received compliance training. However, he seems to have felt that the compliance guidelines were merely a pro-forma exercise, rather than actual expectations for his behaviour as an individual.

So, what’s the problem with compliance training?

One issue, according to Hui Chen, the former compliance expert for the US Department of Justice, is that companies do not even know if their compliance training is working¹². Only 70% of firms measure their compliance training in any way. Of those that do, many firms focus exclusively on whether employees have completed the training, or how many hours they have spent on compliance training. As we can see from Peterson’s example, completing compliance training may have no correlation whatsoever with compliant, or even ethical, behaviour.

In fact, an emphasis on corporate compliance may actually increase your exposure to risk.

In their book “*All You Need to Know about Ethics and Finance*”, **John Plender** and Avinash Persaud argue that,

“The attempt to legislate and regulate people into good behaviour has spawned a compliance culture rather than an ethical culture...Ethics have become something that other people in the organisation worry about, leaving everyone else unfettered by such concerns¹³.”

In other words, while compliance policies and compliance training are clearly important, they can also create a false sense of security. If employees are used to following a set of compliance guidelines dictated from “on high”, they may not spot unexpected risks or know how to respond to situations not covered by compliance policies. Compliance policies and training are certainly helpful, as well as obligatory for many organisations – but they’re no substitute for a risk-aware and ethical culture.



In the world of L&D innovation, compliance has been left behind.

The world of L&D has been transformed in recent years. Many companies have recognised that their learning programs must be agile, responsive, engaging and delivered within the workflow to accommodate today's fast-paced organisational change. As one McKinsey report phrases it:

“Organisations are acutely aware of the importance of learning in today's business environment. They understand that technology is changing the nature of work and the roles within it. They also understand that the ability of the workforce to learn new skills, model new behaviours, and adapt continuously is key to sustained success¹⁴.”

However, despite these leaps forward in L&D, compliance training is still trailing behind in most organisations – even though it is one of the most crucial forms of learning in the workplace.

For example:

- Nearly 40% of firms rate their compliance programs as “basic and reactive”¹⁵.
- After compliance training, 44% don't feel equipped to protect themselves or their company¹⁶.
- 15% click through without reading or listening to online compliance training content¹⁷.
- 34% skim read or tune out.
- 70% of compliance training is over 30 minutes long.
- The word most frequently used to describe compliance training in surveys is “boring.”

So, why is compliance training so boring?

Perhaps the most likely explanation is fear. Compliance training is so important, and the fines for non-compliance are so daunting, that organisations are more concerned with proving that compliance training has taken place than actually making sure that employees have learned anything from it.

As a result, employees perceive compliance training as little more than a “back-covering” exercise, a mere tick-box formality. Surely nothing is more boring than training that bears no relationship with your own professional development or day-to-day work – especially if the training itself has been designed by compliance officers or the legal team, rather than learning design experts.

Even the name “compliance training” is misleading. Compliance, after all, is not an end in itself. Rather, regulatory compliance is the natural consequence of a broader, more thorough risk management program - training employees in risk management, engaging them with short, high-impact learning modules, helping them to understand how risk relates to them personally, and advocating for a culture in which risk awareness is valued.

In short, compliance training is broken. To fix it, L&D teams must apply the new approach to workplace learning – digitally enabled, agile, and eminently practical – to redesign compliance training for this new era.

In the next chapter, we'll look at how to empower your L&D teams to build compliance training that actually works, and how to create a more ethical culture so that compliance becomes “just how we do things round here.”

3. Implementing a risk management program

When it comes to implementing a risk management program that will actually help to change employee behaviour, we'd argue that there are three factors to consider: your risk management training must be engaging; you must empower employees to take ownership of business risk themselves; and your L&D team must be able to support your employees with agile, adaptive risk management resources.

In this section, we'll break three key concepts into actionable steps that you can start to implement in your business today.



3.1 How to empower learners

Now, more than ever, it's time to start trusting our employees.

The COVID-19 lockdowns showed that employees are remarkably capable of doing great things under pressure. Few companies reported a drop in productivity, despite the huge strain placed on the workforce by the sudden transition to remote work and the challenging personal circumstances faced by so many.

If anything, the data suggests that employees were actually more productive than before the crisis. For example, in a large-scale survey by Great Place to Work, 87% of employees were rated as productive in May 2020 (when most were working from home), as compared to just 73% in May the previous year (when most were in the office)¹⁸.

Employees rightly feel that they have earned the trust of their business leaders. And, when it comes to protecting our businesses from risk, it may be

time to show that trust, by placing responsibility for risk management in the hands of the employees themselves.

After all, we expect people to take ownership of their personal development, their professional objectives, their own KPIs. These days, we also often expect them to be responsible for managing their time and planning their own schedule from home.

So why do we treat them so differently when it comes to compliance?

Of course, we'll still need to monitor compliance training and prove attendance. For one thing, evidencing compliance is often legally mandated.

What we're arguing for is that companies should shift their focus from *proving compliance* to *truly managing business risk*, by empowering their employees.



Here's how to create risk management training that empowers learners:



Provide compliance resources via an easily accessible next-gen learning platform or People Development Platform like Learn Amp, so employees can quickly find a handy compliance checklist when they need it, rather than trying to remember something they saw in the annual compliance training last year.



Encourage employees to ask questions and challenge the status quo if they perceive something as unethical or non-compliant.



Document and share management decisions so that all employees can help oversee and improve decision-making.



Allow employees to design their own learning pathways through compliance and risk training, so they can focus their attention on areas where they feel less confident making decisions.



Provide opportunities to apply risk-awareness on the job, such as inviting employees to troubleshoot decisions or suggest possible risks that could arise in an upcoming marketing campaign or client meeting.



Create practical, brief learning resources that focus on “rules of thumb”, instead of trying to create a guideline that covers every possible risk scenario.



Invite learners to request risk management training when they come across a situation which they're unsure how to handle; a recent example might be how to manage cybersecurity issues when working from home on a shared computer.



Nominate employees to act as “risk reviewers” for corporate communications or other potentially risky projects.

Transform your employee directory into a LinkedIn-style platform so that employees can easily reach out to the right person for advice if they're unsure if something is non-compliant.

3.2 How to make compliance training engaging

It really is possible to create compliance training that will engage your learners.

If your employees sigh and grumble whenever they hear the words compliance training, this section is for you! The good news is that making compliance training engaging for learners isn't impossible. Here are a few techniques to try:

“What’s in it for me?”

As with most learning, the secret to engaging compliance training is to show learners why they'll benefit from engaging with the material. For example:

- **Tie learning to performance.** Demonstrating familiarity with risk management, performing tasks in a compliant manner, or correctly identifying and mitigating a risk in advance should all be achievements that are recognised during 1-1 feedback sessions or performance appraisals.
- **Show the practical applications of compliance.** One example – employees could be shown that updating passwords or avoiding phishing attempts are also useful skills in their personal lives.
- **Model from the top.** Make sure that business managers model compliant and risk aware behaviour, and also praise risk awareness when they see it in employees.

Choose the right metrics

Instead of tracking compliance training attendance or completion, use more relevant metrics that actually test how risk-aware employees are, such as¹⁹:

- Assessment results on risk awareness tests, when compared to results before the training;

- Tracking whether employees who undergo compliance training become more or less rule-abiding;
- Monitor the number of employees reaching out to compliance experts with questions and concerns;
- Keep tabs on the number of times compliance or risk was mentioned as a factor in decision making.

Make the learning more enjoyable.

This should go without saying really! Yet far too much compliance training material is long, hard to read and, frankly, dull. An annual compliance training session coupled with a quick Q&A immediately afterwards is not going to drive real behavioural change. Instead, try:

- Using a consumer-grade People Development software with an engaging interface and a great user experience, instead of a traditional, clunky LMS system;
- Swapping long training sessions for bite-sized microlearning content, which many employees find easier to fit into their daily workflow;
- Using real-world testing instead of checkboxes; for instance, test employees' awareness of phishing by running a fake phishing scam and seeing how many fall for it, then directing learning resources on phishing only to those employees, rather than making everyone sit through it;
- Flipping your approach to the content – provide compliance training via short videos or reading materials, then use in-person learning time to discuss as a group and ask questions;
- Inviting continuous feedback from employees, and then using their feedback to inform and improve your compliance learning resources.

3.3 How to amp up your L&D team

The secret to great learning is a great L&D team.

To help your L&D team create compliance training that sticks, you need to give them the tools to become more agile, more responsive to market changes, and better able to create and roll-out relevant, high-impact training resources.

For an example of the impact a fully resourced and agile L&D team can have, we can look at the story of a massive US healthcare company featured in a recent McKinsey report²⁰. The 55,000-strong workforce were able to pivot almost seamlessly to remote work, thanks in large part to an L&D function which began producing and sharing online videos and learning modules on how to work from home within the first 24 hours of lockdown.

Agility isn't just important for handling crises – it's just as important to keep your employees up to speed with changing regulations in fast-paced industries. To amp up your L&D team for better compliance results, try:

- **Sourcing an L&D platform or a People Development Suite that allows your L&D people to create, upload and distribute up-to-the-minute learning resources quickly and easily.** Too many L&D teams are still struggling with unwieldy, outdated, top-down learning management systems – great for proving compliance, but bad for creating responsive learning programs. To make compliance training more effective, your team need to be able to share learning resources that tackle your employees' immediate compliance issues – for instance, updates to mandatory industry regulations, or microlearning resources on how to spot risks to data-security.

- **Open up L&D to employee feedback.** Your employees are the best people to inform L&D about what they need when it comes to compliance training. Make sure that you're listening! Set up your learning platform so that employees can share, rate and recommend learning resources to one another. Use surveys and pulse polls to sound out your employees' current awareness of compliance issues, and also find out what they think about your compliance training offering. Adapt as needed.
- **Centralize learning and knowledge in a single, accessible hub.** Keeping your business compliant isn't just about proving that employees have completed mandatory training – it's about making sure that the information they rely on in their day-to-day work is up-to-date and compliant with the latest regulations. Make sure that all your information is easily searchable in a single hub that can be readily accessed by both in-house and remote employees. Use permissions settings to keep any confidential information on a need-to-know basis.

Agile L&D in Action



Our client, Metro Bank, were able to create and roll out a digital Wellness Hub to support their employees during the first pandemic lock-down – in just 7 days!

“It was great to have a flexible system like Learn Amp in place. It allowed us to provide a greater breath of different resources. By being able to have a blend we were able to support our staff in every way we could on their terms...Learn Amp's clear interface makes using it fool proof, anyone can upskill themselves to use the platform – even if they aren't in learning and development.”

Helen Silvester,
Reward Manager, Metro Bank

3.4 The right tools for the job

When it comes to risk management, you need to get the balance right.

To protect your business and remain compliant, you need a learning platform that will help you monitor attendance and completion of mandatory training. But you also need a tool with a user-friendly, learner-led environment that will engage your employees and empower them with the resources they need, when they need them.

A digital platform can help you avoid fines and damage to your business reputation.

To protect your business and remain compliant, you need a learning platform that will help you monitor attendance and completion of mandatory training. But you also need a tool with a user-friendly, learner-led environment that will engage your employees and empower them with the resources they need, when they need them.

A flexible Employee Experience Platform will save your company and your employees a lot of time.

Companies that use a digital learning platform spend 10 hours less per week on compliance. In part, this is because employees don't have to waste time repeating material – once they've demonstrated they have retained and understood particular compliance-related learning content, they can move on to the next level of learning automatically.

Learners will also be able to direct and pace their own learning, by self-serving their compliance learning when it suits their schedule. They can create and customise learning pathways for themselves, so that they can address areas where they know they need extra guidance without waiting for the HR sign-off or management approval.

Using the right tools for compliance is particularly important in hybrid and remote organisations.

If compliance training is being delivered remotely, it becomes even more critical to make sure that everyone can easily access the content and nobody misses out on the training. A user-friendly digital learning platform is of course a must for hybrid and remote businesses. Additional features like social and collaborative learning, in-platform forums for asking questions during the learning process, and pulse surveys will also help to make sure that everyone grasps the fundamentals of risk management, no matter where they are.

We built Learn Amp with exactly this challenge in mind. In Learn Amp, we combine the reporting and monitoring functionalities of a traditional LMS with the flexibility and engagement of a cutting-edge LXP. Together with access to award-winning compliance content out of the box, our unique Employee Engagement Platform will help protect your company from risk and encourage long-term compliance.



About the Authors

About Learn Amp

Learn Amp is an integrated learning platform that makes life easy for L&D and learners. Our award-winning suite of people development tools energise L&D teams, engage learners and scale with growing businesses.

With Learn Amp, you can drive long-term engagement by embedding learning into your company culture. Our unique toolkit lets you tie learning to performance development and build a long-term alignment between your learners and your organisation.



DUNCAN CHEATLE

Aside from founding Learn Amp, Duncan has spent over 20 years championing UK enterprise through The Supper Club. Established in 2003, The Supper Club is now home to around 500 of Britain's most innovative, high growth entrepreneurs.

Duncan sits on the Chartered Management Institute's Board of Companions, was a co-founder of Start Up Britain (launched by the Prime Minister in March 2011) and was a non-exec of the Start Up Loans Company for its first year.

He has also sat on a variety of Advisory Boards, including the Centre for Entrepreneurs and the Sheffield University Management School.



JOE HILL-WILSON

Joe is Chief Commercial Officer at Learn Amp. He has spent the last 14 years helping global scale-ups in people and organisational development.

As a previous Head of L&D for a global services business, Joe is experienced in building a learning and development culture from the ground up. Working on 4 continents as a partner in a consultancy, he has developed a deep interest in how culture, ways of working and technology drive performance.

He has also been a judge for the UK Customer Experience Awards and regularly writes and speaks about the link between customer experience and employee experience.

Conclusion



Isn't it time to fix compliance training?

Compliance is essential for long-term business success – and it doesn't have to be boring.

Effective risk management depends on rethinking compliance training. Instead of offering tedious, box-checking compliance training, try:

- Using learning best practice to create a more engaging approach to compliance;
- Creating a risk aware company culture, in which risk sensitivity is recognised and rewarded;
- Implementing flexible, learner-friendly People Development tools to make compliance training accessible and relevant at the point of need.

The word “compliance” needn't make your employees' hearts sink. With the right resources, culture, and tools in place, your company's risk management program can transform from an energy drain into a true competitive advantage.

“The implementation of this learning platform has clearly raised the bar in this organisation and showed how learning culture can influence business results.”

Judges comments

from Learning Technology Award win 2020



Making work life, work better

Want to transform your business into the type
of business that everyone wants to work for?

Request a demo on our website

www.learnamp.com

References

- 1 [Gartner: Corporate Compliance Spending, 2021](#)
- 2 [HBR: Managing Risks, 2012](#)
- 3 [Iris FMP: The Cost of Non-Compliance, 2018](#)
- 4 [ibid.](#)
- 5 [Comparitech: Data Breach Analysis, 2021](#)
- 6 [Ponemon Institute: The True Cost of Compliance, 2017](#)
- 7 [ibid.](#)
- 8 [Hyperproof: Compliance Statistics, 2020](#)
- 9 [IBM: Cost of a Data Breach, 2018](#)
- 10 [Hyperproof: Compliance Statistics, 2020](#)
- 11 [HBR: Why Compliance Programs Fail, 2018](#)
- 12 [ibid.](#)
- 13 [FT: When Compliance is Not Enough, 2006](#)
- 14 [McKinsey: The Learning Function, 2020](#)
- 15 [Compliance Next: Compliance Fundamentals, 2018](#)
- 16 [Elucidat: Compliance Training Research, 2020](#)
- 17 [ibid.](#)
- 18 [Great Place to Work: Remote Work Productivity, 2021](#)
- 19 [HBR: Why Compliance Programs Fail, 2018](#)
- 20 [McKinsey: The Learning Function, 2020](#)

Make life easy for your L&D team

Our award-winning suite of people development tools energises L&D, engages learners and scales with growing businesses.

[Request a demo](#)