DeltaNet International

Essential Guide

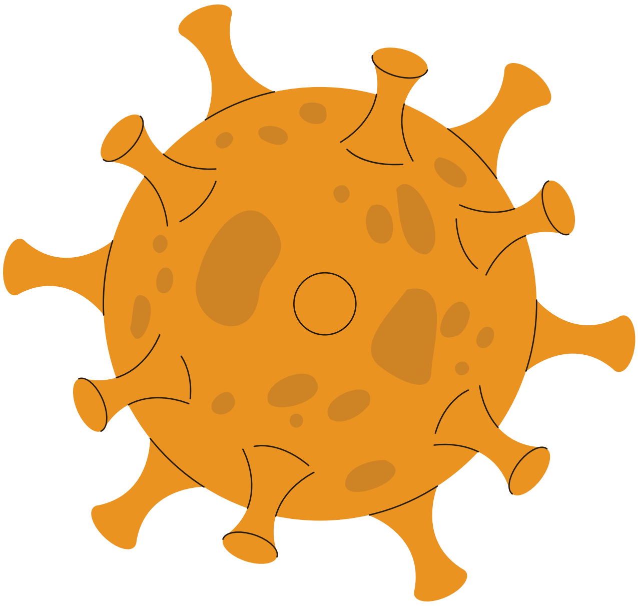
Key Compliance Challenges in 2022

Your workplace post Covid-19.

When it comes to working practices, staying safe, and remaining compliant throughout 2022 and beyond, you'd be hard-pressed not to reflect on Covid-19 and the effects of the virus across 2020/21.

Truthfully, we've seen both devastation and innovation from the business world in the wake of the pandemic – a polarising trend which shows no signs of slowing down as our tentative 'return to normalcy' forges ahead.

Equally, compliance officers across the globe continue to face new and steep challenges in their attempts to mitigate risk and protect organisations inside an ever-changing post-covid corporate landscape; one which also begs the question: 'exactly what does normal look like now?'.



As we know, 2020 saw a mass shift to remote working, resulting in a heavy reliance upon communications technologies and flexible working to keep teams operative and productive during the lockdowns.

This meant that, in 2021, businesses faced some tough questions: when to return to the office, whether to return to the office, and how to support employees' wellbeing and mental health as they battled issues like pandemic fatigue, isolation, depression, and grief.

Predictions point to 2022 as a fresh start; a new world shaped by covid-19 in the same way war and economic depression has shaped life for generations before us. We can expect organisations to implement long-term change to remote and hybrid working policies, to reinvent recruitment policies, employee engagement strategies, and talent retention practices, and to introduce or update bereavement, leave, and wellbeing policies.

Employers will need to get ahead of several covid-related compliance challenges in the coming year, including:

Work-from-home policies

In a report by Findstack.com, 77% of workers say they're more productive working remotely and most indicate a strong preference for working from home for at least part of the week. It's fantastic that so many organisations have seen no loss in productivity with the 'big shift' to home-working, however it will still be important for individual businesses to continually assess the success of home and hybrid working in the months ahead.

For example, compliance issues including how to manage and reduce the risk of misconduct and discrimination whilst working remotely will need to be addressed, as will ways to mitigate the extra cyber-security vulnerabilities that come with a shift to working purely online, in the Cloud, and away from office-based network perimeters. Employees will also find themselves with more bargaining power to request flexible working in a job market offering plenty of opportunities for it.

Strategic returns to work

For employees returning to the office in either a hybrid or full-time capacity, new and updated risk assessments for the building will need performing and changes implemented accordingly (changes may include new air filtration systems, additional cleaning resource, limiting staff numbers, and new office layouts). Both the HSE and GOV.UK have issued guidance for businesses in this respect, however organisations would do well to also consider the emotional and psychological impact of returning to the office for employees too.

Employee wellbeing

Employee wellbeing is a top priority now more than ever, according to Deputy CNO Duncan Burton. Therefore, employers should remain mindful of how to promote greater wellbeing as part of their duty of care towards employees, helping teams reconnect and stay in touch when working remotely (or after furlough) and offering awareness training on anxiety or stress-related ill health and other wellbeing concerns. We do not yet know exactly what the full mental health impact of COVID-19 will be, although early research into the health impacts of lockdown including findings of fatigue, musculoskeletal conditions, poor work-life balance, reduced exercise and increased alcohol consumption.

Mandating vaccines

Across the UK, there has been more than 100 million Covid-19 vaccinations, with just a small percentage of UK adults choosing not to be vaccinated (about 10%). The Government made headlines recently when it announced all frontline health and social care workers in England would require vaccinations by April 2022, leaving workers in other industries to wonder whether their employer would follow suit and mandate the vaccine.

Whilst it's true that employers cannot force current employees to receive the Covid-19 vaccination, many might consider introducing new measures for recruitment or renewal of contracts that require the vaccine from here on. Reasons for doing so could include protecting vulnerable staff members or limiting absences from work. Whatever way employers decide to go about implementing a vaccine policy, though, it's something that needs to be considered carefully in order to avoid facing discrimination claims (say, if refusal for vaccination is on disability, religious or philosophical grounds).

Hiring and retaining staff

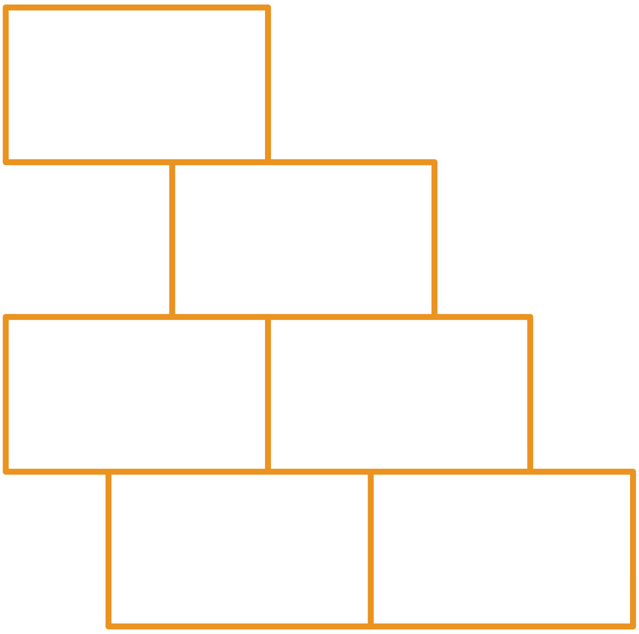
The easing of Covid restrictions and reopening of various sectors has seen the jobs market firing on all cylinders recently, with demand for workers rising across all job categories. Indeed, according to research from recruitment firm, Hays, 80% of organisations are planning to take on more staff over the next 12 months, meaning that employers are likely to feel the effects of a rather unprecedented skills shortage. Extra care from employers will be required to retain top talent who may otherwise be tempted by bigger and better offers elsewhere.

Additionally, organisations may want to revisit employee experience, re-skilling/up-skilling opportunities, and adopt a more flexible approach to recruitment (hiring talent from further afield to work remotely, e.g.). Of course, this will mean balancing the pros, cons, and compliance risks of doing so carefully.

Building and maintaining a compliance culture

Even organisations that had successfully built and maintained a strong compliance culture pre-pandemic may find these efforts need to be redoubled or altered in light of new (and likely permanent) working arrangements. Instilling a strong culture of compliance whilst some teams work remotely, others hybrid, and others are office-based is a new challenge for compliance officers and, as such, organisations' compliance teams need to leverage all the tools at their disposal to keep compliance top of mind and non-negotiable.

Immediate adjustments that can be made to ensure awareness about compliance doesn't fall by the wayside is to make compliance resources accessible virtually, to reach out to employees to discover some of their frequently asked questions about remote compliance, and to introduce compliance refresher training. Even bite-sized refresher programs can be enough to keep compliance issues fresh in everyone's minds and keep employees engaged and proactive.



Best cybersecurity practices

Cybersecurity has long since been a top compliance priority for businesses and yet – despite global technological progress, increased computer literacy, and investments in security software over the years – cyber-attacks continue to blight organisations and breach data protection measures.

Of course, new cybersecurity vulnerabilities arose out of the pandemic and subsequent shift to home working for many of us. Employees using personal devices for work (or vice versa), or generally exhibiting a more relaxed attitude to cyber-hygiene at home (away from the safety of their employer's firewalls, IP blocking, and other security software, e.g.) gave cyber-criminals a unique opportunity to strike – one which was certainly taken advantage of.

Indeed, according to a recent government survey, 4 in 10 businesses (39%) and more than a quarter of charities (26%) report having suffered cyber security breaches or attacks in the last 12 months. Phishing scams which target businesses are also on the rise, in fact, most data breaches begin with a phishing email, with around 94% of malware being delivered via email according to Verizon's Data Breach Investigation Report.

Additionally, 2021 saw the cost of data breaches rise globally, indicative of a worrying trend for businesses in coming years as cyber-attacks are likely to continue increasing in both velocity and scale.
To get ahead, businesses should take a proactive approach to cybersecurity challenges, including:

Keeping a finger on the pulse and being responsive
Bolstering cybersecurity is a continual undertaking for organisations and an important step in the process is to stay abreast of the latest news, industry insights, and up-to-date statistics around cyber-crime and data leakage. Cybersecurity statistics have an empirical value for IT risk owners as they can point to knowledge or training gaps within their own organisation and alert compliance managers to growing or urgent threats. The challenge, of course, will be to translate this information into practical and agile risk management strategies and security solutions.

A good idea is to test new threats to systems in-house to see whether existent security protocols would hold up against them and make any necessary changes uncovered a result. Business should also ensure they have a trusted backup of their key systems and a viable recovery plan in place should those systems be compromised.

Implementing cybersecurity awareness training for remote workers

Many experts recognise cybersecurity awareness training as a key tool in preventing data breaches – a truth that's even more important for organisations that have implemented some form of remote working long-term. This is because, whilst our internet connections at home are likely to be secure, most people simply don't have the same caliber IT security tools as their workplace at home. Likewise, if employees are working from their local café, train station, or hotel room – or indeed from any unsecured public Wi-Fi network – the risk of security breaches rises rapidly.

Continuous awareness training is imperative when it comes to battling the sort of errors in judgement cyber-criminals hope we'll make, particularly when we're working from home and might feel more relaxed. Hackers count on the fact that it's far easier to make an error in judgement, e.g., clicking on a malicious link, connecting to evil twin Wi-Fi, or using and re-using weak passwords when working remotely. This is because – even though we're all well versed in the dangers of these things – without continuous awareness training to keep threats fresh in our mind, it's all too easy to let complacency or absent-mindedness creep in, particularly away from the formal working environment.

Increasing phishing awareness training

As if dealing with the pandemic hasn't been tough enough for all of us, the number of phishing emails aimed at businesses drastically rose throughout 2020 and 2021. Cyber-criminals are getting more efficient too; they have bigger and better technology at their fingertips (in fact, there's an increasing number of 'out of the box' phishing attack kits available to buy if you know where to go) which means improved technical resources to run scams more effectively, with more volume, and across multiple platforms.

The truth is, most employees don’t believe they will fall for a phishing scam – after all, we spot and avoid them several times a week. However, it only takes a momentary lapse in judgement or a distracted mind to fall victim. When we're at work, we're much more likely to feel busy, stressed, and otherwise engaged, and that's what the criminals are counting on: it only takes one click.

To mitigate the risk of falling foul of a phishing attack, organisations should implement regular phishing awareness training (and refresher training) for employees. These learning interventions needn’t take long, in fact microlearning has shown to be effective at keeping learners engaged with core compliance messages, and businesses can always test their training efforts using a phishing simulator tool.

Wellbeing and mental health

Whilst it’s encouraging to see many organisations tackling mental health issues at work and making movements to better support employees’ wellbeing, there’s still big strides for businesses to make in this respect.

Recent research by the ONS revealed that around 1 in 5 (21%) adults experienced some form of depression in early 2021 – an increase of 19% since November 2020, and more than double that seen before the pandemic (10%).

It’s important for employers to prioritise issues like wellbeing and mental health, both as part of their duty of care towards members of staff, but also because it’s good for business. Happier, healthier employees are more resilient, more productive, and more engaged with the company and its goals. Fostering wellbeing can also reduce sickness absence (bearing in mind a staggering 70 million working days are lost each year due to mental health problems), help retain staff, and contributes positively to your overall compliance culture.

Worryingly, the latest findings by Mental Health First Aid (MHFA) England found that a quarter of employees had not received a mental health check-in since the beginning of the covid-19 pandemic, and 29% of those surveyed said they have never had a conversation with their line manager about mental health.

Below are some key areas to consider, helping to ensure your organisation doesn't drop the ball when it comes to employee wellbeing:

Create a wellbeing culture

Workplace wellbeing refers to our overall work-life, including aspects like our general health and happiness, our daily tasks, changing stress levels, and the work environment itself (whether this is home, the office, or both). It refers to the ways our work-life can affect our emotions and mental health, as well as any physical health effects from working, such as aches and pains from lifting or sitting, or requiring regular eye-tests for screen use.

A positive wellbeing culture helps employees to reach their full potential, maintain productivity and creativity, and build solid relationships with coworkers. It also helps employees to manage any unexpected challenges and stresses that come along. Building this type of culture means talking openly with employees about their health and wellbeing and destigmatising mental health issues.

Leadership styles, workplace policies and procedures, and perceptions of what is valued, rewarded, and penalised all contribute to the formation and reinforcement of cultures. As such, it's a good idea to task your people managers with finding out employees' thoughts on wellbeing issues and to ask about any longstanding concerns or worries that arise throughout the day. Organisations might also conduct a survey or questionnaire or assemble a group of employees from various departments and levels in a meeting to discuss these topics, forming a wellbeing strategy around the results.

Once established, new cultures of wellbeing must be nurtured over time. Think of your wellbeing culture not as a destination, but a constant journey and striving for improvement. Remember, culture is not just an HR responsibility, but requires buy-in and behavioural modelling from everybody, particularly senior management.

Training, training, training

The relationship between managers and their team members is key for the health and wellbeing of the whole organisation. Managers who can support the mental health of their teams are far more likely to have thriving, productive, and happy teams. That’s why it’s so important to train people managers on matters of wellbeing and mental health, giving them the skills to facilitate conversations with employees on these topics and spot any red flags, such as drug use or unmanageable levels of stress. Managers should be trained in the types of support available for employees, understand the steps to access any wellbeing initiatives, and have easy access to any materials they might need.

Additionally, all employees benefit from some form of wellbeing training, helping them to deal with mental health issues including depression, stress, and anxiety and educating them in other forms of self-care, such as nutrition, online wellbeing, and healthy sleep habits. Providing wellbeing training for your employees can help them recognise if and when they need help, and where to go if they need to seek such help. Learning more about mental health and associated coping mechanisms can also greatly help employees who may be suffering from feelings of shame or isolation.

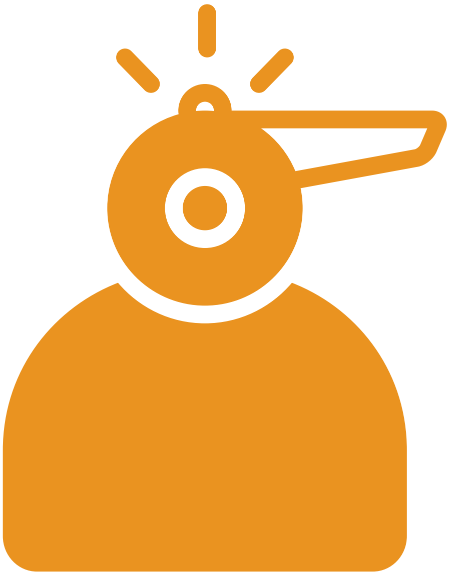
Remember to check-in

It may sound simple but checking in with your employees and colleagues to find out how they're doing is important. Many employees are used to simply replying "I'm fine", but line managers should be concerned with getting to know their team well enough to judge the authenticity of these replies. Sometimes respectfully showing due concern and care is all it takes to help people open up, helping to prevent stress, burnout and conflict.

Whistleblowing

Whistleblowing - and the way organisations handle the practice – is an incredibly important element of your compliance programme. The dos and don'ts for your company may well be laid out in black and white inside your code of conduct (making-up the legal or ethical framework for behaviour that employees are asked to follow). However, it's what happens after an individual reports misconduct that can really make or break your compliance culture.

Employees need to know whether the company will listen to whistleblowing and take it seriously? Will the reporting employee be protected by the organisation? Will there be consequences for the non-compliant behaviour? If so, what are they? These are the actions that characterise the true values, principles, and ideals of your organisation, and it's via this 'tone from the top' that trust in compliance, transparency, and ethics – in doing the right thing, for the right thing's sake – is fostered.



In order to build and maintain a culture wherein whistleblowers feel safe to raise concerns, and where the culture encourages taking matters of compliance seriously, it's important for organisations to offer training in this area, familiarising employees with what whistleblowing is, why it's so important, and their rights and responsibilities as would-be-whistleblowers.

Employees should feel safe in raising any concerns through the proper channels and need to know that no negative repercussions will develop following these actions. Additionally, for employees who witness misconduct and wish to report it, it's imperative they understand their role is to report, not investigate, any wrongdoing.

Comprehensive whistleblowing training should also cover the following:

- Why the policy exists – stress that your business encourages employees to speak up about misconduct and that the management team is ready and eager to address any and all concerns, with an open-door policy.

- What should be reported – give examples of misconduct and other types of concerns that ought to be reported. These may include fraud, bribery, corruption, modern slavery, harassment, theft, and so on.

- How to submit a report – it's always a good idea to offer employees more than one way to whistleblow, so they can choose the method they feel most comfortable with, i.e., face to face, phone hotline, or digital submission. Ensure your employees understand that their reports can be sent anonymously (and will be kept this way) and give examples of the type of information that is helpful to investigators.

- Anti-retaliation measures – training upon this topic should stress the ways whistleblowers will be protected from retaliation and highlight that any form of retaliation will count as a separate case of misconduct for the perpetrator.

Continued awareness training

Designed to keep key compliance messages fresh in the minds of employees, one of the best defenses organisations have against compliance breaches is to offer continued awareness training across relevant topics to members of staff.

In fact, it's hard to overestimate the importance of awareness training as a tool to instill knowledge and confidence – one that is about so much more than regurgitating legislation, pushing policies, and ticking a box once a year.

Awareness training is about empowering employees and equipping them with the right skills to handle the requirements of regulation as these affect their daily work tasks. Ensuring employees are kept up to date on best practices and are able to identify risks has many business benefits (it's not just a matter of avoiding the consequences and penalties of non-compliance!), including protecting individuals and stakeholders and helping the business succeed.

Awareness training helps members of staff to flourish and be productive at work because it helps clarify their responsibilities and the boundaries surrounding these. Done well, awareness training can also serve as a driver for long-term behavioural change, underlining values such as fairness, consistency and vigilance - characteristics which can be leveraged in the business setting and applied elsewhere to create high-performing, motivated, and ethical teams.

Key considerations about awareness training include:

Roll out and campaign launch

The secret to engaging people with compliance is to make training applicable to employees' roles. During roll-out, ensure members of staff understand how this training is relevant to their responsibilities and from their perspectives. It's also crucial that learners understand why the training is important to the company at large and how their participation will positively affect the organisation's goals. Aligning training launches with events in the news is often a good motivator too, helping employees to understand how they can pitch-in, towards a greater common goal.

Organisations may also consider underlining their training launch with offline compliance materials, e.g., posters, leaflets, and video screens highlighting key messages from the training, and by asking managers to announce and reaffirm the training in meetings.

Microlearning

Microlearning is a powerful training technique in the world of eLearning, and it can be leveraged in all sorts of ways to make compliance awareness training more relevant, less cumbersome, and much timelier.

Microlearning is a way of condensing information and key points into short, specific 'bursts' of knowledge that are usually only a few minutes in length. Its compact and highly-relevant nature means that learners are less likely to suffer from learning fatigue and much more likely to slot a slice of refresher training in-between tasks or 'just in time', when the knowledge gap appears in the flow of work.

More than this, microlearning is modular as well as scalable. This means it's easy to update or replace the content of microlearning courses regularly and that different microlearning courses can be pieced together or swapped out to make longer, more personalised learning interventions that address individual gaps in knowledge.

Adaptive learning

Adaptive learning is an educational method that uses artificial intelligence to present users with individually customised learning programs. It works by gathering data before, during, and after the learning process and using this information intelligently to create optimised learning paths for each user. This means, as the user continues to complete more awareness training and take more assessments, the adaptive platform is able to identify and feed them content of particular relevance (based off previous performances, learning preferences, engagement times, and so on). In other words, adaptive learning platforms can automatically and intelligently determine which learning content, activities, and techniques will benefit the learner most and provide the best learning results.

Whilst it still bridges important knowledge gaps when it comes to compliance, adaptive learning doesn't devalue employee time by forcing them to complete unnecessary training. Naturally, this has the benefit of increased engagement levels and higher morale.

Gamification

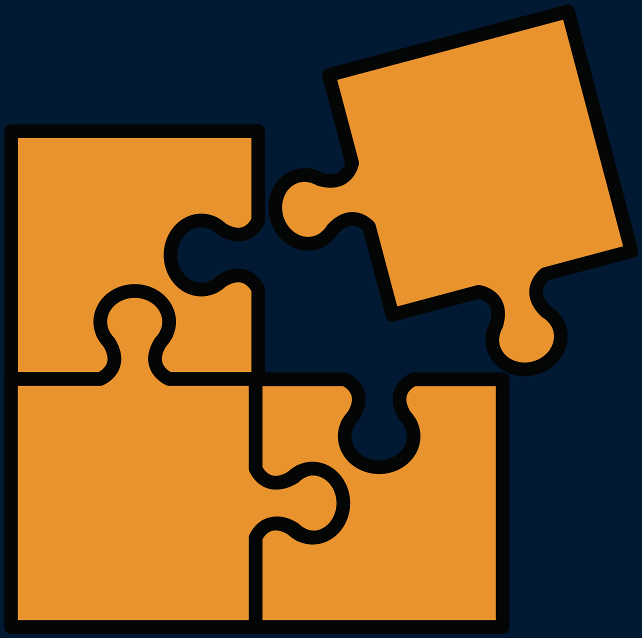
Gamification exploded onto the eLearning scene years ago, but is still a hot trend when it comes to increasing engagement, motivation, and retention levels with learners. When used inside compliance training programs, gamification offers a strategic, integrated approach that makes learning more fun. Elements of game-design (e.g., point scoring, competition, themes, rewards, and so on) are appealing to users who might not relish the idea of learning about regulation but could enjoy the concept of 'leveling up' a whole lot more.

The key with gamification is to make learners feel like they're moving vertically through 'achievements' rather than horizontally pawing through the same old exercise. With gamification, there's an 'end goal', something constructive to strive towards in a relaxed, non-threatening environment.

Keeping things interesting

Employing educational diversity in the form of different learning styles and design techniques can help accommodate diverse learning preferences and, thus, ramp up engagement for your awareness training. Compliance programs can benefit from incorporating multimedia; think videos, animations, infographics, interactivity and audio cues – all of which help to avoid monotony and add variety into your learning interventions.

Furthermore, utilising immersive eLearning is a great way to bring compliance modules to life and contextualise them by placing individuals into virtual, interactive learning environments that simulate real work-place scenarios. Immersive eLearning is a safe, inexpensive way for users to learn from their mistakes and for organisations to check their employee's understanding of certain compliance measures. Another option is scenario-led learning (also known as problem-based learning), which combines online training with story-telling techniques, independent-thought, and analysis to encourage learners to use information and apply it to their decision-making process.



Asking for feedback

Online surveys, questionnaires, and polls can provide an opportunity for your learners to share their opinions and voice any concerns about their training. These are all valuable insights into the way your awareness training program has been received and is a great way to uncover areas in need of improvement. Asking for feedback also helps employees to feel more involved in their own training and thus more engaged when it comes to future learning interventions.

Measuring performance

xAPI is an eLearning software specification that allows learning content and learning systems to speak to each other in a manner that records and tracks all types of learning experiences. This means it's great for collecting plenty of useful data to help measure performance and can be compared and contrasted with changing employee behaviours and other compliance tools (e.g., phishing simulations) to measure the effectiveness of your awareness training.

Fraud awareness

Fraud is a serious criminal offence, with consequences ranging from fines to imprisonment. Unfortunately, close to 4 in 10 organisations (39%) experienced an increase in fraud throughout 2020 (according to BDO's Fraud Track Survey), while three quarters (76%) of business owners and directors believe their company is more exposed to fraud since the Covid-19 pandemic began.

Indeed, many of us will recall receiving fraudulent emails and text messages from criminals last year, often claiming to be services such as the NHS (offering the opportunity to book vaccines or receive PPE, e.g.) or delivery companies (claiming we had missed a package and must input details to book re-deliveries).

Throughout 2021, a type of fraud called 'account takeover' led the pack when it came to sheer number of attacks recorded – this is a form of fraud that involves criminals accessing the victim's login credentials in order to steal data and/or money. In this scenario, criminals immediately change the account's original password, making it difficult and time-consuming for the legitimate account owner to take back control.

Sadly, criminals continue to use every opportunity to exploit vulnerabilities and commit fraud against individuals and organisations, and this includes taking advantage of companies that implemented remote working models in 2020 and 2021 (as this posed a challenge for real-time monitoring and direct communication to take place).

Employees working alone are more vulnerable to exploitation by fraudsters as they may not realise that fraud has taken place before it is too late.

In coming months, organisations must ensure that their anti-fraud controls remain responsive and are robust enough to mitigate risk when it comes to the changing face of work post-Covid.

Watching out for the following types of red flags and ensuring employees have continuous awareness training about these warning signs can help prevent fraud at your organisation:

Behavioural red flags

- Employees consistently working longer hours than their colleagues for no apparent reason and who are reluctant to take time off.
- Employees who are secretive about their work and delay giving information.
- Employees with a sudden change of lifestyle and/or social circle.
- Employees under apparent stress without identifiable pressure.
- Aggressive or defensive employees who break the rules and are subject to complaints.
- Employees with new and unusual relationships with other people or departments.
- Employees who request significant detail about internal audit scopes or inspections.

Financial red flags

- Poorly reconciled cash expenses/customer accounts, or large numbers of refunds to customers.
- Unexplained rising costs, or costs that are not in line with increasing revenue.
- Employees under external financial pressure.
- Employees who appear to make many mistakes leading to financial loss through cash or account transactions.
- Employees who are inexplicably better off, or there are concerns that they are top performers (e.g., sales) through suspect activity.
- Employees with competing or undeclared external business interests.
- Employees who submit inconsistent and/or unreasonable expense claims/unusual transactions, or inter-account transfers (even for small amounts).

Procedural red flags

- Prospective employees who are reluctant to provide background information or who provide inaccurate or inconsistent information.
- New employees with knowledge of industry procedures without experience disclosed on their CV.
- Employees making procedural or computer-system enquiries inconsistent with or not related to their normal duties.
- High numbers of customer complaints.
- Customers or suppliers insisting on dealing with just one individual.
- Managers avoiding using the purchasing department.
- Tendering to only one or the same supplier.
- Poor engagement with corporate governance philosophy.
- Too much delegation by senior managers without proper review procedures.

Data Protection

Data protection has always meant serious business for organisations, particularly since May of 2018 when the European Union introduced the biggest overhaul of privacy regulations in decades, the GDPR. The GDPR was introduced to harmonise data privacy laws across all EU member states, as well as provide greater protection and rights to individuals living and working in the digital age.

Post-Brexit, on 28th June 2021, the European Commission adopted an adequacy decision for the UK, demonstrating that it believed the UK offered an 'essentially equivalent' level of data protection to that within the EU, namely the UK's implementation of GDPR, the Data Protection Act 2018 (DPA 2018). This meant personal data could once again flow freely from the EU to the UK – at least until 27 June 2025, when data adequacy may or may not be extended.

For organisations within the UK, then, complying with the DPA 2018 involves implementing data controller / data processer agreements or contracts with your clients (particularly if you work with or process data from EU citizens). It also means complying with the GDPR's seven principles of data protection, which the DPA 2018 has adopted.

These involve continuing to:

- Process data in a manner which is lawful, fair, and transparent and which maintains the data subject's rights.
- Process data only for the purpose it was collected – if your purpose changes over time, or you have a new purpose which you did not originally anticipate, you may need to seek new consent for processing data.
- Limit the storage of data only to that which is strictly necessary and relevant. In the case that excessive data is (or has been) collected, the data should not be used and should be deleted securely.
- Maintain data records which are accurate and up-to-date. Where any personal data is found to be inaccurate, reasonable steps must be taken to ensure that such inaccurate data is deleted or rectified without delay.
- Store personal data only for as long as is necessary. Under GDPR, organisations must not keep hold of personal data 'just in case'.
- Process and store data with integrity. Every reasonable measure should be taken to maintain the security and confidentiality of data and to prevent unlawful processing, loss, destruction, or damage of data.
- Maintain a culture of accountability. Data controllers are responsible for and must be able to demonstrate compliance with, data protection laws.

Continued data protection awareness training will help keep the principles of data protection fresh in the minds of employees and help to reduce human error. Remember, in order for awareness training to be effective, it must focus on how the DPA 2018 impacts employees' job roles in practice.

Paying attention to employee behaviour, rather than their knowledge about legislation alone, will also help organisations decide when and which refresher training to administer (i.e., where behaviours indicate there are gaps in knowledge that pose a breach threat).

Data privacy post Covid-19

As we know, the fight against Covid-19 meant many businesses switched to remote and hybrid working practices quickly; an action which uncovered a new set of data protection risks that some organisations may not have been prepared for.

To counter these risks, organisations may wish to develop and implement procedures for the protection of personal data as part of remote work specifically, including regularly reminding employees about best practices for processing, storing, and sending information. This might include refresher training about the use of inadequately secure messaging apps or social media platforms, the transfer of data from home to office, or the importance of not using private devices (with no antivirus software, out-of-date operating system software and applications, no encryption solutions, etc.) for work purposes.

Additionally, whilst we understand it may be necessary for companies to continue to take certain public-health measures in coming months, organisations must also balance this responsibility with individuals' personal data-protection rights. For example, many companies are collecting information from members of staff, e.g., whether they have self-isolated or self-quarantined, or are using device location data to track the spread of the virus. Remember, under GDPR and the DPA 2018, this data is considered personal data and therefore must be protected according to the usual directives. This will include only collecting as much data as is necessary, maintaining a legal basis for processing this personal data, and remaining transparent by informing affected individuals about the use of their data.

Climate change

Prior to The 2021 United Nations Climate Change Conference (commonly referred to as COP26) the UK announced it would become the first G20 country to pass legislation mandating climate change TCFD disclosures for Britain's largest companies and financial institutions.

TCFD stands for 'The Task Force on Climate-Related Financial Disclosures', an environmental reporting group comprised of 32 members which aims to standardise ESG reporting, in particular the financial impact of climate risks across industries.

By April 2022, when the new requirements come into effect, over 1,300 of the UK's top registered businesses will be asked to publish climate-related financial information. Many of our largest organisations, including banks and insurers, as well as private businesses with over 500 employees and a turnover of £500 million, will be included.

Originally launched back in COP21, the eventual adoption of TCFD disclosures by large UK businesses in 2022 will help to ensure that the world's largest corporations are taking their responsibilities about climate change seriously. These organisations will have to develop emission reduction strategies and sustainability programmes in earnest, finally doing more than just talking about the UK's net-zero obligations.

Looking ahead

The new legislation is set to be one of the most important ESG-related mandatory disclosure rules ever enacted. The European Union is moving forward with its corporate due diligence and corporate accountability legislation, which necessitates organisations to identify, address, and mitigate their impact on human rights and the environment.

Whilst these regulations are not likely to take effect immediately - perhaps requiring several years to come fully into force – it's nevertheless an important compliance consideration for us today. After all, the UK already has a series of piecemeal ESG-related disclosures mandated, including equal pay disclosures and requirements for strong compliance programmes for governance issues such as bribery and tax evasion.

Additionally, the G7 Finance Ministers and the G20 Sustainable Finance Roadmap established the Taskforce on Nature-related Financial Disclosures (TNFD) in 2020. Given that nature accounts for more than half of the world's economic production, the project aims to secure and protect the natural environment.

Currently, the TNFD lacks enough data to understand nature's influence upon their immediate financial performance or longer-term financial risks. However, with obligatory disclosures, TNFD hopes to improve this. Given the UK's support for TCFD, TNFD is bound to follow suit in the near future.

Money Laundering, 6AMLD, and Brexit

It is estimated that money laundering activities in the UK equate to approximately 2-5% of GDP. This means that between £36-90 billion of criminal finances are laundered through the UK economy annually. Criminal finances can be generated through organised crime, individual criminal activities, and high-end money laundering schemes – but all of these impact businesses, individuals, and communities in a negative way. These activities also put national security at risk by financing terrorist activities, armaments, and nuclear weapons.

Following 4MLD in 2017 and 5MLD in 2020, the Sixth Money Laundering Directive (6AMLD) was transposed into EU law in December 2020, with firms having until June 2021 to implement the changes. 6AMLD was intended to improve clarity and harmonisation among EU member states, but it also increased member states' reporting duties (since money laundering continues to go widely undetected).

Unlike 5AMLD, the UK did not transpose 6AMLD into its domestic AML framework following the country's withdrawal from the EU in January 2020. The key reason for this decision being the government's understanding that the UK's anti-money laundering systems are already compliant with many of the 6AMLD rules – in fact, the government believes 'the UK already goes much further' in many respects.

UK AML rules, for instance, already enforce longer sentences for certain money laundering offences (including imprisonment of up to 14 years in some cases) and UK law does include broader provisions relating to predicate offences than the specified crimes that qualify as predicate offences set out in 6AMLD

There is one area where the UK does not meet the standard of 6AMLD, however, and this is the issue of corporate liability for the failure to prevent money laundering.

Under 6ALMD, criminal liability is extended to individual 'legal persons' if they fail to exercise control or supervision which consequently allows money laundering to take place. Some of the sanctions and penalties following this new criminal liability include criminal or non-criminal fines, but Article 8 also lists other punitive sanctions, e.g., being disqualified from the practice of commercial activities (temporarily or permanently), going under judicial supervision, or the closure of the organisation used for committing money laundering.

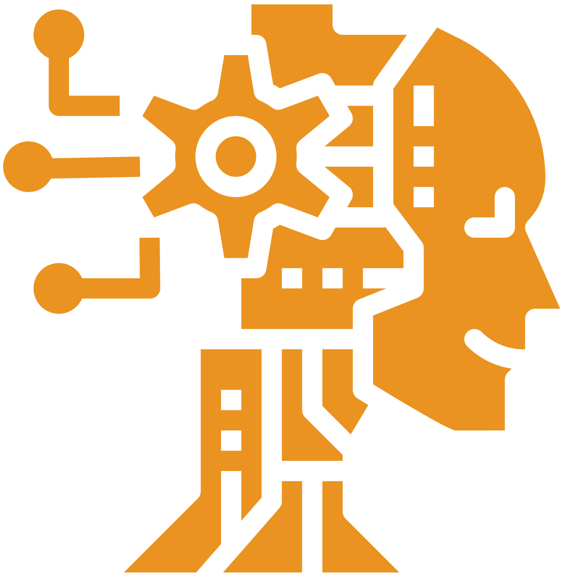
It's true that the principle of corporate criminal liability does exist under UK law, but it remains to be seen whether it will be expanded to include a 'failure to prevent' type offence. Objections from various organisations on this matter include the risk of 'putting too much pressure' on already highly regulated, controlled industries.

Artificial intelligence

Ever a hot topic, the transformative power of artificial intelligence (AI) is widely considered to be one of the biggest commercial opportunities of the 21st century. Indeed, it already enhances many of our modern business functions, allowing organisations to do things like automate processes, gain insights through data interrogation, and engage with customers and employees seamlessly.

Of course, AI is also useful for risk management and compliance functions since both these operations rely on information and analysis by design. That is, they involve collecting, recording, and processing a significant amount of data and, as such, are particularly suited for deep learning (a type of machine learning that imitates the way humans gain certain types of knowledge, and also the dominant paradigm in AI).

Artificial intelligence and machine learning technologies are incredibly powerful, but expectations must not exceed reality in this sense. Indeed, in the coming months and years, organisations hoping to leverage AI across various functions will need to remain vigilant as to the new types of risks this involves. AI can, for example, amplify bias (say, in hiring practices or consumer advice), breach data privacy or use laws, or pose cybersecurity threats by allowing for faster, better targeted, and more destructive attacks to take place (although, it can be used to counter cybersecurity risks too).



Business leaders, it seems, will ultimately face one fundamental challenge when it comes to AI: finding a way to utilise its benefits without creating unreasonable compliance and risk issues.

To mitigate the risks AI can introduce, it may help organisations to:

- Monitor and document AI solutions – Organisations should remain aware of the types of data its AI functions are analysying in order to make decisions and whether this data could have any considerable or unfair impact (e.g., when it comes to equal opportunity).

- Assess compliance within AI functions – Understanding which types of data AI is using to reach its outcomes means that organisations can also assess the technology's compliance with relevant legislation and organisational codes of conduct.

- Encourage cross-department collaboration – Artificially intelligent technology is still in its infancy, meaning that few possess the expertise necessary to install and manage its systems. For this reason, it's important that organisations ensure technical IT teams are continually collaborating with risk managers about their use of AI. In order to be effective, each team must provide the other with appropriate information and expectations in a straightforward manner.

The road ahead

As the list of regulatory compliance challenges facing companies continues to grow it's worth remembering that, whilst no technology offers a cure-all solution for compliance managers, well-implemented and measured AI solutions can improve business processes substantially.

Additionally, with fines for non-compliance increasing year over year, and increased reporting duties in many industries, any technology that can reduce false positives, reduce costs, and address human error offers a valuable addition to regulatory compliance programs.

Resilience and your compliance culture

The term 'compliance culture' isn't new; for years we've heard about the need for organisations to create one in order to really get on top of and mitigate regulatory risk. However, in the aftermath of one of the most significant shifts to working-patterns and change in management thinking ever seen (following covid-19), business leaders face new challenges when it comes to maintaining compliance across a somewhat world-wearied, yet more flexible, and even fully remote workforce.

In the newly hybrid/remote world of working, developing comprehensive processes and maintaining a strong culture of compliance will be crucial – especially as we are not out of the woods yet when it comes to covid-19. This starts with encouraging an organisation-wide compliance-first culture. In this culture, employees at every level accept responsibility over risk management and know how to remain resilient to compliance risks, even during times of crisis.

In business, our 'culture' is the filter through which we conduct ourselves, it's the DNA that runs through the organisation, colouring its everyday operations. When we refer to 'workplace culture, then, we're really pointing to the beliefs and behaviours of the workforce at large. This is made up of the various values, attitudes, actions, and norms visible in those around us and regarding various factors in the workplace – one of these, of course, being compliance.

A team effort

We know that compliance is all about doing the right thing, the right way. It's about setting principles and standards and acting accordingly. It's not enough to have written policies and procedures (although these are important benchmarks that should be communicated clearly). A true culture of compliance will not only point to and promote such policies, then, but will also bring them to life.
In short, a compliance culture is a critical area that connects everyone and permeates every aspect of business. If it's successful, it will positively influence our vocabulary, our values, our targets (and the way we achieve them), and our interactions/transactions with those we encounter.

In order to build a strong compliance culture, organisations might consider several factors:

The Leadership Team

To form a strong compliance culture, your leaders need to do more than communicate rules to be obeyed; they must model consistently good behaviour themselves. Company leaders set the cultural tone by consistently sharing their vision, reacting quickly and fairly to non-compliance, and by celebrating when employees act in a compliant manner. Embedding systems and processes to support the tone from the top as should be considered the norm – just 'business as usual' – as this will help build your culture over time.

Training

A successful compliance culture does not view training as a ‘once and done’ exercise, but as a continual process aimed at closing knowledge gaps and upskilling employees. Equally, employees are not forced to repeat training they don’t require as this wastes time and fosters resentment and pressure. Instead, learning ought to be adaptive and personalised; it should respond to gaps in knowledge, facilitate upskilling, and always be relevant and appropriate to the employee’s job and position.

Not incentivising compliance

One of the biggest mistakes organisations make it when it comes to building a compliance culture is to incentivise it. Of course, compliance and positive behaviour should always be positively reinforced, but it’s important to remember that compliance is about doing the right thing for the right reasons – not simply to get a reward.

Incentivising compliance is a risky business because it can erode the trust and commitment that’s necessary to cultivate a true compliance culture in the first place. It doesn’t make sense to ask employees to self-regulate, to trust their instincts, and to do what’s right on the one hand, whilst simultaneously conditioning them that compliance can be bought and sold somehow. By trading compliance for favours, you muddy the message and this should be avoided.

Accountability

Compliance cultures don’t have ‘win at any cost’ mentalities, but evolve and train employees to be accountable for their own decisions and actions, building trust via consistency and transparency. Designated risk owners should be assigned to manage key-risks on behalf of the organisation and, as custodians of compliance, these individuals will have clear roles and responsibilities when it comes to the job. Organisations might also schedule ongoing feedback sessions to enhance employee accountability whilst also nuturing a no-blame culture (which can lead to employees hiding their mistakes rather than learning from them).

Monitoring

Inside a successful compliance culture, strategies are delivered to monitor ongoing compliance (think inspections, investigations, regular risk-assessments and simulations to test knowledge). Plans should also be put in place to manage and respond-to any vulnerabilities or non-compliance uncovered by these actions – whether this is further education, increased awareness training, or other disciplinary action, the goal is to discover weak links and deal with them promptly.

About us

DeltaNet International are eLearning specialists. We provide off-the-shelf and tailored compliance, health and safety, and performance training solutions to organisations around the globe, helping to raise awareness and promote positive behavioural change every single day.

Our cutting-edge, intelligent learning experience platform, Astute LXP, is designed to enhance user-experience and promote adaptive learning.

Available in over 30 languages.

Try our courses

See why over 1 million learners love our courses!

To arrange a free trial (or just to chat about your eLearning requirements) please use the information below. Don’t be shy, we’re a very friendly bunch.

Call: 01509 611 019
Email: enquiries@delta-net.co.uk
www.delta-net.com

Or scan the QR code below:

DeltaNet International Ltd
www.delta-net.com
enquiries@delta-net.co.uk
01509 611019
Suite B
The Technology Centre
Epinal Way, Loughborough LE11 3GE