

The Three Pillars of Compliance

A guide to approaching, becoming and staying compliant



Talking about compliance as an exercise - or even as a distinct process- now seems hopelessly old-fashioned.

If they ever existed at all, the days when information managers were able to “do” compliance and then forget about it for another six months are long gone.

Just as the law has changed, so too has the nature of compliance. Nowhere is this more clearly illustrated than with the upcoming General Data Protection Regulation (GDPR). For the first time, there’s an across-the-board notification duty, so if a personal data security breach occurs, the regulator needs to know about it - and quickly. Among other changes, security now has to be hardwired into your infrastructure and processes (privacy by design), while the Regulation ushers in a series of new rights for individuals - and it’s your job to ensure that these rights can be exercised.

To stay on the right side of the law, compliance is now everyone’s business: it’s not about ticking boxes, but about building a culture of compliance throughout your organisation. From day-to-day interactions with customers, through to upgrading your security measures, compliance should shape and determine your decisions across the board.

So how do you approach compliance? How do you become compliant? And how do you stay compliant in 2017 and beyond? We look at each of these pillars in turn ...






Pillar 1: Approaching data security

Integrate compliance into your risk assessment process

There has always been a marked overlap between risk management and compliance. The line always taken by legislators and regulators - whether it's the EU or our very own Information Commissioner's Office - is that a robust legal framework should be seen as a positive thing. In other words, the law exists not just to safeguard consumers, but also to make businesses better able to manage security risks.

Compliance readiness usually involves simultaneously taking positive steps to strengthen your security posture. So in this respect, it's true that there's a "carrot" element to compliance: take it seriously and you can make your business stronger.

But of course, along with the carrot, comes the stick: get compliance wrong and there's the possibility of being hit with a penalty - along with all the financial and reputational repercussions which flow from this. And with GDPR ushering in maximum fines of up to 4% of global annual turnover, that "stick" is getting bigger. All of this has the following implications:

-  **For any legal or regulatory changes, your preparation and readiness project should always involve revisiting your risk assessment.**
-  **Regulatory risk should be treated as a distinct risk category. As such, it's good practice to have a separate section devoted to it in your risk assessment. So when a new law is introduced, it's a matter of systematically going through it, identifying the obligations it places on you, and identifying the impact of non-compliance for each obligation.**
-  **More broadly, consider how the new law affects other areas of your risk assessment. This is especially relevant to your "likely impact evaluation" for specific risks. So for example, the impact of theft of data from a rogue insider might lead not just to the loss of customers to a competitor, but also to an ICO investigation.**





Compliance awareness and training must apply to the entire organisation

Compliance should not be the concern solely of your information manager or other senior staff. The reason for this is simple: even though the penalties for non-compliance fall on the organisation, it's very often the day-to-day actions of ordinary members of staff that give rise to breaches in the first place:

- ⚠️ **A customer requests a copy of all personal information your organisation holds on her. This request is regarded as very low priority by the customer service advisor and is not actioned.**
- ⚠️ **A staff member transfers unencrypted customer data from your system to a memory stick and then onto a personal laptop.**

In both of these situations, the organisation could be sleepwalking into non-compliance through the actions of its employees. Avoiding it requires the following approach:

- ⚠️ **Revisit your code of conduct and guidelines. People are much more likely to follow a rule if they know why it's there in the first place. A workable policy shouldn't just be a list of dos and don'ts; it should give the reasons why specific actions and behaviours are acceptable or unacceptable. From a compliance perspective, this means explaining the rules in a way that's easily understood - and explaining the implications both to the organisation and to the employee of non-compliance.**
- ⚠️ **Contextualised training. Compliance training becomes much more relevant and better understood if it's built around real life examples.**



Pillar 2: Becoming compliant



Refer to the guidelines

Ignorance of the law is no defence - which is why the tracking of legislation and regulatory developments is a vital part of information security management.

For the most part, big changes are usually well signposted. The ICO and industry-specific regulators are the natural first port of call for guidelines. That said, the more you are able to 'read around' the topic, the easier it comes to pinpoint the specific practical steps you need to take to ensure compliance. With this in mind - and with a major compliance shift just around the corner, our very own [GDPR compliance portal](#) is definitely worth checking out.

Solutions: approaching buying decisions the 'compliance-friendly' way

A change in the law can often provide precisely the call-to-action an organisation needs to carry out a review of its IT framework. Yet this shouldn't necessarily be seen as a limited, reactive process. An IBM study showed how the approach taken by enterprises has changed over recent years: according to IBM "Companies are realizing that simply checking the box for compliance requirements is no longer a sufficient security strategy".

Purchasing tech shouldn't just be about filling in a compliance gap. Rather, it should be about focusing on your specific business needs - and finding the solution that best meets them. It's about asking the following questions:

- 🚩 **What risks am I faced with - in terms of technical, business and regulatory risks?**
- 🚩 **Does a specific solution make my organisation better able to address those risks - and meet my regulatory obligations?**
- 🚩 **Does the solution add value to my organisation?**

Our very own offering provides a useful illustration of this. Primarily, it's designed to address a very real business risk: the potentially catastrophic loss that can occur through unauthorised insider behaviour. Yet at the same time, it features crystal clear visibility and forensic reporting capabilities: in other words, precisely the type of functionality businesses need to keep on top of GDPR's significant new reporting obligations. Compliance isn't an add-on or side concern: it's actually hardwired into the solution.

Pillar 3: Staying compliant

Compliance is an ongoing process. It demands the following steps on your part:

1

Monitoring. How successful are your attempts to build a culture of compliance? Bear in mind, an organisation's culture is manifested through the behaviour of its people. For instance, are employees continuing to play fast and loose with customer data? Are they drifting towards potentially problematic situations? Because ZoneFox is concerned with behaviour, it's the ideal solution for helping you detect telltale signs in this area.

2

Stress testing. You are of course under a duty to check regularly that your security processes remain appropriate to address the specific risks you are faced with.

3

State of the art. Laws and regulations are built to last: they tend to be worded in deliberately general terms - leaving the onus on you to ensure you are following best practice at any given time. A proactive approach is key here: the need to constantly survey the state of the art to ensure your framework is still fit for purpose.

The good news is that the [ZoneFox Compliance Reporting feature](#) will help make becoming and remaining GDPR compliant simpler- and breach reporting less complex.

Compliance Reporting has been built from the ground up to help you respond to, and manage, potential non-compliant activity efficiently and effectively - whether you're an IT security analyst investigating a potential breach or a Data Protection Officer responsible for incident management and stringent regulatory reporting. You can find out more about Compliance Reporting [here](#), or [contact us](#) to arrange a 1-2-1.

About ZoneFox

ZoneFox helps businesses around the globe protect their business-critical data against the insider threat. Our award-winning technology provides the 360 visibility of activities around your data – the who, what, where and when – by monitoring user behavior and data movement both on and off the network, and instantly alerting to anomalous activities.

Security posture is strengthened, sensitive information is protected and regulatory compliance is supported.

Like to Learn More?



zonefox.com



youtube.com/zonefoxvideo



[@zonefox](https://twitter.com/zonefox)



alerts@zonefox.com



40 Torphichen Street

Edinburgh

EH3 8JB



0845 388 4999

