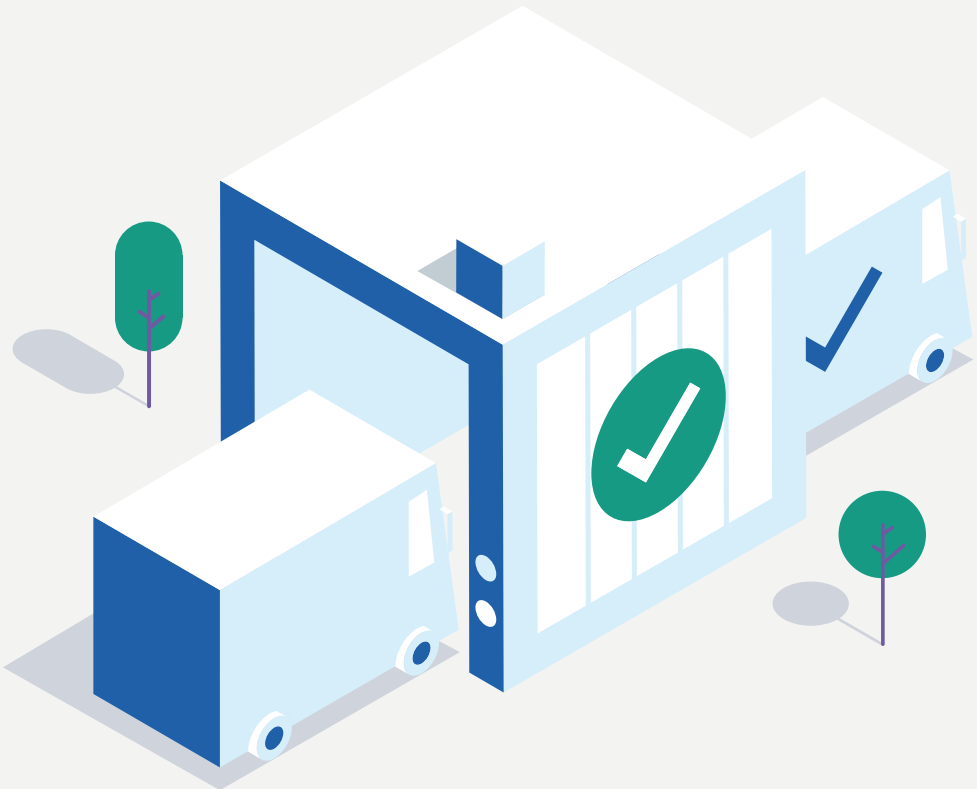
Pulsant
Business Unlimited

WHITEPAPER

Making the case for continuous compliance



Find out how we can help your organisation:
call **0345 119 9911**

Landscape

Compliance is a word that has been bandied about by business, regulators and the media for the last few decades. For those in the public sector, financial services and healthcare, it is an ever-present concern influencing the entire organisation. But for other companies, those not in heavily regulated industries, compliance has always been a bit of a challenge, unchartered territory.

In today's market the compliance question gets even trickier. Your business might not be in a constant state of change, but the compliance landscape is. A case in point is the upcoming European Union (EU) General Data Protection Regulation; the deadline for compliance is 25 May 2018. However, there is a lot of uncertainty in the market as to which companies need to comply.

Simply put, all companies must comply. Those organisations that don't actually hold personal data still need to prove it by completing a Data Privacy Impact Assessment (DPIA) on a continual basis.

Putting aside the uncertainty around GDPR, its presence has opened the floodgates, so much so that almost every organisation is asking the question: am I compliant? Do I need to be?

MORE ABOUT GDPR

The purpose of GDPR is to standardise and strengthen data protection for all individuals within the EU and the consequences of getting it wrong, either through non-compliance or experiencing a breach, will be far reaching. Companies will face significant fines, for example:

- **Up to 4% of global annual turnover or £20m**, whichever is greater
- **Up to 2% of global annual turnover or £10m**, whichever is greater

The challenge for smaller businesses or those not in heavily regulated industries is that compliance isn't necessarily already part of daily operations. Indeed, these organisations are not alone in experiencing issues.

For the most part, compliance is an organisational commitment that spans both technologies and processes. It forms part of a governance regime that embodies good practice and makes sense commercially, too.

From a technology point of view, there is the added challenge of its fast-developing nature and the effect that newer technologies like cloud are having on compliance.

And these challenges aren't restricted to the process of compliance; a key part of implementing a framework and meeting the requirements set out by specific regulatory bodies is that it is an ongoing endeavour. It's all about change and as the business transforms or grows, and the market evolves, maintaining that compliance becomes an issue all on its own.

Set against the backdrop of a cloud environment, this whitepaper takes a look at continuous compliance, how technology makes it easier, and how it can strengthen business value.

THE COMPLIANCE CHALLENGE

We are all aware of the benefits that cloud computing brings to business, whether that is consumed through a private, public or hybrid model. With almost every technology business decision having a cloud component — think business intelligence, analytics, IoT or DevOps — compliance is a major challenge for IT.

Historically, security was one of the main obstacles to cloud adoption. Today it remains a concern, one that is largely well-handled, alongside compliance. Much like with security, there is disparity in translating legacy compliance requirements into new cloud environments; a lack of maturity from IT and security teams in understanding the cloud controls that need to be put in place to meet compliance. For example, how does the ISO27001 framework differ from physical infrastructure to cloud?

There can also be technical challenges; in migrating applications and systems to the cloud, how can companies accomplish this without significantly redeveloping them? And again, what controls are needed and how do they differ from physical controls.

On the flip side, leveraging cloud technology overall can reduce operational complexities, so why shouldn't this also apply to IT compliance? With cloud you could take the data generated by multiple compliance tools and bring it all together in a single view.

Of course using cloud to monitor and control compliance brings up another question: is it really cheaper? Looking at the total cost of ownership of running security or compliance tasks as-a-service versus what you are currently doing can yield some significant savings — mostly around automating certain processes, simplified reporting and cutting down on the number of compliance and reporting tools that are actually needed. In addition, it makes your approach to continuous compliance that much more streamlined.

GETTING INTO THE CONTINUOUS COMPLIANCE MINDSET

Continuous compliance is something that many businesses are already doing in some form. However, what this typically means is manually bringing together data from multiple tools because there is no real method of making these disparate systems work together. You may have a large, capable team, but are they helping your organisation comply in the most efficient way?

This is especially important given the changing attitudes towards increased liability of compliance offers. According to DLA Piper's *2016 Compliance & Risk Report: CCOs Under Scrutiny*, 81% of compliance officers are worried about their personal liability[1].

THE IMPORTANCE OF GETTING COMPLIANCE RIGHT

According to Verizon, in the 10 years it has been producing its PCI Compliance Report, none of the organisations that suffered a data breach were fully compliant at the time[2].

Continuous compliance challenges

Size, growth and understanding remain the three largest obstacles to continuous compliance. Firstly, the sheer size of risk management and compliance frameworks are difficult to manage. Looking at something like the NIST Cyber Security Framework, for example, there are almost 400 specific requirements that need to be met. Now, if this isn't your only framework, the complexity is just magnified.

Secondly, your organisation is influenced by internal and external changes. As your business grows, your requirements change. In parallel, the market is changing around you as is the technology landscape. Your compliance framework therefore covers environments that are changing while also being influenced by external factors.

Lastly, there is a tremendous lack of understanding over what compliance actually means and what it applies to. What should you monitor? When should you do it? How do you should you report on it, and how can you prove compliance?

While these might be the biggest challenges, there are other issues. Lack of skills, for example. As mentioned earlier, IT teams may not have the right skillset to translate compliance and controls in the physical world to the virtual world. In addition, while teams might be good at manually carrying out continuous compliance, they don't necessarily have a broad industry view, an understanding of what other similar organisations see as challenges and how they are overcoming them.

THE PULSANT APPROACH

Compliance isn't a one-off task, a case of checking a few boxes and forgetting about the regulation once you've received your compliance certificate. The aim of regulation is that it is regular, an ongoing endeavour that caters for changes in the market and your organisation.

Maintaining this compliance is essentially managing this change and ensuring that whatever is going on internally or externally those boxes remain checked. Of course the idea of continuous compliance, as discussed above, is one that comes with challenges, especially when there are multiple tools, frameworks and processes involved. You need to collate data from different sources, such as monitoring, usage, audit or event-driven data that resides across multiple tools. The question is, what do you do with it? And how do you gain meaningful insight without manually generating reports and analysing the data?

A single pane of glass

The Pulsant Continuous Compliance service does just that — integrating everything you need to know about your compliance into one dashboard. The platform has been developed by cloud and security architects and validated by regulatory experts. It isn't a replacement for your existing tools; rather it supplements them by consolidating them and all the associated data sources into a single pane of glass, which aligns itself with and queries itself against a policy engine that incorporates a regulatory tool set.

Essentially, during the onboarding and mobilisation phase of any deployment we work closely with our customers gaining an in-depth understanding of their business and their regulatory requirements. This includes a full review of existing tools, as well as Pulsant's tools and rule bases. As a result, we are able to use these existing tools and our own to create a bespoke platform with policies relating specifically to certain regulations or company mandates that must be adhered to - in effect, helping our customers to optimise their existing investment. The high levels of customisation ensure businesses can effectively bring together and leverage all data sources from that single dashboard.

How do we do it?

There is a significant amount of overlap between various regulatory frameworks, which means that if you're compliant with one, the chances are meeting compliance on the next one, won't be as complex. Especially if you are using a technology platform to help you.

One of the key elements of a framework like ISO27001, for example, is encryption of data 'at rest'. Data is encrypted while on disk and then decrypted when someone with the right permissions accesses it. In this way, the platform creates a policy to ensure the data is decrypted on the way to the reader. Now, if you are completing GDPR compliance where there are similar data-at-rest encryption requirements, they can be incorporated into the policy with a slight change. The process makes use of the same technology and the same platform, just with a tweaked parameter.

The result is a compliance monitoring platform that combines data sources from across the organisation to ensure your business is compliant (and remains compliant) with the necessary regulations.

MONITORING AT A GLANCE

The platform's rules are very flexible and can be easily set up to enforce any compliance statement or requirement by leveraging our proprietary domain specific language.

We maintain a dynamic configuration management database (CMDB) that tracks your infrastructure and triggers alerts in real time. Using pre-defined rules and bespoke policies, the platform continuously pulls information and checks it against the controls it has in place to identify any instances of non- conformities. If something is flagged, a notification is proactively triggered to inform relevant stakeholders. In addition, any changes to your infrastructure or software could be set up to be monitored, audited and controlled, all within a centralised dashboard.

More than that, the Continuous Compliance platform provides a managed security service wrap that ensures these non-conformities are resolved within the scope of the infrastructure scope within the SLA.

WHAT ABOUT SECURITY?

With a multi-layered approach to security, Pulsant adheres to cloud industry best practices, while being compliant with a number of standards — such as ISO27001, Cyber Essentials Plus, CSA Star (cloud security) and IASME Gold.

Unlike other continuous compliance solutions, our platform can read, process and analyse configuration data from multiple data sources, including operating system logs, software configuration, applications, cloud platforms, such as AWS and Azure, and other compliance tools. This also means that the platform can work in public cloud, on-premise or in hybrid environment environments, with specific rules and policies defined during the mobilisation phase of the relationship.

CONCLUSION

It is important to understand that cloud isn't a hidden landscape. It offers a tremendous amount of transparency, which helps in its acceptance and continued adoption of the technology and an approach to compliance. This is especially important with the growing role that compliance is paying in business. Yes, compliance may be challenging, but it is achievable. So is continuous compliance, something that can add significant value to your business. The use of the right platform, supported by a team of experts, can go a long way towards removing the complexity from the process of complying in the first place, as well as maintaining it.

SOURCES

1. https://www.dlapiper.com/en/hongkong/news/2016/04/2016-compliance-and-risk-report/
2. https://www.goanywhere.com/blog/2017/02/03/8-shocking-pci-compliance-statistics

Find out how we can help your organisation,
call **0345 119 9911** or visit **www.pulsant.com**

Cadogan House, Rose Kiln Lane,
Reading RG2 0HP

info@pulsant.com
pulsant.com

Pulsant
Business Unlimited