A delicate poise: research into the state of compliance capability in UK enterprises

QUOD ORBIS

Introduction

The ability to comply effectively with an ever-expanding portfolio of legislation, regulatory demands and best practice guidelines has pushed compliance capability to the fore of many boardroom discussions.

As many of these frameworks have a profound impact on the risk and security posture of an organisation, particularly with regards to cybersecurity, they have led to the development and implementation of crucial metrics and controls that has driven a great deal of investment in technology; ensuring the efficacy and positive impact of this investment – that is to say, making sure that the technology bought keeps businesses compliant and safe - has led to the development of many new disciplines, including continuous controls monitoring (CCM).

This inaugural report represents a keen insight into this ‘compliance capability’ at businesses within the UK. The research focuses on businesses of more than 1,000 employees in the domestic UK market, drawn from a range of sectors. As one of the leaders in the emerging CCM market, we have also offered our take on the facts and figures to provide some context.

Right here, right now: the current state of play

When asked: “With regards to your current compliance capability, which of the following statements most accurately describes your organisation?

- 42% identified that they have a dedicated in-house compliance capability with direct access to all necessary data and systems
- 26% have an in-house compliance team that consults with other departments for data and access for compliance
- 16% said they prepare compliance activities periodically, in accordance with regulatory / external demands
- 14% claim they maintain continual compliance readiness
- 2% outsourced compliance

These figures suggest firstly that compliance remains an in-house affair. With over two-thirds of businesses featuring a dedicated in house compliance team (regardless of how they access the data they need to do their job), it is hardly surprising that that there is already an emerging leaders category that has a continual compliance readiness.

Our take:

We have already seen the development of compliance leaders as businesses such as XXXXX have embraced CCM to provide direct access to the data and technology so they remain continually ready for any compliance demands. But our experience would suggest that the reality on the ground is a little more fragmented. Firstly, it may be that the number of businesses claiming direct access to all necessary systems is a little optimistic. Secondly those organisations whose compliance teams rely on other departments are often those in most pressing need of a single source of the truth to create a bedrock of compliance capability.

In too deep? The extent of compliance activity and metrics

To get an idea of the current compliance landscape as it is actually happening, we asked businesses if they track some basic metrics, and the extent to which those metrics represented the full technology estate within the business.

- Just under half (48%) track the financial investment in any technology necessary for the compliance team to acquire data from other departments
- 42% kept an eye on the time spent processing or formatting data from other departments to make it usable for the compliance team
- Just under a third (30%) monitored the time spent by other departments in getting the data necessary for compliance projects, and the same amount tracked the time spent checking the veracity of internal data before submitting to external auditors
- More than one-in-ten (12%) did not track any such metrics

We then asked how deep into the technology estate these businesses had to dive, in order to ensure they had representative and accurate figures.

- 15% of businesses reported that they needed to access more than 90% of their technology for compliance
- A further 37% said they needed to access between 70 and 90% of the estate
- Another 25% said they needed to access between 50 and 70%
- 16% felt they needed to access less than half the estate to achieve compliance

Our take:

The first point of analysis we make from these replies is that there is a lot of time spent preparing, formatting and checking data for use in compliance projects. One might reasonably expect the primary concern of IT decision makers to be tracking the investment in technology, but they are clearly also having to keep a close eye on the time spent on tasks that could easily be eliminated or automated.
Again we see the emergence of a leader category with the 15% claiming high penetration throughout the technology estate to achieve compliance. But for the 41% of companies accessing only up to 70% of the estate, concerns over the comprehensiveness of their compliance posture must arise.

Tell me why: the drivers behind compliance capability

Compliance is a broad church, and the compliance capability of any organisation must be keenly aligned to the primary strategic concerns of that business. We therefore asked businesses to identify the main, current drivers of their compliance activities.

- An active risk reduction strategy was the clear leader with almost three-quarters (74%) identifying as the driver for compliance activities.
- However, validation of security controls was the second biggest driver, with 60% identifying it as the driver, further reflecting the link between compliance and security
- Just over half (53%) identified the demonstration of third party regulatory compliance as the main driver, just head of the 50% looking to achieve industry best-practice
- Lastly, a substantial 36% are using compliance to highlight areas in need of investment

Our take:

Compliance is always going to be driven by an attempt to reduce risk: the potential losses that may arise from noncompliance with laws, regulations, standards, and both internal and external policies and procedures range from expensive to existential. But these figures clearly demonstrate that a technology that can also validate the security controls in place within an organisation offers a compelling advantage: one that may even outrank considerations of regulatory compliance.
We can hazard a guess or two as to why this may be: cybersecurity threats might now simply be bigger or more pressing than regulatory demands (especially as businesses have become more compliant whilst cybersecurity threats such as ransomware continue to grow.) Or it could be that businesses are now focusing on making sure that their security investments are doing what they said they would.

When tomorrow comes: the now and next of compliance capability

So, based on this set of parameters, what is the current state of compliance processes within these UK businesses? According to our research:

- 45% of businesses feel their compliance processes are completely automated and integrated end-to-end, compared to 52% that would characterise such processes as manual and fragmented, requiring dedicated projects for each certification
- 47% of respondents report a general level of ignorance of key risk indicators throughout the business
- 57% of respondents said that the sources of data that they require for compliance are easily accessed
- 70% of respondents believe they have full visibility of their compliance posture, but only 51% has full confidence in their outsourced compliance provider

Our take:

It is hard for us to conceal a note of surprise with some of the confidence present in these figures – for the seven out of ten businesses claiming full visibility of their compliance posture and the near half of businesses claiming completely automated and integrated compliance processes. Our experience is that once businesses begin to examine their compliance posture, they quickly realise some of the gaps present, be it in terms of availability or indeed, the confidence in the data.

Orientating towards the future, we asked businesses what they saw as the main obstacles when it comes to investment to change or improve compliance processes

- 28% cited the fear of embracing new processes – the top obstacle – and keenly related to the additional 23% that identified attachment to the time and effort invested in developing the existing processes.
- This was closely followed by a lack of senior management sponsorship of new initiatives (27%) and the related 24% that cited the perception that compliance is solely a cost of business to be borne.

- The biggest technological issue reported was the inability of solutions to access all necessary data and systems, identified by 25% as a barrier.

Our take:

Compliance can be complex and it is therefore entirely understandable that there is a great deal of attachment to established processes and a fear of change – these are perennial issues when it comes to new technology and ways of doing business. It is disappointing that there is still a substantial perception that compliance is simply a cost centre to be tolerated, but as projects continue to demonstrate the additional business value that compliance can deliver, we expect this to change.

The technological barrier of access to any data source, or indeed any framework, has been overcome, so it is very telling that so many IT decision-makers still see it as such an obstacle to effective compliance readiness. Clearly there is still a pressing need to demonstrate that modern technology such as CCM can pull data from anywhere and interact with any set of standards.

In conclusion

Many of the numbers in this research paint a picture of faint poise in the compliance posture of UK businesses; a confidence held by those who have overseen the investment in the technology that delivers report and tracks the alignment of actual operations to how things ‘should be done’.

But it seems this is a fragile assurance: businesses are split down the middle when it comes to characterising their compliance processes as integrated or fragmented. Visibility into the technology estate is not exactly myopic, but there are clearly holes to be stumbled into. And the ever-present spectre of risk has been joined by a pressing need to prove cybersecurity controls are doing what they should.

There are however, some rays of good news. We can confidently assert that the barriers of compliance technology not being able to access any data source, or interact with any framework, have been overcome. This alone can increase the amount of businesses able to see further and clearer into their technology estate to improve compliance. And the same technology can also validate the effectiveness of cybersecurity controls.

Compliance will continue to be a complex, nuanced affair for most businesses and we look forward to tracking increases in confidence as we run this research in the future.

QUOD ORBIS

Quod Orbis Limited, 2nd & 3rd Floor, 2 Burgon Street,
City Of London, London, EC4V 5DR, United Kingdom

T +44 (0)20 3962 2206

www.quodorbis.com