WHITEPAPER

STRENGTHENING GOVERNANCE & COMPLIANCE

5 Steps you can take to meet regulatory compliance across your supply chain

Nick Francis

Chief Technology and Marketing Officer
Brooklyn Vendor Assurance

TABLE OF CONTENTS

Introduction

As always, the pace of change is unprecedented. Services continue to be delivered faster and cheaper than ever before, increasing how many vendors organisations are using and for differing and new services affecting how large the supply chain has potentially become. It remains that the most commonly outsourced services are either technical (information technology) or financial (accounting services) in nature. Consolidation activity and cost containment continue to be top-of-mind issues for most organisations.

Global supply chain resiliency has been continually tested by events over the last five years including BREXIT and COVID-19. The pandemic is responsible for a massive increase in the number of home workers worldwide. Governing practices required updating and digitisation to cope with the changes as we are yet to return to the previous working conditions, and it is debated if we will.

All the while regulations are maturing, now becoming better defined across an increasing number of industries. The impact of this against all industries and verticals needs to be considered now as to how it may affect internal operating models in the future.

There is an increasing amount of risk now residing outside of the boundaries of the organisation where visibility needs to be achieved, utilising different methods as opposed to the workforce and process beings under the control of the same management hierarchy.

It is now being recognised that Vendors, especially smaller more agile ones are able to add much more value to an organisation if engaged in the right way. What is low value for even a small niche supplier can be of high value to their customers increasing the buyer's agility and ultimately time to market. Performance and building fully integrated valued partnerships is what matters and no longer based on just the relationship of certain key individuals within both businesses. Everyone in the organisation working with or alongside vendors needs to be given the clarity of task and capability to succeed in capturing meaningful data points as they go.

The need to accelerate growth is now more urgent than ever. The old growth model – loosely based on the premise that a rising tide lifts all boats – is gone. In such circumstances, unlocking growth from within the organisation is essential and, fortunately, eminently doable. Companies that rethink and reinvent the way they manage procurement, vendors and supply chains have a significant opportunity to improve their bottom line.

Consultants McKinsey estimate that poor management of supplier performance is adding 10-20% to total costs in the contracted category. Most companies recognise they can do better: one study from the Massachusetts Institute of Technology found that 77% identified two of their three greatest procurement risks as ‘dependency on suppliers’ and ‘supplier quality problems.’ Historically, procurement has been regarded as a function that does, rather than thinks, yet any CPO who can argue credibly that they can add a percentage point or two to operating profit will grab other stakeholders’ attention.

McKinsey stated in their Next generation supply chain 2020 report that Supply chains of the future will need to have dedicated

functional leaders, and companies will start to focus on the transformation of the supply chain through dedicated supply chain academies, and develop change agents to achieve supply chain excellence. How do you measure up to this today and more importantly how will you tomorrow.

Comply, why bother?

A company's supply chain can present significant compliance risks. Aspects to consider include corruption; fraud; export controls and sanctions; environmental, social and governance (ESG) compliance requirements; labour law compliance; and health and safety laws, among others.

Since the financial crisis in 2008, local authorities and regulators around the world have drastically increased the amount of regulation being published for financial services with other sectors now following suit.

This somewhat accelerated in 2013 when the Financial Services Authority (FSA) was restructured into the Financial Conduct Authority (FCA), who today work very closely with the Prudential Regulation Authority (PRA).

The FCA now acts as watchdog for the conduct of all regulated and authorised firms and individuals alike, whilst the PRA, under the watchful eye of the Bank of England (BoE) and Financial Policy Committee (FPC), are responsible for prudential matters, ensuring financial stability of the larger organisation.

The approach seen in Financial Services is now starting to extended in to other previously unregulated industry areas and is forming the basis for some of the guidance issued by other governing bodies such as the ICO through the 2018 GDPR legislation

and via HMRC, NCSC or the Gov.uk website, there are in fact over 90 regulatory bodies in the U.K alone.

It is a challenge and ongoing burden for an organisation to achieve, maintain, and demonstrate regulatory compliance against their supply chain. There is a growing need to show substantial evidence and auditing

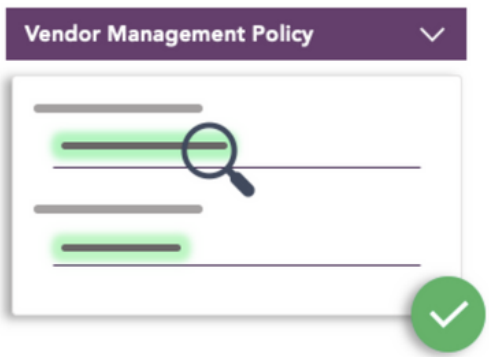
measures across numerous regulations and law enforcements throughout a number of industries and geographies. Therefore, presenting a large burden on legal and compliance teams to ensure contracts are compliant against these requirements making adaptation difficult. However complex this challenge its now proving to be much less significant when compared with the impact of a breach or being found to be non compliant;

- Average cost of a Global Data Breach in 2022 was £3.5m
- 6.5x Regulatory rules growth since 2008
- GDPR total fines rose to €1.08 billion since 2021 in comparison to €158.5 million in 2020.
- 45x increase in fines since 2010

Ponemon Institute, Cost of a Data Breach 2022 Report*
Thomson Reuters - Cost of Compliance Report*
DLA Piper GDPR Data Breach Survey 2022*
McKinsey Report - A best-practise model for bank compliance*

5 Steps to demonstrate regulatory compliance across your supply chain

Not all is lost, there are a handful of steps that a department responsible for managing vendors as the associated supply chain can take in order to iteratively improve things.



1 A Clear Policy and Control Environment

Be it external regulation or an internal strategy, it makes little difference and it is usually a combination of the two that are required in order to define a clear and easy to communicate Vendor Management Policy.

A policy should clearly outline what needs to be completed, how frequently, to what vendors and by whom. These individual policy elements or controls need to be curated by interpreting them directly from the external regulation released and maintained by the regulatory body in question.

This collectively layouts out the basis for your Control Environment and will provide operational clarity to the employees across the organisation the things that need to be undertaken, when to do so and who to lead it.

You may go further than this and start to include against each policy element or control what the indicators are of each one that means the control is healthy, these may be leading or lagging in nature and maybe be performance or risk based in measurement.

What a policy shouldn't really do in great detail is set out the process or steps that need to be followed to meet them. It's more a document that outlines what MUST be done, not the HOW which is similar to the majority or the regulations that are inflight today. There aren't prescriptive on the how and to what level is acceptable, this is for the organisation to define through engagement with those with direct experience of what is being asked for to set the bar.

2 A Set of Consistent Processes

In order to effectively meet the control environment laid out in the policy the method or way of working used to fulfil these needs

to be carried out in a consistent manner that is not only measurable but something that is being continually optimised and improved based on feedback passed to the process owner, more on this person later.

These are essentially the key processes that a function needs to make use of in order to carry out its duties on a day to day basis. Processes need to be well documented including fully defined workflow steps, RACI models showing who is accountable and responsible and who needs to be consulted and informed. There needs to be guidance on what an acceptable outcome looks like or the definition of done captured, the evidence assets that need to be collected and collated throughout the steps.

Where possible examples of what good looks like should be referenced and linked to. It is a fundamental ask that each and every process have a defined owner that will manage and incrementally improve the process. By ensuring this level of rigour is included it will result in the process, when being followed, to automatically ensure that it complies with the policy / controls it's aimed at fulfilling demonstrated at the point of delivery.

Common processes that are being recognised in most regulations cover topics such as regular Risk Assessments, business continuity testing and exit strategies to name a few.

3 A Clearly Defined Operating Model

Considering the right operating model archetype that has the required level of control balanced with the ability to scale is key.

Underpinning this would be a fully defined set of roles and capabilities matched with an effective talent management plan linked by to an organisational operating construct driving the right level of accountability and responsibility that can be mapped back to process and policy.

There are many models that can be considered such as centralised or decentralised operating models, all have their benefits and drawbacks.

A centralised model can maximise control and quality but struggle to scale and is expensive. A decentralised model gives control away to those in direct daily contact with the vendor but struggles with quality and in most cases visibility is low in these situations.

However, a mix of both approaches in a coordinated and aligned way might show the most benefit when supported by the right high-quality guidance and digital tooling; it will return over 99% of the benefit seen in both models with very little of the drawbacks. Each organisation will need to consider this carefully.

4 A Way to Measure Control Effectiveness

The ability to easily view where across the vendor landscape you have met your control environment objectives and where there needs to be more focus given at a particular point in time will result in being able to measure in a meaningful way how compliant an organisation is to its policy at a per vendor, tier / segment, sourcing category or across its entirety.

The ability to comply with regulations us not about ensuring that an organisation never has any problems, which would be nice, but more about when they do the organisation has the right controls in place to initially detect the anomaly and then are able to apply the right processes put in place to ensure that once acknowledged the defect or deviation can be managed to its conclusion via a set of clearly defined steps.

Collectively, this shows that 'reasonable steps' have been taken to manage the situation thus alleviating or mitigating any risk in part or in its entirety

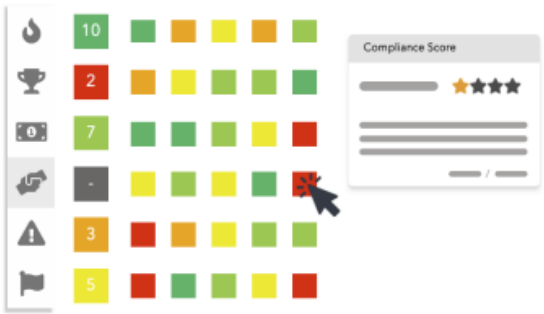
5 An Ability to Report on any Compliance Gaps

No longer is it appropriate to only be able to show where intervention was needed at a particular point in time.

Being able to retrospectively demonstrate not just only where and at what point in time an event occurred or deviation was detected but what were the events that took place proceeding the event and what took place thereafter.

his full audit log or event journaling is set to become commonplace not only for auditory purposes but to be able to use the data to learn and refine processes for each event.

This approach is akin to that of Post Incident Review (PIR). A PIR is an evaluation of the management response and recovery effort for major, critical and high priority incidents or events. A meeting is initiated once the event has been resolved where information captured during the event's life-cycle is included in its review. The output of the meeting is a report of potential findings detailing how the event could have been handled better. For that reason, consistently performing post event reviews is a great way to continuously improve the event handling process what ever the said event may be in the situation.



Some of your organisations Post Event Review Goals could look like the following;

- Eliminate or reduce the risk of event reoccurrence.
- Improve the initial event detection time.
- Identify improvements needed to diagnose the event including what was impacted, priority level and the correct resolver teams to be engaged.
- Review the repair / intervention steps and identify recommendations to reduce a future event repair duration.
- Review the duration to initiate and complete activities to ultimately identify improvement recommendations.
- Ensure event communication is proper or if anything can be improved.
- Update the major event management best practices as needed to continuously improve.

Summary

The need and or desire to comply with sometimes complex regulation cannot be a fleeting thing nor is it something that can be addressed overnight.

The ability to really comply with regulation and be able to demonstrate the desired outcomes at scale means that you need to have a balanced and systematic way of breaking down tasks (controls) into both a repeatable and scalable format that is well documented and widely available for consumption.

Coupling this with a clear operating model where everyone knows the part they play, that is consistently applied and improved over an extended period will deliver the kind of returns that all regulators want and hope to see in their supervisory audits and investigative reviews.

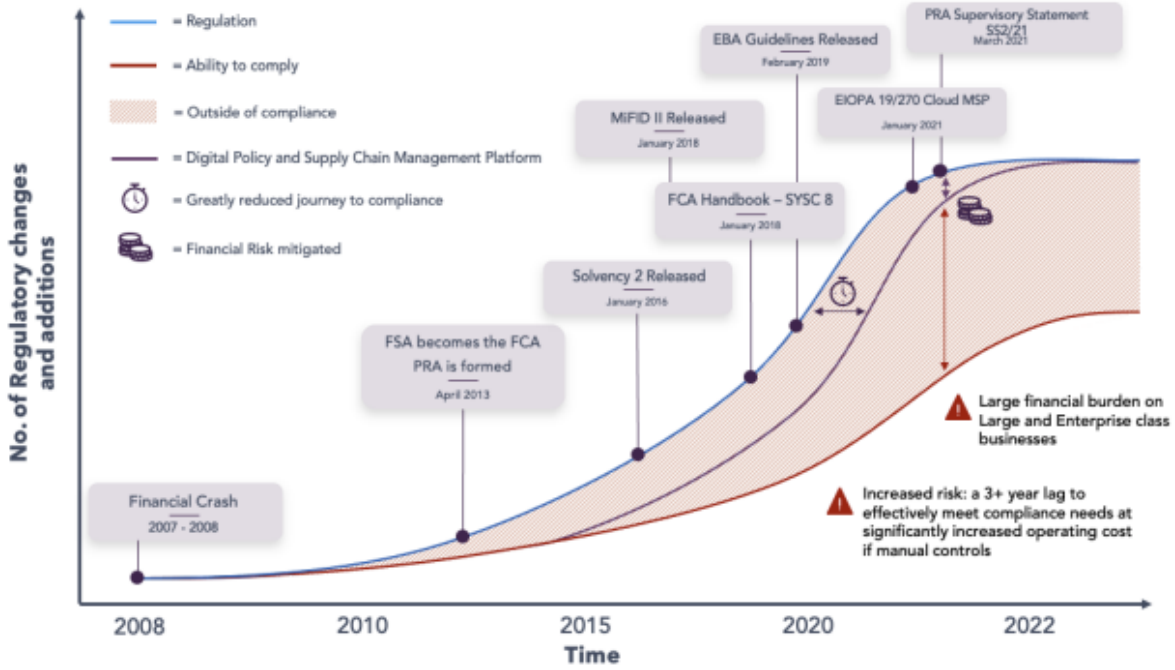
As should be apparent by now the five steps outlined above are in all likelihood the minimum set of success criteria or objectives that one can take to demonstrate the effective management of vendors against any regulatory requirement.

They are the minimum because there is heavy overlap between each of them, each one reliant on the next meaning one really cannot exist in isolation without the others. To go beyond these five steps and when matched to the right digital tooling will accelerate implementation, as well as dissemination of knowledge and help demonstrate ineffective or missing controls faster through the out of the box reporting and alerts whilst reducing the cost of compliance year on year to the organisation.

Stay Fit for Audit, Always

Our Brooklyn Vendor Assurance (BVA) SaaS platform is built on ensuring businesses stay ahead of the curve from a regulation and compliance perspective, doing so across three key pillars – Company Policy and Process, Contractual Compliance and Regulatory Adherence.

Our customers make use of Brooklyn to help automate and operationalise the best practice require to ensure they can not only meet regulations but iteratively increase the



effectiveness in which they do whilst being able to ensure consistent governance which can be easily adapted to the ever-changing requirements from governing entities or regulatory bodies.

Accompanying this is the ability to automate processes related to Contract, Performance, Risk and Relationship Management, allowing Compliance teams to rest assured that the supply chain is evaluated and assessed regularly, against the needs of the business and always fit for audit.

So confident are we that we would happily support the supply of evidence for any vendor management audit your organisation is involved with whilst you are a customer.

Get in touch

If you would like to know more about becoming digitally fit for audit, risk and compliance management or Post-contract Customer-Supplier Management, please get involved through the comments or just like, share and subscribe via the details included to ensure that you don't miss out on any future content.

To speak to someone from the Brooklyn team about the solutions that we offer, **Request a demo**.