

**Maintaining your compliance
monitoring programme**

Is your CMP fit for purpose?

National and international regulators are stepping up their scrutiny of corporate behaviour, and new risks to your business emerge on a regular basis. Non-compliance can result in financial and reputational damage and serious business disruption. And it can introduce inefficiency into your systems and undermine the trust of investors and customers.

Good compliance monitoring programmes (CMPs) help to avoid these problems. CMPs assist businesses to adhere to a complex web of rules that cover everything from AML and KYC to ESG and data privacy. They test policies and protocols to identify gaps in cover and where direct remedial action is needed. When your CMP works, it is your best defence against a potentially damaging compliance misstep.



¹. Thomson Reuters Risk & Compliance Survey Report

But CMPs do not always work. As compliance specialists, we see too many programmes that are more of a comfort blanket than a bullet-proof vest. Businesses feel reassured simply because a CMP exists, ignoring potentially harmful limitations.

CMPs are created in good faith, so why do they go wrong? Often, it's because they are created but never updated and gather dust as the world moves on. It's also common for CMPs to be properly designed but improperly applied, usually through a lack of resources. Others are tick-box exercises that do not meet the needs of the organisation concerned.

Too often, it's nobody's job to review an existing CMP – or at least nobody's priority. With too little time and too few resources, firms may take the view that if a compliance programme has worked up to now, it will keep on working in future – or that informal monitoring activity through close collaboration between colleagues will suffice.

This is risky thinking. In these uncertain times, investor due diligence teams and corporate customers value good compliance monitoring as much as industry regulators do. A strong CMP should be designed to evidence adherence to regulations while also being part of your risk management framework and appropriate systems and controls.

If you don't have a CMP, we strongly advise that you create one. If you do have one, this guide will describe the ways in which even the best plans fail and the steps you can take to make sure your CMP always remains fit for purpose.



Mark Spiers
Managing Partner
Bovill Newgate

Our authors



Mark Spiers

Managing Partner

Mark has over 20 years' experience in the industry. He has worked in multiple compliance roles including as a Money Laundering Reporting Officer in several large international investment banks, including UBS and Kleinwort Benson.

Mark is a hands-on practitioner who specialises in the practical interpretation of the rules in a commercial environment. He also has significant experience in handling regulatory intervention including thematic reviews and potential enforcement action.



Matt Browne

Partner

With 18 years' experience in financial regulation, Matt brings experience from PwC, where he was a Director in their Risk and Regulatory Practice, leading a team supporting clients across retail investment markets. He has worked on a broad range of conduct and culture issues, including governance reviews, Senior Managers and Certification Regime (SMCR) frameworks and digital advice platforms.

Having also worked at the Financial Conduct Authority leading on regulatory initiatives including the RDR and investment platforms, Matt has gained a deep understanding of the regulator's strategy and approach.



Abi Reilly

Partner

Abi looks after several hundred clients on an ongoing basis, many of which have been with the firm for over 10 years. As well as looking after traditional asset managers, her team covers alternatives such as private equity, real estate, venture capital and impact funds. She also provides support to some corporate finance businesses, research providers, depositories, and placement agents.

She prides herself in providing straightforward, practical advice to firms to explain the current regulatory climate and how it effects them.



Ben Arram

Practice Lead, Payments

Ben works with clients to provide comprehensive regulatory and compliance advice for firms at all stages of their development. This includes, helping firms throughout the regulatory application process, drafting tailored policies and procedures, assisting with regulatory reporting, and providing ad-hoc advice.

He has over 15 years of experience advising global financial services firms, having previously held positions spanning regulatory finance, regulatory reporting, strategic capital management and risk. He also has specific expertise and interests in prudential regulation, risk management, wind-down planning, change in control applications and operational resilience.



Mike Harrison

Consulting Lead

Mike is responsible for project delivery and quality across our retail and consumer facing clients including wealth management, financial advice, consumer credit, mortgages and insurance.

A seasoned regulatory consultant, he has over 25 years' experience in financial services regulation and has worked for the 'big 4' and two of the UK's leading independent consulting firms. He was also Director of Risk & Compliance in a well-known mortgage and credit intermediary.



Chloe Arnold-Martin

Principal Consultant

Chloe provides regulatory and compliance advice on CASS and safeguarding. Before joining Bovill Newgate, Chloe was an external audit manager at PwC for both financial statement audits and CASS audits for a range of financial services firms.

Her experience on CASS audits has covered a variety of product offerings and business models, exemptions and outsourcing arrangements. And her audit history has also provided experience with one-off transactions, system migrations and business model changes to give a breadth of scenarios impacting regulatory risks.



Ronnie Kwok

Principal Consultant

Ronnie helps a wide range of clients across all our jurisdictions with regulatory applications, risk assessments, compliance monitoring, and day to day compliance advice and support. He also assists asset managers implement remuneration requirements.

Before joining Bovill Newgate, Ronnie was the Head of Compliance for a financial group with asset management, advisory and brokerage businesses. He has also worked for the Securities and Futures Commission of Hong Kong, where he developed a strong understanding of how regulatory bodies operate and how policies are made.



How CMPs fail

Why might a CMP fail? In some cases, it might never have worked properly in the first place. Generic, one-size-fits-all compliance monitoring will not stand up to scrutiny. A CMP needs to be bespoke to your organisation and appropriate to your size, sector and risk exposures.

Another common issue with the cookie-cutter approach is proportionality. CMPs should provide the level of compliance monitoring your business needs – not too little or too much. Many businesses struggle with CMPs that are overly basic for their evolving needs, but we also regularly see plans that are far too elaborate and impenetrable to be of practical use.

These hefty tomes – often generated by consultants – are bogged down in unnecessary detail that can result in paralysis. Instead of focusing on the most likely areas of risk, the attention of compliance teams (or, sometimes, a single compliance professional) is scattered and diluted. Updating unwieldy compliance monitoring plans is a herculean task that nobody wants to tackle.

Yet updating a CMP is almost as important as creating it in the first place. A CMP that sits on a shelf gathering dust is an exercise in denial. Monitoring has to move with the times because businesses and regulators never stand still. When change happens, your risk assessment should change and, with it, your CMP.

Triggers for review include regulatory changes (or changes in regulator focus), business growth (including M&A), cross-border expansion, new products or services, new distribution channels, recruitment drives, changes in management structure and more. In short, if it impacts your risk assessment, it should prompt a review of your CMP, which in many cases lags far behind business development.



“Too often, we see risk assessments and CMPs that don’t align. In those cases, compliance monitoring is not protecting a business from risk and needs urgent review.”



Abi Reilly
Partner

Early symptoms of an inadequate CMP



It doesn't make sense

Does your CMP make sense for the kind of business you are and the risks you face? Is it practical and executable, and is monitoring frequency appropriate? When was it last updated and why, and what has happened to the business since then?

Sometimes, there are no symptoms at all and gaps only become obvious when regulators find something wrong or investors walk away. Regularly reviewing your CMP is the only way to be certain that it remains fit for purpose.



You lack resources to properly monitor compliance

Monitoring is a process, not a project. If the compliance function is overworked and falling behind, monitoring will be falling behind too. You may find you have a monitoring plan but not the resources to effectively implement it.



There's a disconnect between compliance and the business

Compliance monitoring should be considered a top priority by the organisation from top to bottom. If it is considered a nuisance – if the compliance function is seen as the "business prevention" team – a change of culture is in order.



There have been issues

Customer or client complaints, negative feedback and repeated disruptive incidents – such as onboarding mistakes, data protection missteps or incidences of employee fraud – may be evidence of a failing CMP.



74%

of organisations say they lack the budget and resources to properly address vulnerabilities²

What happens when your CMP fails?

The consequences of a compliance monitoring failure range from a slap on the wrist to potential jail time if there is evidence of criminal activity.

Common risks include:



Fines

Regulators will fine companies that fail to comply in a significant way or repeatedly flout rules. Fines vary depending on the seriousness of the issue but can run into millions



Reputational damage

Investors and customers have reputations of their own to protect. Your non-compliance can persuade the people you do business with to look elsewhere.



Business disruption

Non-compliance findings force organisations to quickly redirect resources to fix the issue, disrupting day-to-day operations. Organisations that are found non-compliant in one jurisdiction may find themselves under more intense scrutiny in other jurisdictions where they operate.



Legal action

If non-compliance leads to legal action, time, money and resources will have to be ploughed into your defence, whether the action is successful or not.

3. IBM Cost of a Data Breach Report 2024

\$220k

Data breaches cost companies nearly
\$220,000 more on average when
non-compliance was considered a factor³

How to keep your CMP in good health

What does a good CMP look like?

- It is proportional to your needs, providing the right level of monitoring for the size of your organisation, the sector you operate in and the resources at your disposal.
- It evolves with your business. Every significant change in the way you operate, the products or services you offer or the way the business is run automatically prompts a review.
- It reacts quickly to regulatory updates or changes in regulator focus. It is a dynamic plan that moves with the world around it.
- It is practical and pragmatic, tailored to the operational realities of your business. It is executable and, where applicable, tied to specific and relevant regulatory references.
- It adds value. A good CMP can aid improvement in processes across your organisation, drives efficiency and provides commercial insight. Applying results from compliance monitoring can make everything from onboarding new clients to business acquisition simpler and quicker.
- Finally, a good CMP brings you peace of mind. It provides structure, allowing you to manage and grow your business in the way you want, knowing that comprehensive but proportional compliance monitoring protects you from unnecessary risk.

74%

of risk and compliance professionals see part of their role as enabling, supporting and enhancing business activities⁴

"A good CMP does more than keep you compliant. It drives process improvements and efficiency and can save money. By streamlining areas like onboarding, it can help you do more business."



Ben Arra
Practice Lead

4. Thomson Reuters Risk & Compliance Survey Report

Three steps to creating a dynamic CMP



Conduct an annual review

Reappraise your CMP at least every year to assess effectiveness, identify gaps and ensure it continues to offer adequate risk protection.



Conduct ad hoc reviews when required

When something changes, you should reassess your risk and, with it, your compliance monitoring programme. That includes any changes in regulation or regulatory focus and any significant evolution of your business.



Adopt a "stitch in time" philosophy

You give your car an annual service so it doesn't break down on the motorway. Compliance should be viewed in the same way. Catch problems when they're relatively small and cheap to fix, rather than waiting for a crisis.



The role of technology

How can technology enhance compliance? Technology provides a repository for all of your disparate data, rules and policies, and allows you to track and monitor compliance filings.

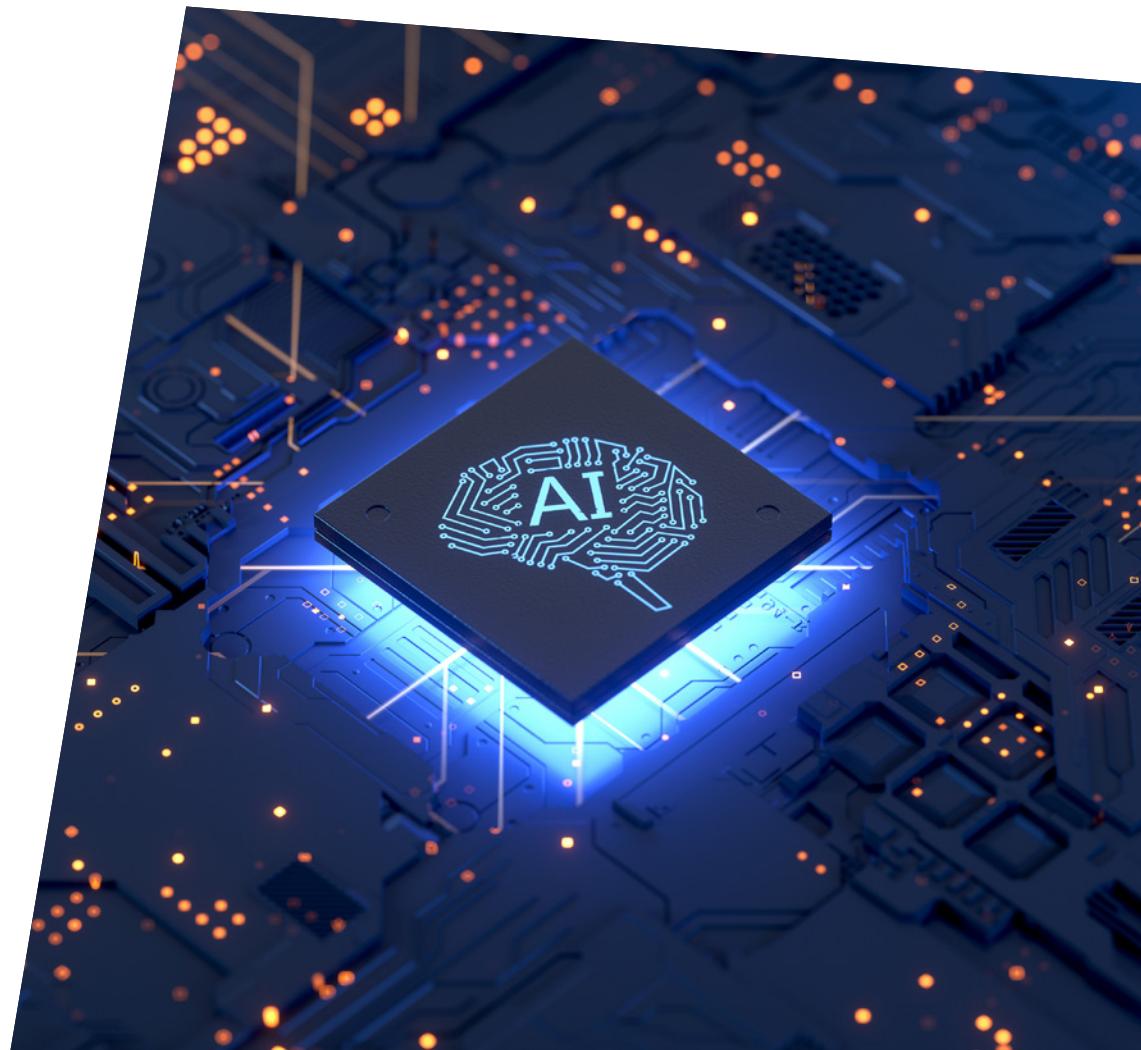
A compliance platform should be easy to update and accessible to everyone in the business. As well as centralising data, good compliance platforms can streamline processes, enhance communication and make compliance-related information widely available. Technology can help with all this – but it's not a magic bullet.

Vendors are apt to oversell platforms as cheap one-size-fits-all solutions. Even the best technology needs to be tailored to business needs, maintained and updated. That takes IT manpower and compliance expertise. A balance needs to be struck between IT and human resources.

Predictably, AI is now being hyped as the answer to every compliance officer's dreams. There's no doubt that AI has the potential to significantly enhance compliance monitoring by automating routine tasks, providing alerts on suspicious activity and predicting upcoming compliance risks. Generative AI assistants might support frontline operatives in the first line of defence by providing instant answers to compliance queries based on an organisation's proprietary information and risk policies.

But AI creates compliance challenges of its own. The regulatory environment around the use of AI is still evolving and codes of practice are largely untested. The accuracy of generative AI is also an open question. And AI's hunger for massive amounts of data is potentially problematic in terms of security and privacy.

For these reasons, the best advice is to proceed with caution when exploring AI as part of your CMP. AI is already proving its worth in certain areas and its benefits will become more apparent over time. Nevertheless, it would be dangerous to rely too much on such a nascent and rapidly evolving technology in the short term.



The role of third-party providers

At some point in their development, many businesses decide they need third-party support with compliance monitoring activities, for a number of reasons:



Growth plans

Compliance issues can throw a spanner in the works of expansion. Businesses on the cusp of rapid growth often turn to third-parties to bolster compliance monitoring as workloads mount.



Unexpected surprises

The regulator gets in touch. An investor due-diligence team demands improvements. A competitor faces regulatory censure. Shocks to the system like these often persuade internal compliance teams of the need for external resources and a fresh eye.



Missed deadlines

As time ticks towards year end, internal teams realise that their compliance monitoring schedule is badly off track.



A compliance review

An internal or external review finds an out-of-date CMP, a lack of resources, a misalignment of risk and monitoring, an overreliance on third-line auditing, or all of the above.



A problem

Third parties are often called in when, for whatever reason, a compliance event has occurred.

33%

The costs of compliance have risen by a third since 2021⁵.

The benefits (and pitfalls) of external compliance resources

What do third-party providers bring to the table?

Outsourcers are typically brought in for one of two reasons.

1

Third parties might be asked to lead a project to replace a misfiring or obsolete CMP with a proportionate, current and tailored upgrade. This project work is often triggered by a compliance issue and is typically time limited. The CMP is created and then passed back to in-house teams to implement.

2

Alternatively, third parties are brought in to provide an ongoing compliance monitoring function. Whether they've created the CMP or not, they're tasked with reviewing, updating and implementing it on a day-to-day basis. They become an integral part of your second line defences, freeing up internal resources for other tasks.

In either case, there are significant benefits to third-party involvement:



Resource

The cost of compliance professionals is high and getting higher. Using third-party personnel takes away the costs of recruitment and retention. Manpower can be scaled up and down as circumstances demand.



Speed

When speed is of the essence, bringing in a ready-made team of compliance professionals is a lot quicker than building one from scratch.



Expertise

Firms may need compliance expertise at crucial moments, but not all the time. Tapping into this expertise can be expensive, but outsourcing makes it an occasional cost rather than an ongoing one.



Viewpoint

A specialist compliance consultant has a market view. They will have worked with businesses like yours before. They understand proportionality and what the regulator wants to see, and bring a depth of experience to your compliance challenges.



Corroboration

Compliance teams may identify problems, but convincing the rest of the business to act can be tricky. A third-party specialist can act as an ally, providing independent corroboration in dealings with the wider organisation.



Early warning

Third parties provide an early warning of potential problems. It's better for an external specialist to find a glaring omission than the regulator.



Dedication

Small or part-time compliance functions might provide sticking-plaster solutions, or they might put too much faith in third-line assurance. They may ignore compliance issues simply because they have a hundred other things to do. An external party can bring dedication to the function, chasing down challenges until they're solved.



"Third-party relationships break down for a number of reasons. The provider can breach trust by not doing something they promised to do. The relationship may be too impersonal or too generic. Their monitoring function can be either too woolly or too onerous – which means it lacks proportionality. Organisations should review their outsourcer relationship and make sure they still provide the assurance they need. "



Matt Browne
Managing Partner

Choosing a third-party provider

How do you choose one provider over another? Look at the basics first. Do they have specialist expertise in compliance (as opposed to general corporate outsourcing). Do they have experience with businesses that look like yours and a deep knowledge of what regulators in your sector expect to see?

After that, consider the four Ps...



Are they pragmatic?

Will they get to know your organisation in detail and tailor compliance services accordingly?



Are they proportionate?

Compliance requirements are not the same. Ask any potential provider how they'd apply the principle of proportionality to your organisation.



Will they prioritise?

A provider should identify and deal with the biggest risks first. What would they prioritise in your organisation?



Are they people-first?

Can you work with them? Strong personal relationships that build trust are a crucial factor in any business/outsourcer relationship.



The case for compliance

Compliance is easy to ignore, right up until the moment a regulator or client due diligence team wants to see evidence that you take it seriously.

A dynamic CMP, rigorously applied, is proof that you do. Compliance monitoring reduces risks to your organisation but also confers commercial advantage. A well-considered CMP keeps regulators happy, reassures the people you do business with and helps streamline your systems and processes.

Too many CMPs don't fulfil these functions, because they lack relevance and proportionality or gather dust while your business develops. Sometimes, the best-laid compliance plans are only ever partially applied.

As compliance becomes more important and scrutiny more intense, a relaxed attitude to compliance monitoring is not sustainable. Your CMP should be regularly reviewed and conscientiously updated. Technology can streamline monitoring and reporting, and third-party specialists can provide the resources, solutions and expertise that in-house compliance functions lack.

However you do it, the most important message is that your CMP is too vital to ignore. A CMP that is well-designed, regularly reviewed and dynamic will create a culture of accountability and protect your business now and in the future.



Why Bovill Newgate?

At Bovill Newgate, we are specialists in compliance. We don't do anything else. We've been around for more than 20 years and we know what regulators want to see.

We can help you respond to a one-off compliance event, but we also strongly believe that compliance is a process rather than a project.

We can help you create and update a tailored and comprehensive compliance manual that sets out the most appropriate policies for your business. We provide ongoing compliance monitoring and support, including managing your coverage of regulatory developments.

We offer a tailored, personal service that is comprehensive but proportionate. For more information on what Bovill Newgate can do for you, please visit our website.



**Contact
our team**



BOVILL NEWGATE

An Ocorian Company

UK (London) | Guernsey | Mauritius | Hong Kong | Singapore | Americas

 bovill-newgate.com

Disclaimer

This technical information sheet is provided solely for general information. While every effort is made to ensure that anything contained herein is correct, Ocorian makes no representation, warranty or guarantee as to the accuracy, reliability, completeness, validity, suitability, or timeliness of the information. Ocorian neither accepts nor assumes any liability or duty of care for any loss arising from any action taken or not taken by anyone as a result of information provided. Readers are recommended to seek professional advice before taking actions. Ocorian will be pleased to discuss any specific issues.