

CLYDE&CO

Successful risk navigation

When risk becomes reportable:

How organisations navigate the moment of regulatory exposure

Investigations support defensible decisions, and it pays to plan the framework in advance.

2026 Corporate Risk Radar



Today, business leaders see the risk posed by their organisations' regulatory and compliance obligations increasing rapidly. Our latest Corporate Risk Radar research found that 85% of board members, C-Suite executives and General Counsel now consider this a major risk, up from 54% last year.

No wonder: multinationals face diverging, overlapping and fast-changing rules, enforcement priorities and reporting expectations around the world. Preventing regulatory breaches is not their sole concern: just as importantly, their response to any potential violation must stand up to scrutiny.

Whether to report suspected compliance failures to regulators is rarely straightforward. It's typically a highly complex judgement call made under intense time pressure with incomplete information, amid competing commercial imperatives and stakeholder interests. Often, there is considerable uncertainty as to what has happened, when notification is required and which authorities to inform.

Self-reporting, and a decision not to report, can each have significant legal, commercial and reputational consequences. Robust governance across global operations is therefore essential to support rapid escalation, proportionate investigation and a defensible decision based on the applicable legal and regulatory framework.

Reporting decisions are getting harder

Regulators are widening their scope, previously lighter-touch regimes are becoming more stringent, and multiple authorities may police the same activity within a single jurisdiction, resulting in a more complex cross-border compliance picture, and greater consequences from misjudging the response.

“

Many companies put a lot of faith in their compliance systems, and hope their prevention is so good, they don’t need to worry about enforcement action – but even the best compliance programmes have leaks.

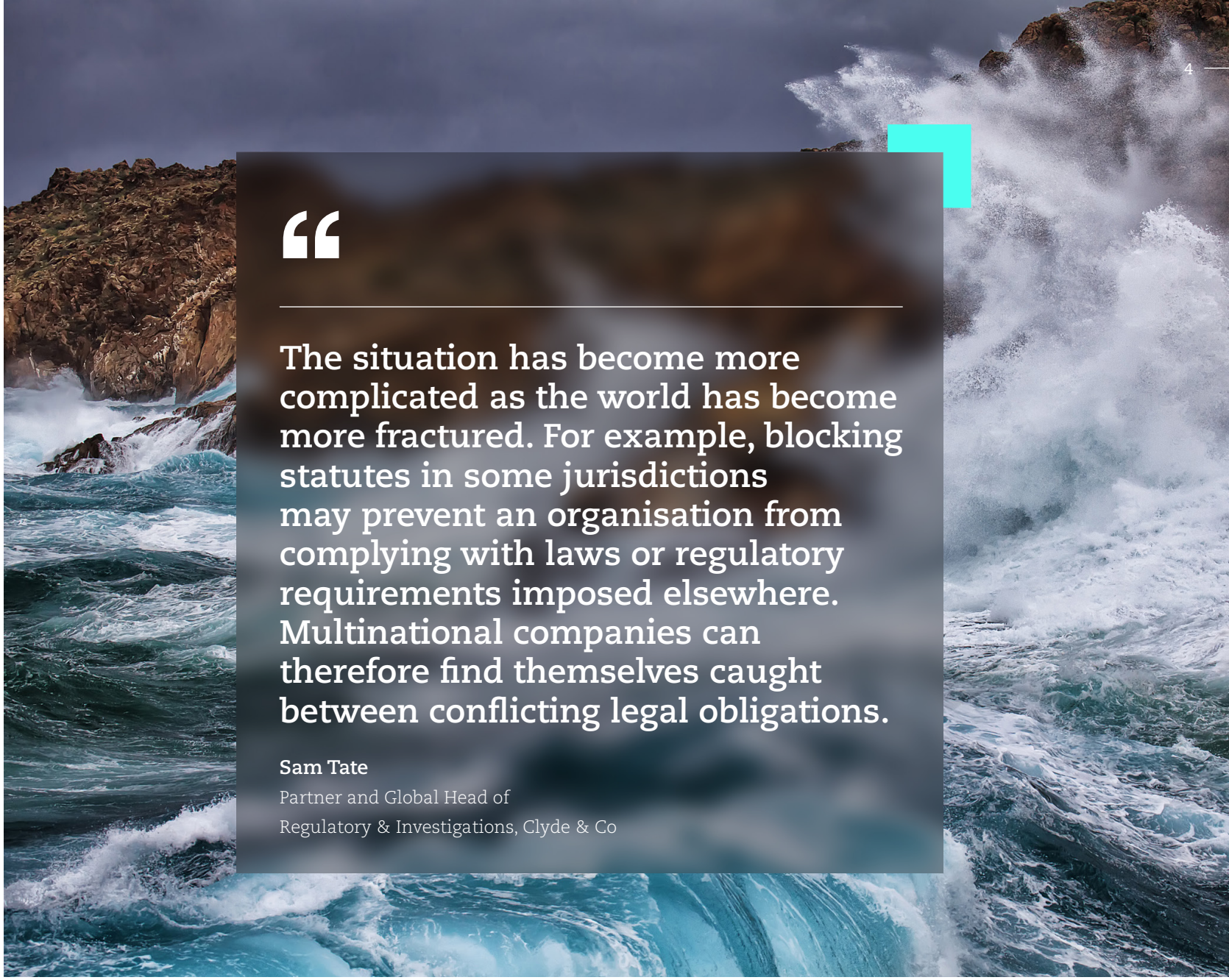
Jeffrey Cottle
Partner and Head of Regulatory & Investigations, Americas, Co-Head of White-Collar Crime & Sanctions, EMEA, Clyde & Co

After a suspected breach, regulators may examine not only the underlying incident but also the organisation’s response, including whether it preserved evidence, limited continuing harm, remediated control failures and engaged with authorities appropriately. A single incident, from an administrative error to control weaknesses, misconduct or suspected criminality, may engage several notification regimes, regulators and timeframes, as well as remedial action in multiple locations.

Confirming whether a breach has occurred will often require investigation. At the outset, an organisation may not know whether an allegation has merit, which legal regime applies or whether the relevant reporting threshold has been met. It may nevertheless need to act before the facts are complete because some notification obligations arise quickly and may be triggered by awareness, suspicion or reasonable grounds, rather than a final finding. The practical tension is clear: premature reporting can create avoidable regulatory and commercial consequences, while delay can result in a missed deadline, reduced cooperation credit, enforcement exposure and reputational harm.

“Organisations may feel required to report when they are not ready to do so,” explains Omar Khattab, Partner, Regulatory & Investigations, Middle East, Clyde & Co. “Now there are more channels to raise the alarm, such as whistleblowing hotlines, the press and even social media, which means that a company can face a storm all of a sudden without being prepared.”

Meanwhile, varying enforcement approaches can make the calculation about whether and when to report even more challenging. For example, US Safe Harbor provisions can shield companies that report suspected sanctions and other violations early from prosecution. However, in other parts of the world where no such protections apply, choosing to report early may have limited benefit – and might even be detrimental.



> **The situation has become more complicated as the world has become more fractured. For example, blocking statutes in some jurisdictions may prevent an organisation from complying with laws or regulatory requirements imposed elsewhere. Multinational companies can therefore find themselves caught between conflicting legal obligations.**
>
> **Sam Tate**
> Partner and Global Head of
> Regulatory & Investigations, Clyde & Co

Why reporting decisions require more than a compliance assessment

What is reportable and what isn't can be a grey area. Companies should assess what they know, what remains unknown, what the authorities expect and the benefits and risks of self-reporting (or not).

"You're unlikely to have complete accuracy on day one, but it should be possible to give some best and worst-case scenarios," says Rebecca Kelly, Managing Partner, Australia and Co-Head of the APAC Regulatory & Investigations Group, Clyde & Co. "It's important to make sure that people take regulatory exposure seriously, but equally that they don't over-react."

Reporting decisions involve more than identifying the legal threshold. Organisations may also need to assess cost, business continuity, staff, customer and supplier relationships, tender processes, insurance, financing and investor confidence. Potential regulatory, civil and criminal exposure should be considered alongside the likelihood that a regulator, whistleblower, contractual counterparty or other third party may disclose the issue independently. Commercial considerations should inform the response but should not override a mandatory notification obligation.

"In this regard, matters involving cross-border regulatory scrutiny may also involve an added layer of complexity, as companies consider the possible implications of cooperation amongst regulators in different jurisdictions", notes Weiyi Tan, Partner and Co-Head of the APAC Regulatory & Investigations Group, Clyde & Co.

Corporate culture can also play a part here. Some companies may be keen to report quickly to demonstrate their ethical credentials. Others may see little point in taking the initiative if they don't believe it will lead to more favourable treatment. Personal liability may affect the judgement: because board members can be held accountable for reporting failures.

While a protective, cautious approach can make sense, Anousheh Bromfield, Partner, Regulatory & Investigations, UK, Clyde & Co warns, "Once you report, you can't take it back, and you risk losing control of the narrative. Companies might later find, with a bit more fact finding, that a notification wasn't required after all. Given the potential unintended consequences of reporting, for example triggering other notification or disclosure requirements, it's important to get the timing of when and what to report right."

If a notification does need to be made, Khattab makes the point that,

"Proactive engagement with the authorities typically helps – radio silence or burying your head in the sand do not."

How investigations support decisions

This is where a robust investigation comes in: to provide a rational basis on which reporting decisions can be made.

The immediate purpose of an investigation is often to gain control of the issue and gather enough reliable information to support the next decision. Establishing the key facts, people involved, obligations, risks and possible outcomes, helps organisations triage incidents according to severity. They can then decide promptly whether to report, which authorities to notify and in what order, based on the relevant regulatory and business requirements.



> **It is also important at this stage to address preliminary legal issues that may arise in the investigations, such as legal privilege, employment laws and data privacy laws that impact the conduct of the investigations.**

Weiyi Tan
Partner and Co-Head of the APAC
Regulatory & Investigations Group, Clyde & Co



Exhaustive fact-finding can follow. Reporting decisions may need to be revisited as new information emerges, and companies should clearly document the reasoning behind them, preserving the evidence at every stage.

Ultimately, investigations are about protecting people, assets and operations. The scope of an investigation should be carefully controlled. It should be broad enough to address every salient point but proportionate to the level of risk. Over-investigation can generate information that confuses the issue, overwhelms decision-makers or gives regulators unnecessary detail.

Investigations need timely access to relevant information, the right internal and/or external expertise to separate fact from fiction, and to demonstrate authority. Companies could also consider where technology can help.

Significant or complex matters may require technology-assisted information gathering, forensic review by independent experts or specialist input across jurisdictions. Any use of artificial intelligence should be subject to appropriate human oversight and safeguards for confidentiality, legal professional privilege, data protection, cybersecurity, accuracy and cross-border data transfer. Engaging external counsel and structuring the investigation appropriately may support a claim to legal professional privilege, but privilege is jurisdiction-specific and is not guaranteed merely because an investigation is independent or lawyer-led. Where a matter is handled internally, an external legal, forensic, technology, data or sector specialist may provide useful assurance.

Pre-response preparedness: Why building the decision-making architecture in advance matters

“

In the first 24-48 hours, good organisations investigate quickly; great organisations govern effectively while the investigation is underway.

Rebecca Kelly
Managing Partner, Australia and Co-Head
of the APAC Regulatory & Investigations Group, Clyde & Co

Preparedness is essential. Effective responses tend to combine local identification, regional coordination and global strategic oversight, particularly where local judgements may overlook group-wide exposure. A matrix, mapping operations, locations and applicable rules, can provide a practical starting point.

Organisations can benefit from establishing the investigation priorities and processes and building the decision-making architecture before an incident occurs. This framework may include defining which issues require internal notification; identifying the available reporting channels and their recipients; clarifying the responsibilities of legal, compliance, management and the board; and setting thresholds for escalation to senior leaders or external advisers.

It should also establish the practical mechanics of decision-making: how matters are triaged, who forms the core response team, how privilege and confidentiality will be managed, where information will be stored, and how risk, actions and deadlines will be monitored. Internal and external communications, stakeholder management and business continuity planning may need to run in parallel.

“You’ve got to have a very well-coordinated battle plan,” comments Cottle. “You’ve got different capabilities, you’ve got different threats, and you’ve got to coordinate them multi-jurisdictionally.”

Those who design the investigative response plan may not be responsible for implementing it. Risk, compliance and legal teams may monitor regulatory change, maintain the plan and advise the C-suite and board. However, the plan should specify who will activate and oversee the response and who has final authority over reporting decisions, usually at senior level. Those roles may vary by incident type. The reasons for delegating decision-making authority should be documented.

It’s good practice for the investigations protocols to be clearly communicated, regularly updated and (where possible) stress-tested, with sufficient flexibility to adapt to the circumstances. Education and training are also critical: for example, gaining practical pre-incident experience through workshops based on realistic scenarios can help ensure people are ready for what they could face.

Bromfield adds, “Companies may want to review how their investigations and decision-making process has worked in recent years to see if there are patterns they can learn from, for instance issues they should have reported earlier or cases where they reported too early.”



> Whether to report your company to a prosecutor is about the hardest business decision anyone ever has to make.

Sam Tate
Partner and Global Head
of Regulatory & Investigations, Clyde & Co

Defensible decisions are a governance issue

No company can entirely eliminate the risk of non-compliance, so an organisation's response at the point of regulatory exposure is vital. In many cases this is not a narrow compliance issue, but a wider corporate governance concern, and for organisations operating across borders, a local incident can rapidly become a global problem.

Reaching a defensible reporting decision is difficult when information is incomplete, details are uncertain, deadlines are tight and obligations vary between jurisdictions. Robust investigations should give senior leaders the confidence to act – or not act – on a rational basis, by establishing key facts quickly, determining if a deeper dive is subsequently needed and documenting evidence. By being well-prepared in advance, organisations can remain in control when the reporting clock starts ticking.

How we can help

Clyde & Co has extensive experience helping organisations navigate risk around the world. Learn more about how we support organisations through a full-cycle regulatory and compliance advisory approach spanning prevention, investigation and enforcement.

Discover how leading organisations are responding to today's most pressing risks in our Corporate Risk Radar 2026 report, informed by interviews with more than 700 senior decision-makers across eight regions and benchmarked across ten sectors.

Read the Corporate Risk Radar Report

Clyde & Co contributors



Anousheh Bromfield

Partner, Regulatory & Investigations, UK



Jeffrey Cottle

Partner and Head of Regulatory & Investigations, Americas, Co-Head of White-Collar Crime & Sanctions, EMEA



Rebecca Kelly

Managing Partner, Australia and Co-Head of the APAC Regulatory & Investigations Group



Omar Khattab

Partner, Regulatory & Investigations, Middle East



Sam Tate

Partner and Global Head of Regulatory & Investigations



Weiyi Tan

Partner and Co-Head of the APAC Regulatory & Investigations Group

Clyde & Co LLP accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary. No part of this summary may be used, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, reading or otherwise without the prior permission of Clyde & Co LLP.
© Clyde & Co LLP 2026