REPRINT

R&C risk & compliance

THE CHANGING REGULATORY HORIZON - 2021 EXPECTATIONS FOR RISK AND COMPLIANCE MANAGERS

REPRINTED FROM:

RISK & COMPLIANCE MAGAZINE

APR-JUN 2021 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

SAI GLOBAL
RISK | COMPLIANCE | SAFETY | ETHICS

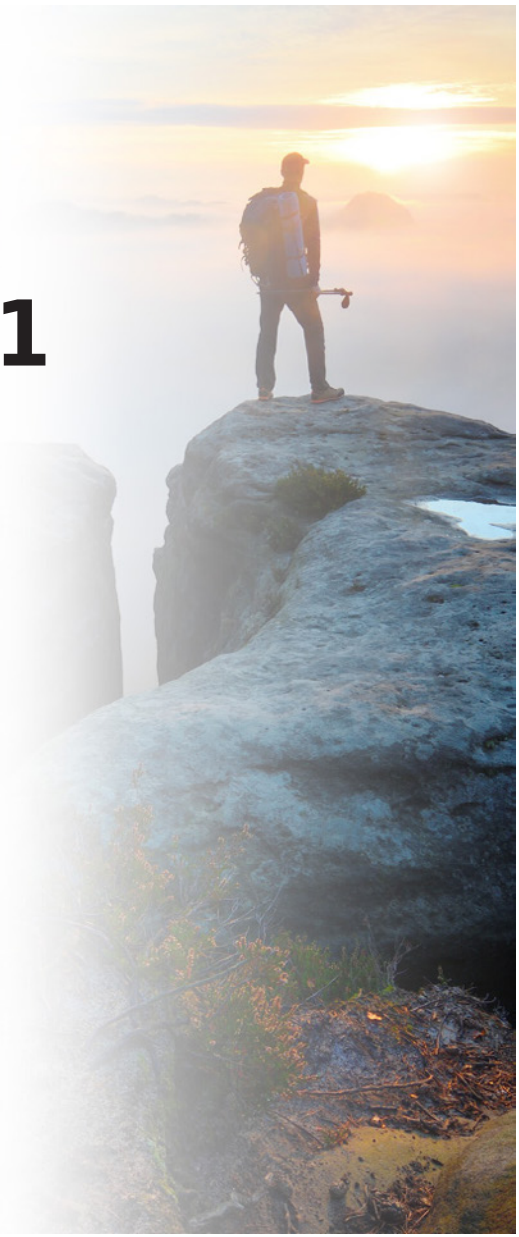
Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

© 2021 Financier Worldwide Ltd. All rights reserved.

www.riskandcompliancemagazine.com

ONE-ON-ONE INTERVIEW

THE CHANGING REGULATORY HORIZON - 2021 EXPECTATIONS FOR RISK AND COMPLIANCE MANAGERS



Paul Johns
Executive Vice President
SAI Global
T: +1 (917) 689 5876
E: paul.johns@saiglobal.com

A governance, risk & compliance (GRC) industry veteran, **Paul Johns** joined SAI Global in October 2017, bringing a wealth of experience and thought leadership, redefining how the business engages with the market and its customers. Mr Johns formerly led the global marketing strategy for Thomson Reuters' $6.1bn Financial and Risk division.

R&C: How would you describe the current regulatory landscape and the extent to which it is subject to change? What should risk and compliance managers expect as 2021 unfolds?

Johns: Coronavirus (COVID-19) upended regulatory plans and programmes in 2020 as pandemic relief for companies and their customers took precedence. However, regulators were still working on their programmes and supervisory priorities, so we expect an active regulatory environment in 2021 fuelled by the complexities of legislation post Brexit. In the UK, the topics we are watching in the regulatory landscape include the following. First, Brexit legislation requirements and the future stipulations for trading with the European Union (EU). Many organisations will need to address policies and processes to align with UK and European legislation. Second, imminent UK Sarbanes-Oxley Act (SOX) legislation and Sir Donald Brydon's review of reshaping the audit profession. As the UK exits the EU, financial reporting will also need to align. Many key FTSE 100 organisations are already addressing their risk and control framework and, as a result, the governance risk and compliance (GRC)/ integrated risk management (IRM) market thrives with new SOX initiatives. Third, rollout of the Financial Conduct Authority's (FCA's) Senior Managers and Certification Regime (SM&CR) and the completion for solo-regulated firms in March 2021. Many organisations have addressed this legislation directly in point solutions, however as programmes mature, this GRC use case is now finding its way into larger requirements. Finally, the Bank of England and the FCA's commitment to phasing out the London Inter-bank Offered Rate (LIBOR) by the end of 2021 raises additional compliance issues for companies and not only impacts existing lending facilities but also any new financing. There are also important ancillary issues such as environmental, social and governance (ESG), climate change and diversity. These are all taking place in an environment where companies are still managing through accelerated digital transformations and digitalisation of their processes. With the regulatory landscape shifting toward greater accountability, it is imperative for companies to focus

> **"One significant proposal could hold C-suite directors personally liable for the accuracy of a company's financial statements, much like the US version."**
>
> *Paul Johns, SAI Global*

on operational resilience and establish frameworks that recognise the interconnectedness of risk.

R&C: To what extent are proposals to introduce a UK version of US Sarbanes-Oxley (SOX) legislation gathering momentum?

Johns: Legislation is imminent. This is a process that has been ongoing since December 2018 when Sir John Kingman recommended replacing the Financial Reporting Council with an independent statutory regulator, the Audit, Reporting and Governance Authority (AGRA), to strengthen corporate governance and reporting in the wake of several high-profile accounting scandals. Two other government-backed reviews followed Sir John's report, including the Competition and Markets Authority's study of competition in the audit market in April 2019 and the Independent Review into the quality and effectiveness of an audit led by Sir Donald Brydon in December 2019. It was Sir Donald's 138-page report that suggested a 'UK SOX' framework – with chief executives and chief financial officers of major listed UK companies giving a statement on internal controls over financial reporting (ICOFR), reporting on any weaknesses – much like US SOX. So now we are here. It is widely expected that SOX-type rules targeting company financial reporting and audit oversight will be introduced at some point early this year. As of late February, the Department for Business, Energy and Industrial Strategy (BEIS) is expected to solicit feedback on its long-delayed white paper documenting 200-plus pages of recommendations set to be issued.

R&C: What might a UK version of SOX regulation look like? In your opinion, is it likely to mimic US standards, or make additional accommodations for foreign companies accessing the UK market?

Johns: There seems to be consensus that the standards should expand on current UK regulations rather than adopt additional and unfamiliar provisions. It is not as if the UK is starting from square one when it comes to internal controls, as the 1999 Turnbull report and its successors have put us already ahead of where the US was in 2002. Whatever version of SOX is decided on, it will have to be shaped by that history. The Audit Committee Chairs' Institute Forum (ACCIF) suggested that a framework for 'UK SOX' balance the cost of implementation and monitoring with the desired benefits and results in no additional requirements for organisations that already follow US SOX, Spanish internal control over financial reporting (ICFR) or Japanese SOX. One significant proposal could hold C-suite directors personally liable for the accuracy of a company's financial statements, much like the US version. Currently in the UK, liability rests with the company. However, it is expected that there will be serious penalties, fines and bans for major failures. Under any scenario, organisations should be looking to GRC/IRM vendors to make use of a unified

control framework, where true control harmonisation and greater risk management can be achieved. This is likely to mean rip and replace projects from older legacy software solutions. Key benefits will be a more efficient control framework that allows 'test once comply many' across all three lines of defence.

R&C: With Brexit achieved, what is the likely timeline for the introduction of SOX legislation in the UK? What factors could affect a rollout?

Johns: We agree with current estimates that the adoption of any proposed regulation likely will not come until 2023 at the earliest. Given that implementation can take upwards of 24 months for larger companies, organisations should be looking to deploy a test run by late 2021.

R&C: Would companies presumably need to adapt existing SOX compliance frameworks to accommodate new UK legislation?

Johns: If you are an organisation that already has US ownership, or you are listed on a US exchange, then you will already have a SOX framework. This will be a great starting point and the likelihood of a 'lift and shift' to new software will be the approach that most take. This provides a great opportunity to enhance and harmonise controls.

R&C: What initial steps should companies take to position themselves for a UK version of SOX legislation? What advice would you offer to risk and compliance managers on this front?

Johns: Companies embarking on a SOX framework for the first time should analyse their current process and protocols for financial control, the IT solutions that support the functions and where all risk data resides. I would recommend a thorough analysis of the internal audit lifecycle and the tools used for workpapers, risk-based control scoping and test procedures. Companies should adopt a three lines of defence model, incorporating management controls, risk and control monitoring and independent assurance. Risk managers on the frontlines should understand and appreciate that this is not just about UK SOX rules, but also the strengthening of their corporate governance and audit regime in general. Every organisation that goes through SOX implementation gains a much greater awareness of key areas of strength and weakness. It becomes a journey of maturity and allows for harmonisation. It is not without investment and therefore a robust business case needs to be built. To make that case, consider a three lines of defence model for implementation and retiring legacy software solutions in favour of SaaS-based cloud subscriptions. R&C