REPRINT

R&C risk & compliance

INTEGRATED RISK MANAGEMENT AND REGTECH – 'RISK-PROOFING' THE FUTURE OF FINANCIAL SERVICES

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2019 ISSUE

www.riskandcompliancemagazine.com

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

SAI GLOBAL

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

www.riskandcompliancemagazine.com

ONE-ON-ONE INTERVIEW

INTEGRATED RISK MANAGEMENT AND REGTECH – 'RISK-PROOFING' THE FUTURE OF FINANCIAL SERVICES

Paul Johns
CMO
SAI Global
T: +1 (678) 992 0262
E: info.emea@saiglobal.com

Paul Johns is CMO at SAI Global. An established risk and compliance thought leader, he has held CMO positions in a variety of technology companies with a primary focus in FinTech. Mr Johns has a wealth of experience across the full marketing, communications and investor relations mix.

R&C: How would you characterise the current readiness of companies to cope with the range of regulatory risks they face? In what way has this risk profile changed in recent years?

Johns: In the years since the financial crisis, the financial services sector has faced a torrent of regulatory requirements. After the crisis, regulators were focused on credit and market risks. But now they have shifted their focus towards non-financial risks — cyber and data stewardship and security, in particular. New regulations laid down by supervisory authorities are raising the stakes for data management. And call it a sign of the times; ethical questions around data privacy have gained significant traction thanks to the EU's General Data Protection Regulation (GDPR), which has armed consumers with a greater understanding of the value of their personal data and protections that have been made available to them. Our recent 'Global Reputation Trust Index' (RTI) dug deeper into consumer behaviours and cyber security: financial services data breaches ranked as the highest company crisis concern for those we surveyed. With the risk landscape continuing to be dynamic as other disruptive factors like imperilling regulatory change and an upsurge of informed consumers becoming the norm, this adds pressure on traditional risk management capabilities. To keep pace with the regulatory change, most firms have responded piecemeal to new requirements, often implementing a number of point systems to address specific regulations and quite often relying on one-time fixes. Moreover, these activities often take place in silos, and with software partners overpromising results, making it difficult to gain a comprehensive view of risk across the whole organisation. The challenge and opportunity is how to balance the rapid complexity of existing and emerging risks with cloud-based, data-led technological advancements.

R&C: To what extent are integrated risk management (IRM) solutions keeping pace with a changing regulatory landscape?

Johns: Risk management functions are traditionally siloed, divided into compliance, finance, audit, and other risk management functions like fraud, vendor management, IT, business continuity and operational risk. This has merit, but lacks foresight. Integrated risk management (IRM) is more than a three letter acronym. It is about a joined-up approach to risk management, one that facilitates a strategic and comprehensive approach to risk-taking. One of its key principles is connected collaboration; risk is connected and a connected approach to risk allows an organisation to add competitive advantage by rapidly deploying mitigation processes and streamlining monitoring of key risks across the business, so that appropriate action can be

taken where needed. After all, operationalising compliance activities is not a one-and-done exercise. Regulations such as anti-money laundering (AML), Know Your Customer (KYC), the Markets in Financial Instruments Directive II (MiFID II), Basel III and IV, the Second Payment Services Directive (PSD2) and GDPR require people, technology, data and process involvement to be sustainable. By implementing an IRM framework, an organisation has the ability to build a rock-solid wall of protection that reduces risks, minimises the overhead costs of governance and compliance, and provides maximum business insight across all operations. In addition, by streamlining compliance functions across silos, businesses can scale down from multiple, disparate teams supporting multiple solution vendors to fewer, more central functions. This enables businesses to reconcile data and results across teams and regions, and can lead to a reduction in costs associated with running multiple functions.

R&C: How can IRM programmes help under pressure companies maintain compliance across the many facets of their organisation? Specifically, how are RegTech solutions simplifying risk reporting and regulatory compliance monitoring?

Johns: RegTech solutions enable businesses to access compliance data that provides valuable insights into their businesses' vulnerabilities – often in real-time – in a cost-effective way to identify risks, predict compliance failures and enhance coordination across all levels of the organisation with capabilities like executive dashboards. Furcating risk information in this way allows for reporting simplification based on stakeholder needs. It also sets the framework for monitoring how the compliance risk profile changes.

> **"Integrated risk management (IRM) is more than a three letter acronym. It is about a joined-up approach to risk management, one that facilitates a strategic and comprehensive approach to risk-taking."**
>
> *Paul Johns, SAI Global*

R&C: In your opinion, how should organisations go about implementing an IRM programme that provides scalability, efficiency and reliability?

Johns: IRM requires a combination of technology, process and data that cuts across operating silos to vertically and horizontally connect strategy down through the organisation. With an IRM approach, compliance teams have access to a set of capabilities to modify, improve and streamline information-sharing, workflows and processes beyond the classical box-ticking exercise into a robust and dynamic programme. This not only accelerates time to value to relieve burdened compliance teams but also offers greater efficiency and visibility within an organisation, ensuring easily traceable audit trails, improved information management and data governance. When it comes to implementation, to start with, an organisation should take an inventory of its risk and compliance technologies and test for any blind spots, as well as to assess how current technologies facilitate or could inhibit the ability to create and deliver accurate, timely and complete data. Then, organisations should look to determine if they have access to all the risk-related data needed. In many cases this includes ingesting regulatory content from all the different jurisdictions where operations occur. Another consideration is determining if the right people are in the right roles, with the right level of training to perform their roles. IRM is also a great enabler to build a strong culture of ethics and compliance by fostering a top-down, ethics-focused and risk-based culture throughout the organisation. Developing the right ethics, values and risk culture with risk and learning solutions can do more in a single day than a technology-only solution.

R&C: What are some of the typical challenges associated with RegTech implementation and how can organisations overcome them?

Johns: The proliferation of regulations across the globe has put added pressure on the efficacy of RegTech investment as new regulatory requirements often come into play without clarity into regulators' expectations. Its implementation must also account for geographic footprint; many compliance departments must understand how regulatory edicts translate into various countries and jurisdictions. Granted, for some regulations, like GDPR, this is more simple. For others, like MiFID II and Dodd-Frank, there must be an infrastructure for compliance departments to substantiate conformance. RegTech must be flexible enough to allow for these differences.

R&C: How important is it for companies to link RegTech solutions to strategic objectives, business operations and IT security? What considerations should they make in this regard?

Johns: While RegTech offers measurable return on investment (ROI), the biggest benefits are

strategic and operational – bridging the gap between regulators and business, while protecting the best interests of consumers. The biggest challenges facing the financial services industry are data quality, cost constraints, legacy systems, manual processes, complex compliance, siloed operations and regulatory uncertainty. At the same time, the industry is also under scrutiny and pressure from supervising authorities and customers to protect their data from fast-moving challenges, such as cyber security. In our RTI, 65 percent of those we surveyed viewed data privacy as the most important attribute when considering a company's trustworthiness, so it is not hard to understand why firms are undertaking reviews of their overall compliance strategies to reflect the growing regulatory emphasis on consumer rights and data privacy. Governance of data needs to be a board-level issue, with significant implications for strategy, business model, IT architecture and capital investment, as well as assurance, reporting and management structures. Differing silos equate to disparate data, security and reporting standards and norms. Standardisation and collaboration are critical to successful implementation, as well as with regulators, third-parties and across industry sectors. Firms need to consider their overall relationship with technology: how will they serve the customer, and how will they compile, monitor, flag and report data to different department stakeholders, as well as regulators?

R&C: With new and higher levels of regulatory risk continuing to emerge, how do you foresee the IRM market maturing in the years ahead?

Johns: As we are in a period of substantially greater strategic risk – more sophisticated financial crime, for example – we are seeing more organisations considering how to enhance their ability to manage both external and internal enterprise and operational risks. While organisations rely on disruptive digital transformation – technology to drive digital change in the future – risk teams expect to do so, too. The function itself will become clearer, streamlined and much slimmer with a rationalised risk infrastructure that uses location and delivery models for cost optimisation and leverages the power of digital for efficacy. We will also see a shift away from a compliance-oriented risk mindset to that of a strong and proactive risk-aware culture. Conduct, ethics and culture management will be pervasive throughout the organisation. We also expect to see more powerful tools that provide greater insight into risk to inform decision making, allow an enterprise-wide view of interdependent risks, simulate impacts and provide real-time and predictive intelligence and analysis. R&C