# PLANNING THE NEW NORMAL: STRATEGIES FOR RISK AND COMPLIANCE

Carlo di Florio
Partner & Global Chief Services Officer
**ACA Compliance Group**
Email Carlo di Florio

Martin Lovick
Director
**ACA Compliance Group**
Email Martin Lovick

COVID-19 plunged the world economy into the worst recession and unemployment crisis since the Great Depression. The pandemic shuttered companies and dispersed employees to work from home where possible.

This remote work paradigm challenged financial firms to deploy their business continuity and operational resilience plans.

Compliance and risk leaders must continue to strategize, embrace change and modernization to re-imagine their functions to drive cost savings while maintaining effectiveness.

The pandemic provides a fast-forward insight to the regulatory trends and industry forces that are driving the future of compliance and risk.

We're seeing a range of industry drivers that have inspired three key strategies to adapt within this new paradigm.

## Strategy 1 - Leverage technology to transform compliance and risk functions while delivering big cost savings

**Regulators have overtaken investment managers:** historically, managers had more sophisticated technology than the regulators - this has changed since the 2008 Financial Crisis. Regulators globally have made significant investments in technology, big data and advanced analytics, also experimenting with artificial intelligence, including machine learning, natural language processing and robotic automation.

**The distributed workforce:** post-COVID, firms are quickly realizing that work-from-home is viable, more efficient and expands the talent pool. All departments need to be equipped to operate as a remote work-from-home team at a moment's notice and for extended periods.

Team collaboration by shouting over a cubicle wall isn't just impossible in today's distributed workforce, it also unfavourable as it leads to poor record retention and an inability to capture useful metrics to measure performance.

**Centralised data:** bringing data sets together empowers compliance teams to do more, faster, and enables a holistic approach to surveillance. For example, orders, trades, and positions are required to complete regulatory filings, transaction reporting, and systematically monitor for inappropriate trading activity. Fees and expenses must be captured to identify potential conflicts and improper allocation issues. Investor data is needed centrally for AML purposes. Electronic communications data is required to conduct surveillance. Firm and personal trading data for detection of market abuse, investment mandate violation, front running and other personal account dealing risks.

**Scale necessitates automation:** personal trading compliance systems now incorporate elaborate brokerage integrations with rules-based processing: a complex web of "if-this-then-that" logic can be applied to new trade data to determine if the trade needs investigation, if it was automatically cleared, or if it corresponds to a trade request that was preapproved.





In the future, firms will rely on more advanced rulesets – for example, a restricted trading list (RTL) specific to a particular product area (e.g. private markets).

**Outsourcing and third-party risks:** with greater distribution comes increased reliance on managed services and outsourcing – an on-demand set of capabilities that is more cost-effective and efficient in delivering repetitive operational tasks to scale. In-house resources will continue to drive strategy, oversight and decision-making.

As firm boundaries expand, a plethora of third-party providers become involved in efficient operations. Many of these 'warehouse' important data or are operationally or financially critical. Third-party risk oversight cannot be a one-time review, or even an annual review. Technology is required to conduct and manage this workflow.

**Accessibility:** firms must react to their environments very quickly and compliance must be ready to support the distributed workforce. Chat bots and automated business assistant integrations will become commonplace to address common employee questions and reduce the burden on the compliance team. For example, "Is IBM on the restricted trading list?" is a question that a compliance bot can readily answer.

## Strategy 2 – Outsource to drive better outcomes and flexibility at reduced cost

**Task specialization:** is the CCO the best person to review and approve marketing materials? If resources are not available internally or turnaround times are not meeting the business expectations, an outsourced solution is likely to yield immediate benefits. If senior professionals are spending too much time on operational minutia, then high risk areas may not be getting the appropriate attention.

**Operational agility:** this is critical for high-volume, time-sensitive tasks with extended hiring and training periods, or where workflow fluctuations can be seasonal or unpredictable. These time-sensitive tasks may also be time-consuming tasks – email surveillance rabbit holes, 60 to 90-minute expert consultations that need to be chaperoned, long DDQs that need to be reviewed. Utilizing a third-party service provider for these tasks protects against staff turnover and unexpected demands.

**Technical expertise and peer benchmarking:** addressing some risks require specialised knowledge and expertise – for example, cybersecurity - but the amount or seasonality of work may not justify adding to the headcount. Also, few firms want to be outliers when it comes to addressing regulatory obligations. Service providers offer insights on best practices and trends, as well as peer benchmarking.

**Investor expectations:** clients and investors insist that managers have robust operational infrastructure – a focus certain to increase post-COVID. Due diligence will examine in detail the sufficiency of the firm's resources, expertise, and resilience. Engaging with a service provider can help provide assurance that these expectations are being met.

## Strategy 3 – Drive operational resilience to optimize cyber, BCP and 3rd party risk management

**Top regulatory priority:** operational resilience is a top priority for regulators, effectively replacing financial resilience that has been the focus over the past decade. The SEC has targeted pandemic response questions centered around resilience on their recent examinations and inquiries are also coming from the NFA, FCA, Bank of England and other regulators. For example, its presence as a key area of focus in the FCA's 2020/21 Business Plan and the SEC's Office of Compliance Inspections and Examinations' (OCIE) recent Cybersecurity and Resiliency Observations Risk Alert focuses on the need for managers to manage their operational resiliency.

**Integrated frameworks:** many firms historically addressed the capability to maintain operations during crisis through business continuity and disaster recovery plans - these were often inadequate and poorly tested. An operational resilience program – properly implemented - gives firms the framework and tools needed to respond to crisis including the following key components:

- Programme governance
- Business continuity and resilience
- Third-party and supply chain resilience
- Cybersecurity resilience
- Technology infrastructure resilience
- Digital systems and software resilience
- Data and information resilience
- Training, testing and feedback loop

**The Path Forward:**

While the above have tended to have a discrete role in a firm's business operations - it is now critical to have a holistic approach to govern and manage these disciplines in an optimal way. We are experiencing a perfect storm of interconnected geopolitical, economic and environmental threats. Embracing smart technology, outsourcing and cyber solutions will help firms survive - and even thrive - despite the storm.