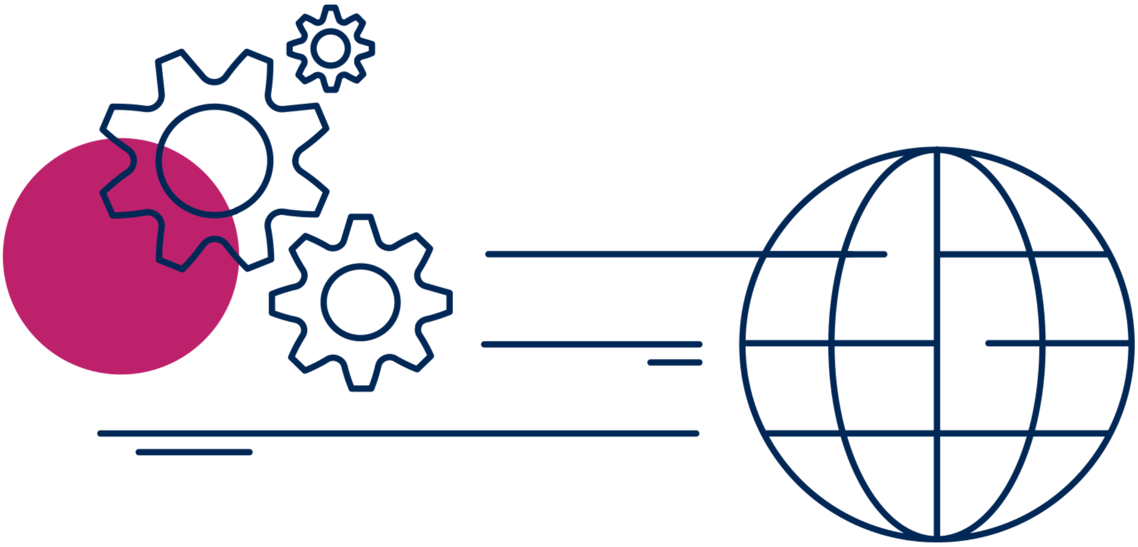
Bovill

Operational resilience in the new normal

Building a practical resilience framework for a remote workforce



Operational resilience in the 'new normal'

The Covid-19 crisis has tested firms' operational resilience in a number of ways. Some of these issues will lessen in importance as the crisis subsides, but others are going to become an integral part of our risk landscape in the future. Foremost among these is the change in working patterns to a more remote model. In Hong Kong, the Securities and Futures Commission has laid out its expectations when it comes to the long-term operational implications of managing a remote workforce.

The SFC's report, published on 4th October 2021 sets out regulatory standards to promote the operational resilience of intermediaries. The report also discusses measures to manage the major possible risks of remote working arrangements, including working from home.

Julia Leung, the SFC's Deputy Chief Executive Officer commented on the publication: "Disruptions are unavoidable and it is crucial for intermediaries to have in place a proper framework to prepare for, adapt and respond to disruptive incidents and to ensure continued operational resilience. As a hybrid mode of working is going to be the new norm, firms should also be vigilant about the risks associated with remote working, especially when it comes to cybersecurity, information security and data privacy."

The report shares examples and lessons learned drawn from the SFC's review of some licensed corporations' operational resilience measures during the pandemic and other disruptive events.

Assessing the impact of remote working on operational controls requires a comprehensive review from strategy down.

Strategy and business plans

Covid-19 kicked a hole in most business plans. Revenue targets have been missed and there has been an even greater focus on cost control. But against this backdrop, firms still need to recognise that the enhanced controls they will need to manage remote working will inevitably come with a price tag.

The pandemic brought in a period of enforced accelerationism. Firms can embrace this (and the changes that will come from the flexible workplace model). Or they can seek to return to their status quo position, in a world that has moved on.

Team effectiveness

Whilst plans have, in the most part, worked effectively, it is fair to say almost everyone is now suffering BCP fatigue. Frameworks that were intended to be in place for days have been stretched

“”

…firms should be vigilant about the risks associated with remote working .

over many months. And it is becoming increasingly difficult to maintain focus and motivation within teams – demotivated people make mistakes.

There is an increasing requirement for managers to step up and deliver effective performance. Unfortunately, much of the current managerial skillset tend towards the custodian not the coach – keeping people at their desks and on task, rather than inspiring and motivating.

Firms should identify and empower those leaders who can bridge these increasingly stretched spans of control, in the new decentralised working environment.

Ways of working

Firms faced challenges with siloed working when teams were a few desks or floors away. Stretch that to miles and the situation has the potential to get considerably worse – with no more watercooler conversations or ‘management by walking about’. This presents a challenge for senior management, and for control functions to get those early insights into potential issues and risks.

Without the availability of informal channels, firms need to be much more active in ensuring information still flows, and that all relevant stakeholders are involved in discussions.

Key person dependency and succession planning

Covid-19 has taken its toll on workplaces across the globe. And the aftereffects will reverberate long after the crisis is over – any shock is followed by a period of reflection, and as the employment market improves, many staff will be reconsidering what they want to be doing in their working lives.

Across many firms, when succession plans were dusted off and taken down from the shelf, they bore very little relationship to the organisational reality. Equally, many organisations were left exposed as they did not appreciate who the key people were (and the fact it often had very little to do with job title).

It is important that firms maintain clear and up-to-date succession plans, and reflect key person dependencies within their operational risk considerations.

And in some cases, personnel may not be able to rise to the challenge, and manage at a distance. Firms will need to consider changes.

Outsourcing

Managing outsourced providers is a challenge at the best of times. But the lack of face-to-face contact has made this all the more difficult. It is important for firms to formalise and document these interactions to ensure the full range of issues are considered (both commercial and conduct).

The increased focus on operational issues may also have identified outsourcing activity which should be considered material. If this is the case appropriate steps should be taken to enhance monitoring and control these increased risks.

Inevitably there will be some outsourcing relationships which are no longer operating within risk appetite (or will not be so within a remote working environment). If they can't be brought back within tolerance, firms will need to consider exiting the partnerships.

Risk landscape and recovery plans

The scale and impact of the pandemic was not anticipated. The next crisis will not be the same, but the lessons learned here can enable firms to be much better prepared. The next 'black swan' will look different from the last 'black swan', but the likely impacts can be quantified.

Clearly, Risk Control Self Assessments (RCSA) and Business Impact Assessments (BIA) will need to be revisited in light of Covid-19, and also with a view towards changing future work practices.

There should be a greater consideration of second order impacts, cascading risks and systemic issues – with an appreciation that remote working brings an increased fragility to the control framework.

Fire drills and red team exercises

The pressures of dealing with a very real crisis put paid to many fire drills and red-team exercises during 2020.

It is important that firms get back on the testing cycle as the inherent risks have not gone away and will only be amplified by Covid-19. And it's vital that these testing plans reflect the operational environment the firm is in. Testing plans should be amended and developed in light of the pandemic and new ways of working. And the focus should not just be on impact to the firm, but to customers and counterparties too.

Governance

All the points above have Governance at their core. It is the senior management that have the ultimate responsibility for ensuring that risks are controlled and learnings are taken.

It is fair to say that the performance of Governance structures has been mixed, during the pandemic. Job Descriptions and Org Charts were often more of an aspiration than a documentation of fact. It was clear that the responsibilities and capabilities were not always where firms expected them to be.

Firms will need to address these issues as they develop their operational frameworks for the future, to ensure there is sufficient expertise to achieve delivery, and also to provide oversight and challenge.

For many firms enforced remote working of the pandemic is being seen as an opportunity to change the model in the future. However, this opportunity has risks attached, which should be fully considered, if operational resilience is not to suffer.

Building a practical framework for operational resilience in a remote working environment

From the top to the bottom of the organisation, and across insourced and outsourced services, remote working presents operational resilience challenges. Even after Covid-19 is no longer an issue, it's important to recognise that things will not return to the status quo.

Remote working is going to be (to a greater or lesser extent) a part of the operational delivery framework. While it has felt like this has become BAU, the controls and the mindset in most organisations have not caught up. Simply continuing the current practices in a post-lock down world will lead to significant risks of operational failures and regulatory action.

Firms need to formally assess their operational models and control frameworks and develop clear processes and procedures to ensure operational resilience, both inside and outside of the traditional office environment.

Within this there are key areas to consider. Here we look at the challenges of each and how to prioritise your approach.

Governance

It is the responsibility of boards and senior management to assess and control operational resilience, regardless of the working environment.

With the added complexities of remote working, it will be essential for firms to have absolute clarity on roles and responsibilities, particularly where there is a spilt between operations and IT oversight, or between resourcing and budget setting.

The regulators expect firms to take responsibility for their own approach and for the appropriate level of risk control.

Governance around operational resilience is part of a broader discussion on board/exco effectiveness. But there are a number of elements that organisations should keep in mind (see over).

> Covid-19 has been a ‘teachable moment’ for the world, but not all will learn from it.

- Board/exco members should be upskilled or recruited with sufficient competencies to have an informed discussion – particularly on areas such as IT, data protection and cybersecurity.
- Enough time should be devoted to review and debate. A regulator may ask: how soon before the meeting were papers presented, what was the overall volume of material in the board/exco pack, how much time was allocated on the agenda?
- Board/exco should be able – and inclined – to have active discussions on complex and subjective issues, and arrive at risk-based decisions which they will be prepared to stand-by and justify.
- A framework should be in place to record and evidence actions.

Culture

Closely aligned to governance is company culture. Organisations should consider the extent to which their ‘lived culture’ (as opposed to the aspirations on their intranet) will help or hinder their aims to control operational resilience in a remote working future:

- Don’t ask, don’t tell
  A combination of incurious management and staff who do not feel empowered to raise concerns is a recipe for failure.
- Closed mindedness
  An inability to learn from mistakes or seek out root causes will hamper the change process. Covid-19 has been a ‘teachable moment’ for the world, but not all will learn from it.
- Lack of customer focus
  An organisation that, at its core, does not fully understand the needs and requirements of its customers and clients, will not be able to build resilient systems.
- Siloed working
  Remote working will make any inherent issues far worse.

> All the risks identified within the firm will also be present within third party providers. And these risks will be harder to identify and control

Control

Your risk identification and control processes will need to be strengthened and refocused for the specific risks that remote working brings.

Policies, procedures and controls should be re-assessed and stress tested for a remote environment.

Guidance and standard operating procedures (SOPs) should be updated to take into account remote working.

A more formalised approach will need to be taken to review points and updates – as those casual conversations and drop ins will not be happening.

Increased training and developing will be needed for line managers and oversight personnel. You shouldn't expect that people are automatically competent to manage remotely – what has been sufficient during the Covid-19 crisis will not be sufficient, long-term.

More active and formalised assessments will be required, with specific considerations of the inherent risks of operating in a remote working environment.

Periodic face-to-face meetings or site visits should be part of the control framework.

Outsourcing

Regulators have been highlighting concerns with the control of outsourced providers, well before the pandemic. The continued practice of remote working only brings an additional layer of risk, and the control requirements that come with it.

Many third parties had historically been working on firms' premises – which afforded easy access and oversight. If they will be working remotely in the future this will require a rethink of the control requirements, and a greater focus on oversight.

Even when third parties were operating from their own premises, physical visits and reviews were easy to undertake. With a decentralised operation, this will require more active and planned oversight.

When it comes to outsourcing controls, you should consider:

- The frequency and extent of the reviews you will be undertaking. And the level of communication expect from the third party.
- Whether current contracts are sufficient to cover the new working environment.
- If you should accept remote working practices at the third party (even if you allow them for your own staff). The risk and

responsibility remains with the regulated firm, so you should control the third party accordingly. It should not automatically be assumed that risks which are excepted internally can be excepted at another party.

- To what extent the third party has adapted and changed their control framework, in response to the new normal. If third parties are simply reverting to BAU with a few cosmetic tweaks, they may not have an acceptable risk culture and risk awareness.

Business continuity

Business Continuity Management (BCM) has, in the most part, performed very well during the pandemic. However, you should not assume that a BAU approach will be fit for future. There should be a clear refocussing within organisations to develop a BCM framework suitable for extended and ongoing remote working. Key considerations include:

- Revisiting plans, and ensuring they are still fit for purpose.
- Engaging with third parties and outsourcing providers to assess the increased levels of risk.
- Ensuring Business Impact Assessments (BIAs) are sufficiently wide in scope. Regulators expect firms to consider the broader impact of business interruption
- Considering how information can be communicated, and how staff can be kept informed of developing situations (the office tannoy will not be sufficient).

IT resilience and data and cyber security

Firms can outsource capability, but they cannot outsource responsibility.

Remote working has exponentially increased the risks. There are now far more points of entry and opportunities for data loss. It's important to be proactive in plugging these gaps:

- A greater increase in monitoring – assessing what staff are doing, and when. This should be risk-based and reflect the activities particular staff are undertaking.
- Increased access controls – disabling USB ports, Bluetooth and printing.
- Providing greater training and guidance to staff on how to use and control data
- More specific pen testing and red team exercises focused on remote working risks.

> You'll need to be more proactive in reaching out to staff and not assuming that 'silence means approval'

- Sufficient granularity in access controls, to ensure only the right users have access to information.
- Clear policies and procedures regarding the use of own devices.
- Multi-factor authorisation.

Data and cybersecurity is part of an overarching IT resilience framework. Maintenance and upgrades of IT systems should be undertaken with due consideration of the risks of remote working. Testing will need to be far more rigorous and tailored.

People risk

The people factor is the constant across all operational resilience issues. And in remote working environments the control, oversight and development of people is stretched. Firms need to be much more active and targeted in their monitoring, training and performance management. Key issues include:

- Enhanced risk of fraud
  Appropriate controls and procedures should be put in place to ensure the correct level of verification and counter signing. The use of video technologies can assist in providing visual evidence of identity as can data analytics to detect issues.
- Staff misconduct
  Without managers overseeing staff, there are increased risks of poor behaviour – breaches of compliance rules, or activities like market abuse. Firms will need to put in place enhanced monitoring and oversight to guard against risks. Controls should be risk-based and focus efforts on the key areas of the organisation.
- Staff demotivation and isolation
  Remote working will not suit all employees. Management should actively engage with staff and closely monitor their mood, as well as their performance. You will need to be more proactive in reaching out to staff and not assuming that 'silence means approval'
- Counter-cultural behaviours
  Remote working means it's more important than ever to ensure employees share and follow the positive cultural values of the firm. Investing in culture is one of the most important mitigants to guard against poor behaviours. It is for senior management to reach out to employees and actively promote and reinforce good behaviours.

Remote working is a journey not destination

The pandemic has felt like an eternity. But in real terms, we have transitioned to a completely new way of working, in a very short space of time. The control frameworks, and people's attitudes are still catching up.

Done right, remote working has huge opportunities for firms, and for staff:

- Reduced office overheads
- Increased work life balance.
- Increased productivity.
- A vastly increased geographical catchment for workers.
- Increased resilience, when the (sadly inevitable) next crisis comes.

But these benefits should not come at the expense of poor customer outcomes, market instability and regulatory infractions.

Building resilience for the long term

Forward looking organisations will take the view that if they are going to be required to spend considerable time and effort analysing their businesses, they should be asking 'why' questions as well as 'how' questions. They should be taking the learnings from the Covid-19 experience and building them into a wider consideration around the overall longevity of the business model.

There needs to be a clear focus on the strength of the operational infrastructure, but this should be within a broader consideration of the sustainability (and potential vulnerability) of the value chain. In essence, resilience is getting through the day, but longevity is getting through the decade.

In essence, resilience is getting through the day, but longevity is getting through the decade…

Frank Brown

Practice Lead, Risk and Transformation

Based in London, Frank is Bovill's expert in Operational Resilience, working with clients to understand there local regulatory obligations and build resilience frameworks for the future.

fbrown@bovill.com

Clarissa Lam

Team Head, Hong Kong

Clarissa leads the Hong Kong team and is an expert in SFC regulation..

clam@bovill.com

About Bovill

Bovill is a specialist financial services regulatory consultancy, established in 1999 and headquartered in the UK with offices in London, Singapore, Hong Kong and New York.

Our sole activity is the provision of high-quality, technically-focused advice and consultancy services on all aspects of financial services regulation. We aim to develop effective solutions to the complex problems of our clients, and do not offer commoditised advice or services.

Bovill Asia (HK) Ltd

Room 407, 4/F, Sun House,
181 Des Voeux Road Central, Sheung Wan,
Hong Kong

www.bovill.com

Bovill