Where Transformation meets Trust

Igniting digital transformation and embedding operational resilience into highly regulated organisations

An Airwalk Reply Guide for UK Financial Services Leaders

REPLY
AIRWALK

The past two years have brought unprecedented disruption to the global economy, and organisations across all sectors have been forced to react and respond in haste. Many of those that have been able to successfully navigate the turbulence have come out the other side in robust shape. Of course, there are many examples of organisations that have not fared so well.

The future looks less punctuated by lockdown, but could be no less turbulent because of; war, economic recession, inflation and a property downturn. Just as the world emerging from its post-covid hangover, a host of global and macro-economic challenges have taken its place.

For financial services organisations, 2023 looks to be a year for consolidation and restraint. But it should also be seen as an opportunity to build the next evolution of your organisation – particularly when it comes to technology and digital foundations.

JFK once said "fix the roof while the sun is shining", meaning get your shop in order while times are good, not when things are tough.

The challenge for financial services is that the road ahead is not straightforward. Return on equity continues to be a challenge in the sector, and new entrants (particularly those pesky technology giants) are becoming much more serious in their adventures into the regulated realm.

This is not the time for sitting back, or for cutting investment in technology to the minimum. In a year or two, when things will perhaps have calmed somewhat in the global economy, those that have spent the time continuing to invest in their digital services, in adopting modern ways of working, becoming more operationally resilient – these are the organisations that will be stealing the march on their more cumbersome or change-averse competitors.

In this eBook, we explore some of the key themes for modernisation and transformation we believe will represent competitive advantage in the months and years to come within financial services. Some, like the adoption of cloud platforms and a more product-led approach, are not new, but are becoming increasingly compelling and fundamental. Others, like operational resilience, are somewhat ancient concepts coming to the fore in a much more modern and strategic way.

Ultimately there is no silver bullet – no single thing on a quadrant (magic or otherwise) that will make or break your transformation agenda. As with most things in life, it is about consistency, genuine investment and commitment, and the realisation that this is a marathon not a sprint.

And of course, the best way to get there is with a partner who knows how to get it done. Everyone at Airwalk Reply hopes we get the chance to be there on the journey with you.

Alex Hammond
Partner, Airwalk Reply

REPLY
AIRWALK

In this eBook

REPLY AIRWALK

The innovation imperative

Most IT leaders in the financial services space, particularly those who are already running most or all of their services in the cloud, understand that digital transformation is no longer a once-in-a-decade investment. It's an always-on imperative. Leaders who have not yet adopted this approach are acutely aware of the technical debt they have accrued with their legacy software and systems, but prior to Covid-19, many felt that the costs didn't warrant the investment that a digital transformation would require. Instead of embracing digital transformation, they opted for patches and incremental improvements to their systems.

Then along came the pandemic – and more specifically lockdowns – which dictated a different way of working for many; consequently, small technical developments are no longer sufficient. A full technological overhaul is now inevitable.

The next generation customer base has different needs. They are more geographically mobile and driven by ease of access and digital enablement rather than human interaction. They don't operate from 9-to-5. They want to consume services when it suits them. Britain's banks, have reacted to this by closing nearly half of their bank branches since 2015.

This reduction in bricks-and-mortar services corresponds to an investment in digital services. For example, the UK's Digital Strategy, recognising the strategic importance of the UK's technology industry, has committed to enhancing the digital infrastructure across the UK and promised heavy investment in areas such as AI, data and digital competition.

Organisations that aren't already investing in their own technology infrastructure could see the momentum of progress pass them by.

REPLY AIRWALK

Embracing partnerships – a lifeline for transformation

Few organisations can undertake the level of digital transformation required without the support of a dedicated network of partners and service providers. But there is a balance to be struck in retaining autonomy over an organisation's tech and digital security and leaning on partners who can provide the scalability and innovation to allow an organisation to focus on what it does best.

For any highly regulated organisation, digital transformation requires an entirely different technology stack and a different type of architecture. It is more about building a full ecosystem than a platform. As a result, much of the narrative in the past few years has explored the potential benefits that legacy financial organisations can gain from partnering with cloud service providers (CSPs) and other digital-first start-ups due to their expertise with new technologies.

There are a huge number of benefits in partnering with technology-led specialists to improve performance and productivity and enable scalability. We'll address some of those benefits and considerations later in this eBook. But the first partnership to consider is that between the financial service provider and its customers.

REPLY AIRWALK

Taking a customer-led approach

The 2008 financial crisis has had a long-lasting impact on the way organisations approach innovation. At its core, the crisis was a result of banks incorrectly managing risk, alongside regulators who were largely asleep at the wheel. As a result, regulators today are far more alert and apt to police industry developments. Likewise, bank leaders, wary of public perception and the fear of failure, are taking a cue from their risk, security and compliance teams and avoiding risk at all costs.

This environment has inadvertently slowed down the progress of innovation with financial service providers using risk and regulation as an excuse not to innovate. In reality, regulation merely provides oversight and ensures guard rails are in place to protect the bank and its consumers. Halting innovation is therefore more likely to have the opposite effect; causing regulation headaches down the line as banks will not be able to provide data transparency when an inevitable failure occurs.

IT leaders are generally aware of this risk, but with more hoops to jump through and added complexity, many opt to only pursue major digital transformations or big-bang opportunities. In some ways this is a hangover from the time of premise-era technology, when it was safer and more cost effective to upgrade systems every five (or even 10!) years than to continually innovate.

Instead, financial service providers must become more product-led where success is based upon customer outcomes. This means understanding their problems and desires, and then delivering solutions to these. Many financial organisations never leverage customer inputs, and developments are assumption-based. There is no emphasis on validating things before they are done. Ultimately, these organisations must focus on their customer rather their senior executives or their opinions, and adapt their approach to what works for customers and the organisation.

This is what makes cloud technology, data-process automation and product-led innovation such game changers.

Financial service providers must become more product-led where success is based upon customer outcomes

REPLY AIRWALK

The game changers

Cloud-enabled continuous innovation

When it comes to implementing a programme of on-going innovation, cloud has completely transformed the process. For example, CSPs have off-the-shelf SaaS offerings that organisations can use on a consumption model, test and see what happens. This eliminates the need to go out to market and procure a product or invest heavily in building their own. Utilising these services lets banks try new innovations at a significantly lower cost and on a smaller scale.

Furthermore, with access to cutting-edge technology and services, organisations are no longer restricted to what they are capable of building internally.

Continuous experiments and improvements are the gateway to innovation

Technology to remove risk

Process automation also has an important role to play as it can remove a lot of risk in the innovation process. With automated processes and delivery through code there is much less room for manual error - the main culprit causing systems to fall over in the first place. By becoming technology-led and automating processes, delivery and operational risk can be largely eliminated.

Establishing this baseline of components and processes in a stable and secure manner puts you in a much better place to innovate and try new things. Without this foundation, the process of securing and testing will need to be repeated at the beginning and at every phase of any innovation process, making each iteration more complex and expensive.

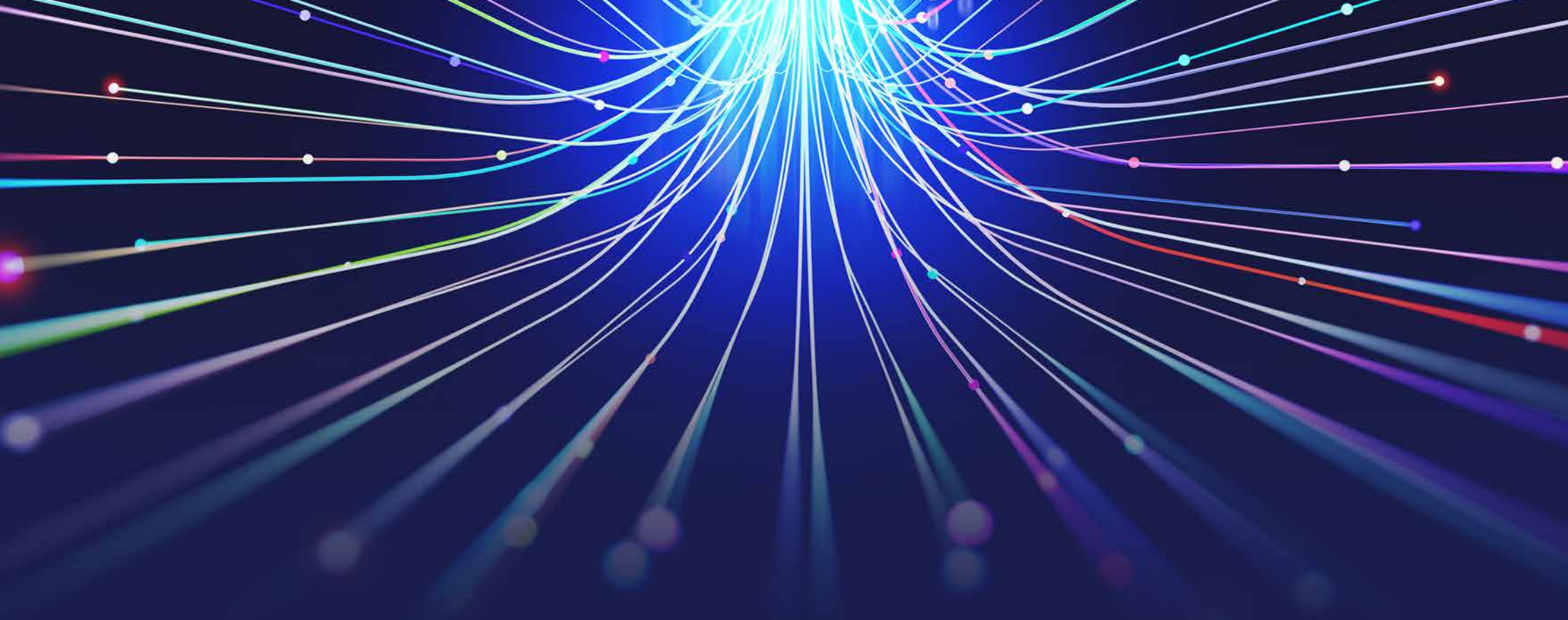
A product-led proof of concept approach

Rather than focusing on big-bang innovation, financial service providers should look to a more iterative and hypothesis-driven approach, embracing proof of concepts, but in their truest sense. Many organisations claim to do this, but their iterative development takes place internally prior to a large final release with no ongoing development. This may take months or years to bring to market, at which point the need may no longer even exist.

There is a clear opportunity to generate much smaller solutions which focus on a specific need or hypothesis, test these with a small number of customers and then scale what's successful. There is an inherent aversion to this within financial services, which does not exist in other industries, and it is holding them back.

All organisations need to evolve and keep pace with consumer expectations as digital services evolve in other areas of their lives. By becoming cloud enabled, automated and product-led, they can focus on incremental developments. In doing so, they become more agile and better able to drive forward innovation that is accepted by regulators and genuinely valued by customers.

REPLY AIRWALK



Five fundamentals to starting any digital transformation process

Any organisation undergoing a major digital transformation programme must have a combination of the right technology, the right processes, and the right people in place to realise its ambition. While every organisation in the financial service industry is unique, the following five steps are fundamental for the success of any digital transformation programme.

REPLY AIRWALK

1. Begin with an outcomes-based approach

The best approach to digital transformation puts customers at the heart of all design decisions. By looking at the end objective and the impact to the end user, organisations can evaluate improved or new processes that best meet their needs while working within organisational requirements. This may result in a new structure and part of the outcomes-based approach must include being open to the possibility of structural change.

2. Exploit existing technology to the fullest

Ask IT managers whether they would consider their organisation an early or late adopter of new technologies, many will say they're late adopters. Yet, according to Global Web Index data, 41% of UK IT managers are already using automation tools, while 31% are leveraging artificial intelligence and edge computing. These are emerging technologies, often on the cutting edge.
So, where's the disconnect? In some cases, financial service providers have access to capabilities that they're not exploiting to the fullest. This could include not integrating data sets between departments or retaining manual processes that could be done more efficiently through automation.

3. Create opportunities to attract and retain talent

Technology can and should be used and promoted as an attraction and retention tool. It can grant employees access to data that can help them make more informed decisions and it can remove the administrative burden of completing manual processes.
By investing in tech, you're investing in people and that must be included in any cost-benefits analysis.

4. Evaluate value rather than cost

An over-emphasis on costs can come at the expense of innovation, but it doesn't have to. The cost equation of adopting new technologies and processes should focus on value – both in the short-term and long-term. That includes the aspect of attracting and retaining talent, as well as efficiencies gained by automating processes, and by removing duplicate processes across departments. It should also be viewed through a long-term lens – anything you don't fix now will be harder and more expensive to address in the future, and in the meantime your customers may have gone elsewhere.

5. Connect data through the cloud

Cloud is undeniably the most transformative technology platform for any organisation today. Yet, while it has generally been readily adopted for front-end user services, it has not been as readily adopted for many back-office functions in the financial services industry. This siloed approach to information makes it impossible for senior leaders to connect the dots between departments and hinders the ability for employees to access all the data they need to make informed decisions. For end users, it results in frustration when they must share the same information with multiple organisations.

Ways of working are shifting to enable greater digital connectivity. By focusing on technology, talent, and value, organisations can ensure they are offering the best value to their customers – as well as becoming innovation leaders in the process.

Moving to cloud – adopting a DevSecOps approach to reduce the risk of a cyber-security storm

1. The need for constant vigilance and a DevSecOps approach

With on-premises solutions, cyber-security is managed on owned servers and are tested and audited prior to launch. They require initial investment and security checks, but they don't require the high level of ongoing vigilance that cloud does.

Risks on the cloud, however, change every day; and every device, from a connected computer to a connected fridge is a potential cyber-attack point. It's a moving beast for security teams to constantly monitor and address. Furthermore, cloud networks and Internet of Things (IoT) systems have produced a staggering proliferation of data making managing a network exponentially more complex.

This creates the need for security to become an ongoing, integrated part of the delivery lifecycle. Securing the cloud must be part of the development team's daily cadence, and a move not just to DevOps but to a DevSecOps model. This is a cultural shift that integrates security testing and protection throughout software development, deployment and operations. Engineers then become responsible for the security of what they build, possessing the knowledge to fix things in the correct way. This will change corporate attitudes to a zero-trust model of 'authenticate everywhere, never trust, always authenticate'. This approach of constant vigilance is a new way of thinking that also requires specialised expertise.

REPLY AIRWALK

2. A shortage of talent

According to a recent DCMS report, the recruitment pool for cyber-security professionals has a shortfall of 10,000 people a year, despite being the most sought-after tech skill in the UK.

Reliance on traditional security, risk management processes and auditing measures in the financial services space has resulted in a lack of cloud-skilled IT teams, as the trend has long been for IT and security support to be operationalised and executed by more junior (and often offshore) resources. With cloud security, there is a growing concern about the lack of highly skilled, experienced, and cloud-knowledgeable professionals to tackle these challenges. There is a naivety and over-reliance on the CSPs (such as AWS, Microsoft Azure or Google Cloud Platform) for financial services organisations to take on this burden for them.

3. Handing over security responsibilities to a CSP

Existing in a cloud ecosystem means participating in the shared responsibility model, as both CSPs and their customers have some degree of management over security in the cloud. Some IT teams mistakenly believe that when a bank uses a CSP, all its data-security requirements are managed by the provider. However, banks are still required to ensure the security of their customers' data and should be able to audit the security provisions of the companies that manage and control their data. To further complicate this, CSPs do not always make it easy for companies to access their security protocols – there is a culture of, "there's nothing to see here," which cannot be reconciled with the regulators' need for demonstratable security and control.

REPLY AIRWALK

The silver lining

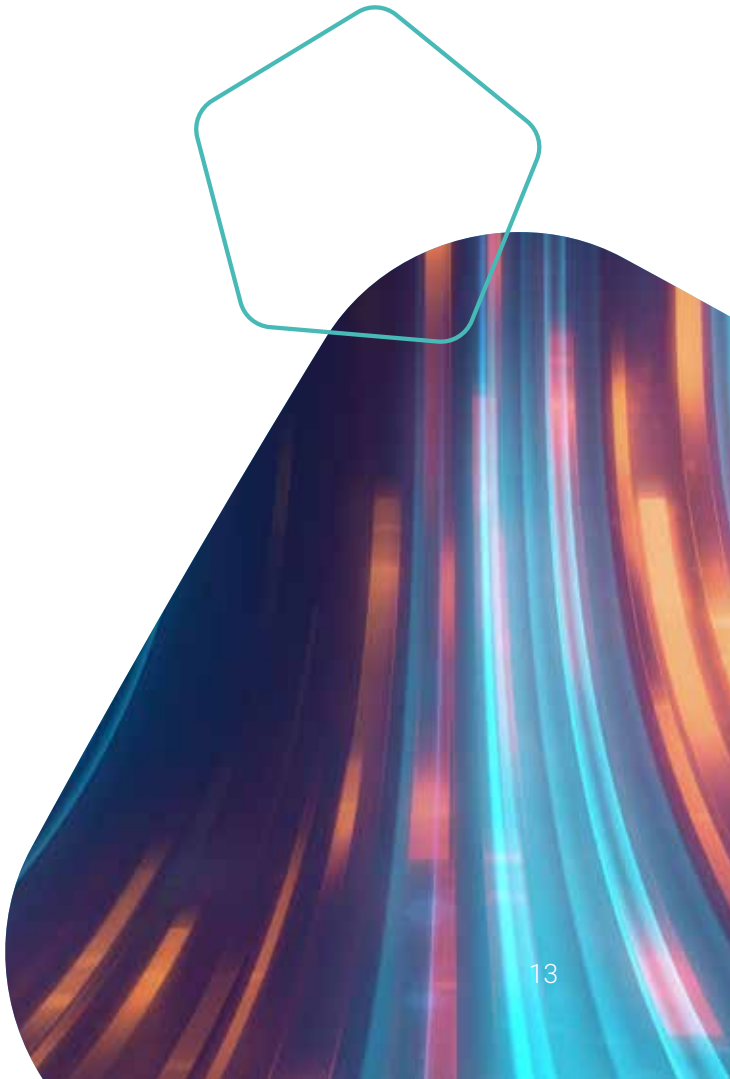
Every cloud does indeed have a silver lining, and for financial service providers who can successfully navigate this digital transition, there are many.

Firstly, CSPs are constantly innovating, evolving, and maintaining their services which takes the burden away from the banks of investing in massive IT estates. This allows cloud users to implement the best practices of modern policies, architecture, and operational processes built to the requirements of the most security-sensitive customers. Banks can then focus on what they do best: building and providing services for customers.

Also, cloud offers a scalable solution. This is particularly useful in instances when regulations make actual demand difficult to predict. For example, when Open Banking came into effect in 2018, it required banks to release their data in a secure, standardised form which could be shared more easily with other banking applications. There was no way to predict whether banks would need to share that data with 10 or 30,000 others, or whether their entire customer base would engage versus a handful of users. But banks partnering with CSPs could lean on their flexible computing capacity to scale and meet those demands.

Finally, and perhaps most importantly, cloud infrastructure is a key enabler for DevOps. It accelerates IT transformation, and with advanced tools and automation, banks can double down on their work to streamline and embed greater efficiencies that are truly transformative. Unless banks can shift technology estates to these new security paradigms, they will be left behind by the rapid pace of more agile start-ups and challenger banks.

With cloud being the destination for the majority of organisations, many of the existing challenges about security and talent will continue to be addressed by the CSPs. Think of it as a ‘safety in numbers’ approach. But banks must still invest in their own internal resources and/or find partners outside the CSPs to minimise their risks and maximise the returns on investment of a cloud approach.



REPLY AIRWALK

Beyond regulation: The growing need for the financial services sector to embed operational resilience

Earlier this year, the Financial Conduct Authority (FCA) began enforcing new rules and guidance relating to operational resilience for firms, financial market infrastructures and the overall financial sector. The FCA defines operational resilience as the ability to respond to, recover, and learn from operational disruption, and it's easy to understand why this is a priority. In today's hyper-dynamic and ultra-connected environment, operational disruption in one organisation can have wide-ranging implications for the wider economy.

It's fair to say that the financial crash of 2008 highlighted the contagion risk that the financial services sector has overall. The key development since that time has been the increased importance of technology in transaction channels. As a result, the impact of technological failures and risks have increased significantly.

Becoming resilient clearly has strategic importance, yet too many financial service providers still view operational resilience as a box-ticking exercise to meet the requirements of regulations like the Bank of England Supervisory Statement on Operational Resilience, and HM Treasury's Regulation on Third Parties. Currently, it is very much the external pressure of regulators, and firms' willingness to satisfy them, that is driving the industry's pursuit of operational resilience.

It is the purview of risk teams to manage and make it go away. But this view is myopic - operational resilience can be a significant strategic advantage for organisations and frankly, it is the right thing to do, not just because a regulator is saying it's sensible and enforcing it.

REPLY AIRWALK

The reasoning for resilience

Ensuring the UK financial sector is operationally resilient is essential for consumers, firms, and financial markets. Operational disruptions and the unavailability of critical business services have the potential to cause wide-reaching harm to consumers and risk to market integrity, threatening the viability of firms and causing instability in the wider financial system.

Every organisation will, at some point, experience problems. Whether it is cyber-crime or tech issues, operational failure is inevitable.

As organisations scale, innovate, evolve, and increase the number of people relying on their services, the greater the likelihood is that something goes wrong. The goal behind operational resilience is to identify these issues before they happen and embed contingencies to mitigate the impacts or allow the organisation to quickly recover.

Why is it broken?

The concern from the regulator has evolved somewhat, from financial resilience to operational resilience. The response to the former, Basel II regulation, for example, has taken over a decade to fully bed into ways of working, and the same will be true for operational resilience. Clearly then, external pressure takes a long time to change the industry. The lack of internal buy-in for operational resilience is where the real problem lies. While they will make the necessary changes to satisfy regulators, financial service providers currently underappreciate the true business value and competitive advantage of being a resilient, responsive organisation.

REPLY AIRWALK

Moving the needle

No one knows when operational resilience will be needed most – but with an exponential increase in the connections and complexity of digital services, introducing innovation will only get harder the longer businesses wait.

Organisations must buy-in to the strategic importance of operational resilience – in the same way that building digital services quickly is vital. Beyond regulation, it is valuable to know what the key systems are, where data is stored, how secure it is, how to stop systems from breaking and how, if they do break, they can be fixed almost immediately.

Risk teams are traditionally focused on just that, risk, so they may look at technology apprehensively but, in most cases, it is the solution to the problem. The cloud enables a real-time, automated, highly visible and integrated approach to managing operational resilience. Organisations must deliver this in a way that significantly reduces risk and enables much easier action to be taken when things do, inevitably, go wrong.

We are seeing some organisations evolve, particularly with the management of their cloud estates, building automated control frameworks and platforms that provide unprecedented levels of visibility, control and security intervention, but there's much more that can be done. The challenge is changing the mindset and embracing the strategic opportunity. If your systems fail and you have no way to recover them – and recover them quickly – you are not a resilient organisation, and the impact of that can be catastrophic. Promoting internal buy-in from firms for operational resilience, and supporting this with a dedicated investment into the correct technology and systems can kick-start a push for operational resilience in the financial services industry.

The cloud enables a real-time, automated, highly visible and integrated approach to managing operational resilience

REPLY AIRWALK

Why Airwalk Reply?

We deliver end-to-end transformation, from strategy and ideation through to execution and optimisation

We deliver transformational change in complex, regulated organisations. We bring experienced, multi-disciplined teams, with expertise across technology strategy, architecture, service design, engineering, security, and programme execution.

Our focus is at the confluence of business and technology

We know that business outcomes are all that really matter. In today's world, technology is perhaps the most crucial and strategic enabler for our clients to compete, differentiate and evolve.

In everything we do, we are focused on delivering tangible benefits – not technology for technology's sake, but strategic outcomes for our clients.

- New digital platforms, products and services
- Technology modernisation
- Ecosystem development
- Modern ways of working
- Cost optimisation
- Operational excellence

We combine delivery capability with technical expertise

We recognise that while never easy, technology is rarely the greatest source of complexity in major change or transformation programmes.

We deliver in environments where regulatory restrictions, risk, compliance, security concerns, resource limitations and evolving customer needs are just some of the elements that we need to manage as part of execution. In many cases we own transformation programmes and portfolios in their entirety, alongside technical execution.

We are uniquely placed to bring both deep technical expertise and heavyweight delivery capabilities to bear, owning full execution from end-to-end.

Our Services include

- Technology strategy
- Portfolio and programme delivery
- Technical execution

REPLY AIRWALK

Airwalk Reply
160 Victoria St
2nd floor Nova South
Westminster
London
SW1E 5LB

T: +44 (0) 20 8142 8686
E: info@airwalkconsulting.com

airwalkreply.com