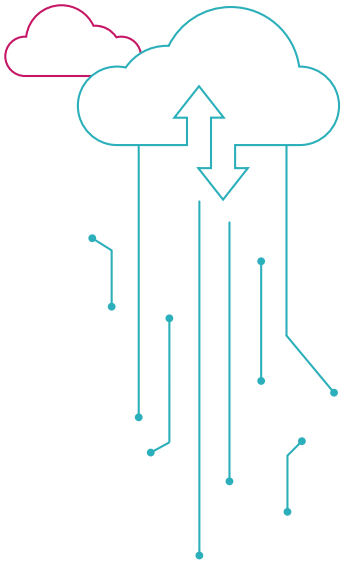
Scott Logic

Backup like a startup

Modern software engineering approaches that minimise downtime

Contents



Access more content

Throughout this document, we'll connect you to thought leadership material and other relevant content. To view this document online and access the additional content, follow this link or scan the QR code:

go.scottlogic.com/operational-resilience

Keeping the lights on is easier than you think

Strengthening operational resilience is a complex challenge for banks, particularly banks with large legacy IT estates. However, at the heart of operational resilience is business continuity, and there's a modern approach to this that any bank can adopt.

We are in a new era of operational resilience. Banks and other financial institutions operating in the UK must now comply with the UK Operational Resilience framework, and institutions that also provide services in the European Union must comply with the Digital Operational Resilience Act (DORA).

Both regulatory frameworks place an obligation on banks to understand dependencies across their IT estates and supplier networks, and to have robust backup plans in place to ensure business continuity in the event of outages. However, neither framework makes any recommendations of strategies banks should follow to strengthen their resilience. For long-established banks with large and complex legacy IT infrastructures, the challenge can appear daunting.

The standard approach followed by many banks is to replicate key systems as standby systems hosted on different premises from their primary IT infrastructure. In the event of an outage, these 'cold' or 'warm' backup systems are manually operationalised, which can take hours or even days. Tested less frequently than the bank's primary IT infrastructure, these systems are more likely to be error-prone, resulting in a heightened risk of data loss. If a bank's clients are significantly impacted as a result of outages, serious fines and reputational damage can follow. But what's the alternative?

Backup live, like a startup

A solid alternative is to take a leaf out of a challenger bank's book in achieving business continuity.

It's certainly easier for such banks to implement modern approaches to operational resilience thanks to their loosely coupled architectures and freedom from legacy IT; however, those same approaches aren't out of reach for more long-established banks. Core to such approaches are modern technologies for storage, messaging, deployment and networking.

The more you can adopt automatic switchover to backup systems, rather than manual, the more resilient your banking operations will be. Later on, we'll share some expert insights into how you can automate key aspects of operational resilience. First, we'll use Monzo Stand-in to illustrate a highly successful approach to business continuity and explain why it's adaptable to any bank, including yours.

Monzo Stand-in involves running a live alternate system on a different cloud provider, continuously handling a portion of live customer traffic. This approach provides real-time monitoring and ensures seamless failover in case the primary provider has an outage or experiences significant service degradation. This removes the need for complex business continuity processes, because the backup systems are being tested continuously as a first-class citizen in the production environment.

Monzo Stand-in, a smarter approach to DORA and Operational Resilience

Read the blog post

Any bank can follow the core principles of this approach. Here's how:

Identify critical functions

Monzo Stand-in doesn't attempt to replicate the bank's full suite of services. It offers only the core functionality used daily by the majority of customers. This reduces the cost of keeping a live alternate system running continuously, with fewer systems to operate, test and maintain.

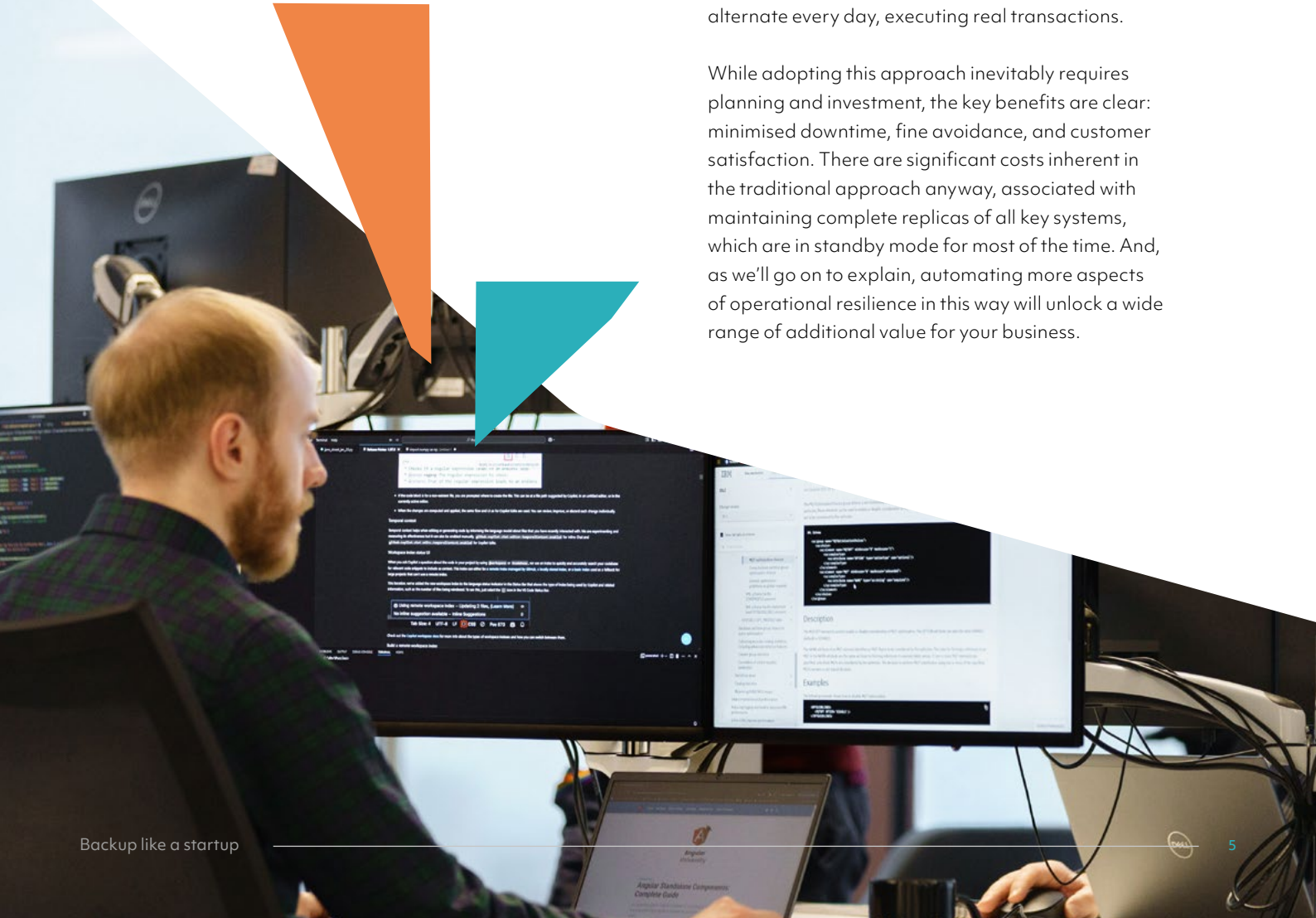
Any bank can identify the most critical business functions and workflows. Once identified, modular backup systems can be designed and built to support these core functions, running continuously as a live alternative. These primary and alternate systems can be hosted on separate clouds, or on a mix of cloud and on-premises. In the event of an outage, workflows can be rerouted automatically to execute a seamless failover, removing the need for engineers to boot up dormant backup systems manually.

Test continuously

In the Monzo approach, a small, random selection of customers is flowed through the live alternate system each day, allowing the bank to test whether the core tasks can be completed successfully, with any issues being flagged for resolution. In addition, Monzo tests accuracy by sending the same customer transaction data through both flows at the same time – as real customer transaction data and matching test data – and checks whether the results are the same.

Again, this is achievable by any bank, regardless of the scale of its legacy infrastructure. With critical functions identified, a subset of clients can be redirected through the live alternate system without any impact on user experience. This continuous testing provides ongoing confidence that the backup system is functioning optimally and capable of fulfilling core functions. The standard approach of performing manual Business Continuity Tests on backup systems at the weekend will never give the same level of confidence as testing a live alternate every day, executing real transactions.

While adopting this approach inevitably requires planning and investment, the key benefits are clear: minimised downtime, fine avoidance, and customer satisfaction. There are significant costs inherent in the traditional approach anyway, associated with maintaining complete replicas of all key systems, which are in standby mode for most of the time. And, as we'll go on to explain, automating more aspects of operational resilience in this way will unlock a wide range of additional value for your business.



Gain visibility, maintain vigilance, deliver value

In the next section, we'll provide further expert insights on how automating processes strengthens operational resilience, reduces risks, and improves reliability. These insights are grouped as follows:

Visibility

The importance of gaining and maintaining comprehensive visibility of your entire IT estate and understanding all its key dependencies.

Vigilance

The importance of continuous, proactive vigilance to identify potential causes of impactful events and correct them before you feel the pain.

Value

The additional value that you can derive from the above, beyond regulatory compliance and operational resilience.

Not all of the insights we share may be relevant to your bank, and you may be further advanced in some respects than your competitors.

Whatever stage you are at, Scott Logic can bring rich experience and expertise to bear to support you in strengthening your operational resilience.

Visibility

You can't fix issues if you can't see them. Operational resilience is contingent on gaining a holistic view of your IT infrastructure and an understanding of its dependencies. In this section, we explore some ways for you to achieve this visibility.

Identifying gaps in compliance

The Bank of England's Operational Resilience regulations and DORA have both now come into force. When the complexity of each framework is taken into account, they present a significant challenge for banks to manage.

What you need is visibility of relative maturity levels across the different pillars of each framework, supported by actionable recommendations for improvements.

Scott Logic can help, bringing to bear our expertise and experience from different banking clients, and leveraging our partnerships with hyperscalers like AWS and Microsoft Azure. With actions identified and prioritised, we can help you address them at pace, delivering enhanced compliance and strengthened resilience.

aws PARTNER Advanced Tier Services

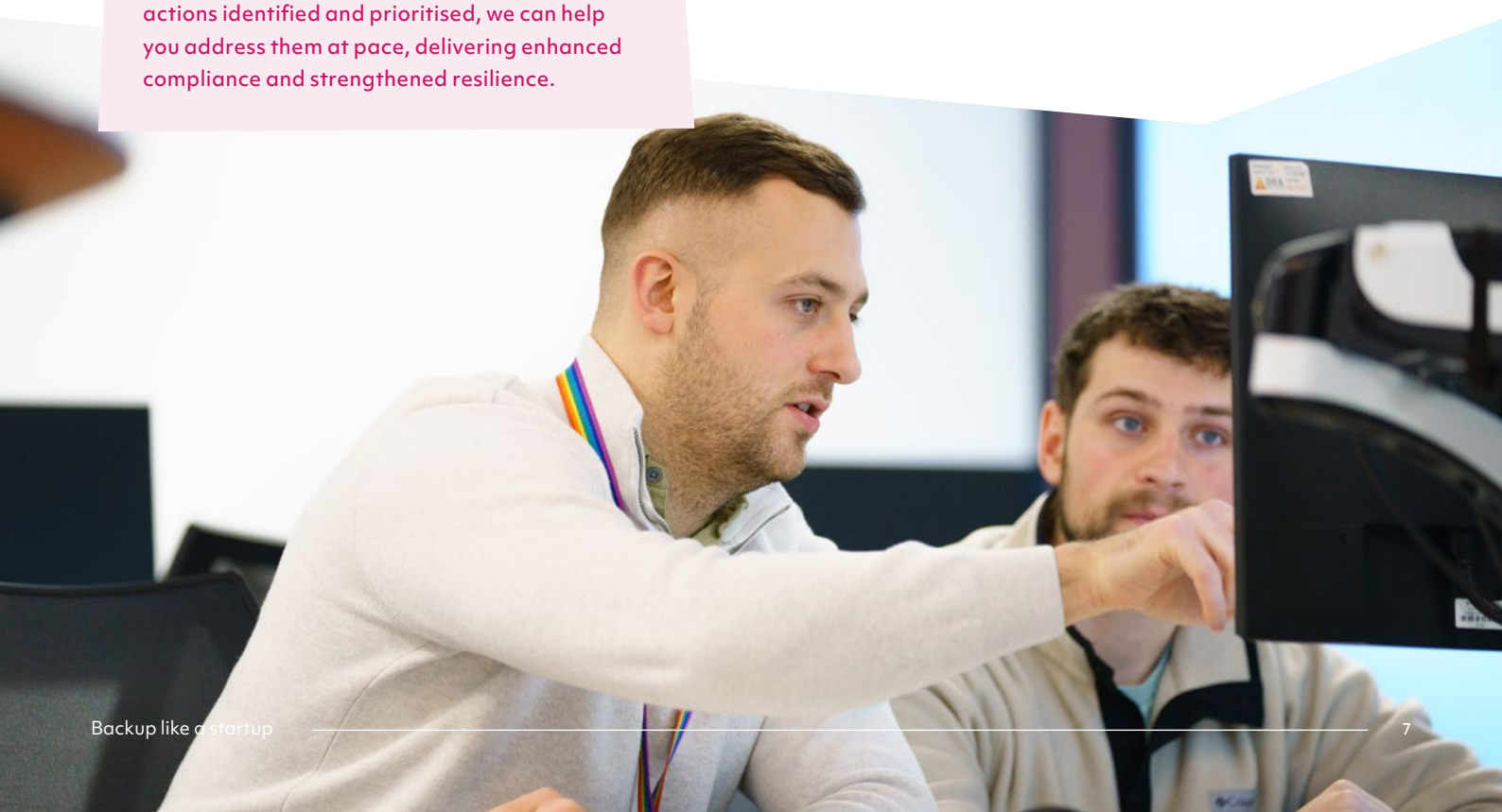
AWS DORA Compliance Recommendation Tool (D-CAT)

Launched in partnership with Scott Logic, AWS's DORA Compliance Recommendation Tool is a self-assessment framework that helps you identify gaps in compliance and provides directional guidance on how to tackle them.

D-CAT uses a five-level maturity scale from Level 1 (Base) to Level 5 (Expert) to rate your current compliance posture. The recommendations it provides are tailored to different maturity levels, enabling you to progress systematically towards higher levels of compliance.

With a pragmatic appreciation of the scale and complexity of the compliance challenge, D-CAT's recommendations present cost indicators, difficulty levels, and priority levels to help guide your implementation efforts.

Find out more



Surfacing and tracing risks

Modern software architectures are a complex web of dependencies, increasing every organisation's exposure to risk. That's why both DORA and UK Operational Resilience regulations require financial entities to track and manage third-party software, including open source libraries.

Software Bills of Materials (SBOMs) are crucial for compliance, providing a nested inventory of all the components, libraries and other dependencies that make up a software application. Given the likely scale and complexity of your IT estate, automating the generation of your SBOMs will save a huge amount of money and time. It will also ensure accuracy, drive efficiency and underpin compliance.

This is no small undertaking, but Scott Logic can provide you with the expertise, experience and additional resources you need.

Client Story

Scottish Government Payments Service

What they aimed to do
Launch a payments platform for Scottish citizens that was Secure by Design and highly resilient.

How we helped
We used GitLab to generate SBOMs to the CycloneDX standard and integrate them into the Continuous Integration/Continuous Deployment pipeline. With each deployment, GitLab generated a versioned SBOM and scanned it against vulnerability databases (such as those provided by **CVE** and **VulnDB**), while also checking the licences of dependencies in the supply chain.

Business outcomes
The ScotPayments service has processed tens of millions of pounds in transactions with no security incidents to date.

Read the blog post

Open Source Sustainability through Corporate Social Responsibility?

Watch the video

Gaining comprehensive observability

Conventional monitoring approaches are not equal to the challenge presented by complex distributed software architectures, which introduce a significant overhead while increasing risk exposure. Metrics are limited in scope, coverage, and read-across, making it extremely difficult to gain any kind of holistic view of system health and performance.

Modern observability approaches enable the collection of richer and more extensive data across distributed architectures, providing detailed insights into system behaviour and enabling faster problem resolution.

Scott Logic's experts can implement observability tooling at your bank, including instrumentation to automate the scraping of metrics and enrichment of data, providing you with a comprehensive overview and real-time insights.

Is observability just the new name for system monitoring?

Listen to the podcast

Vigilance

Operational resilience is a continuous process rather than a state to be achieved. It depends on proactive efforts to surface and mitigate risks, and to imbue resilience into your Software Development Lifecycle (SDLC) by automating processes and cultivating modern engineering practices.

Baking in resilience

Traditional approaches to operational resilience are not merely outmoded and suboptimal, they represent a threat vector for organisations. Periodic testing exercises, disaster recovery drills, and manual backup and restore processes are costly and inefficient approaches that leave banks exposed.

Security and resilience should be integrated throughout the SDLC. The discipline of Site Reliability Engineering promotes the reduction of manual intervention in managing systems by automating as much as possible. It factors in reliability, resilience and security at every stage, from planning and design, through development and testing, to deployment and operation.

Scott Logic's engineers are experts in helping clients automate in this way, and they can coach your teams in software engineering and DevOps practices that weave site reliability throughout the SDLC.

DevSecOps, a portmanteau too far?

Listen to the podcast

Strengthening resilience through experimentation

Planned manual resilience testing of isolated systems can only provide incomplete insights and is unlikely to surface issues that could not have been predicted in advance. Modern distributed architectures have complex integrations and multiple dependencies, and when real-world events such as large-scale outages are taken into account, it is extremely difficult to predict where errors will arise.

Experimentation can play an important role in tackling this. For example, Netflix's Chaos Monkey software automates the random termination of instances in production, helping to surface all the knock-on consequences of the failure. The objective is to instil in engineers the expectation that instances will fail so that they design systems to work in the event of such an outage.

Resilient Systems and Experimentation

Watch the video

Our AWS- and Azure-certified experts can support your teams to automate these kinds of experiments and upskill them in how to build systems for greater resilience.

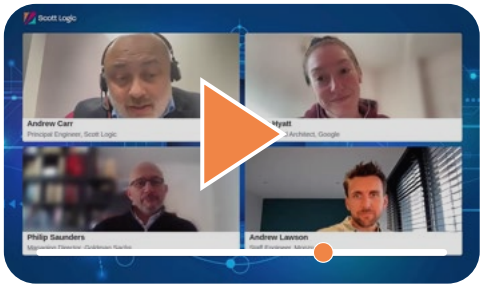
Adopting the cloud incrementally

Fundamentally, on-premises systems impede modern operational resilience. The tight coupling of legacy systems means that they often have unintended single points of failure. This is exacerbated by the complex dependencies between systems and components, which are often not fully understood. The result is that an issue with a given component can lead to far more error scenarios than expected.

Incremental cloud adoption is the answer, as it allows you to create loosely coupled architectures and automate security and resilience at every stage of the SDLC. Failures can be isolated more easily so that they don't impact other components, and automated failovers allow business continuity in the event of an outage.

Operational Resiliency in Financial Services

Watch the video



Our expert architects have extensive experience with Financial Services IT infrastructures, and we can leverage our hyperscaler partnerships to shape with you a prioritised, long-term roadmap for your cloud migration.

Value

Complying with any given regulation has some intrinsic business value. However, complying with DORA and UK Operational Resilience has the potential to create much wider value for your bank due to the way they promote best practices in cloud engineering.

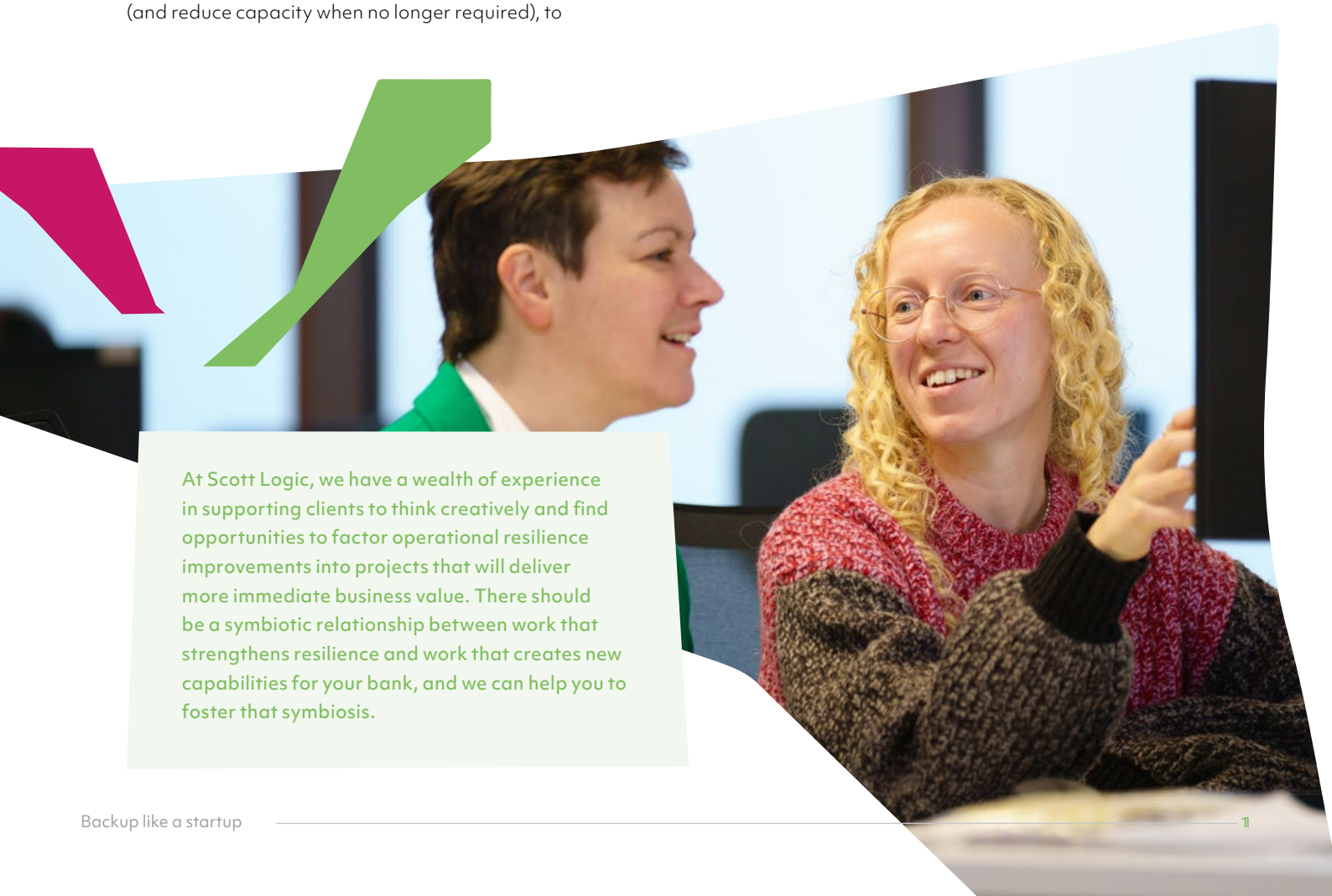
As a result, the improvements we've recommended above will not only promote operational resilience but also increase your speed to market, enhance your agility, and give you a competitive advantage.

Cloud platforms provide an unprecedented level of technical agility. In the early stages of product development, the ease of provisioning facilitates experimentation with, and evaluation of, different technology solutions. Within the construction phase, the team can rapidly provision environments and adapt to feedback with speed and confidence, backed by high levels of automation.

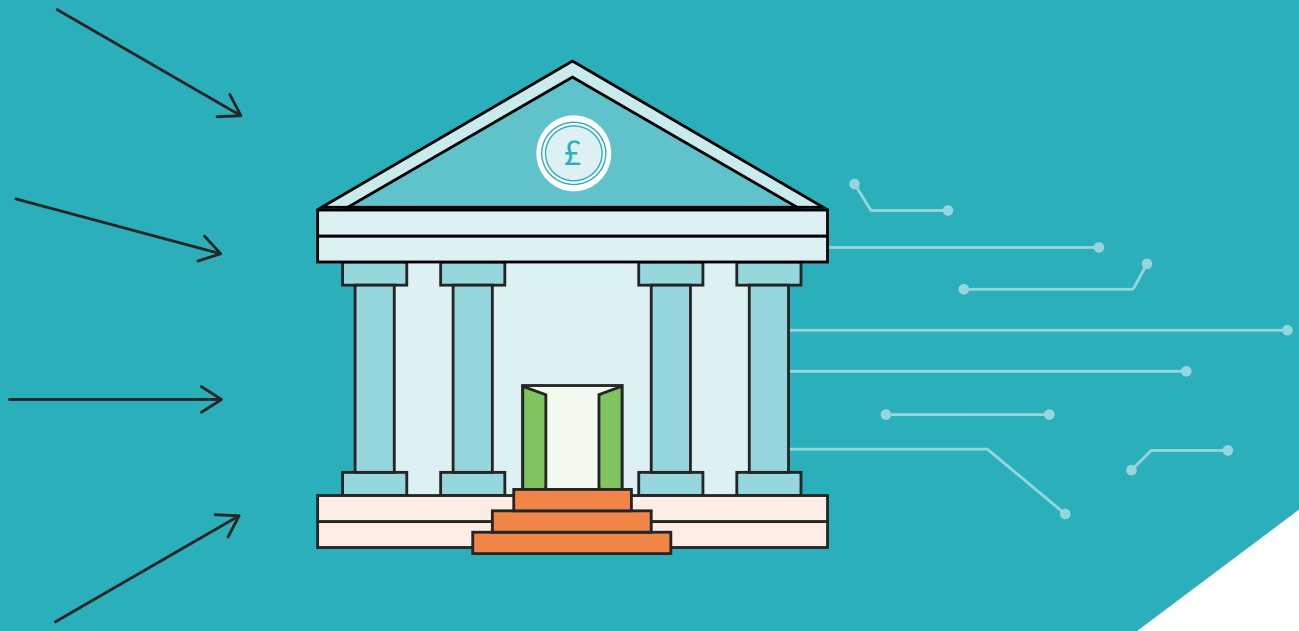
When moving to production, the cost-effective scalability of the cloud allows you to easily create systems that provision extra capacity in real-time (and reduce capacity when no longer required), to create truly elastic solutions. Finally, production issues can be resolved rapidly and deployed with complete confidence, thanks to infrastructure as code and the levels of automation it offers.

As a result, technology teams can spend less time solving technology problems and more time on the problems that really matter – the business problems. That's the most important property of the cloud, its ability to provide a platform for change and a foundation for business agility. The cloud is a platform that supports rapid and confident change, and this ultimately leads to a faster time-to-market and a much more agile business.

All that being said, it can still be a challenge to make a successful business case for investment in projects where regulatory compliance is the goal.



At Scott Logic, we have a wealth of experience in supporting clients to think creatively and find opportunities to factor operational resilience improvements into projects that will deliver more immediate business value. There should be a symbiotic relationship between work that strengthens resilience and work that creates new capabilities for your bank, and we can help you to foster that symbiosis.



Ready to enhance your bank's resilience?

For two decades, we've helped financial services institutions take a pragmatic approach to achieving their business goals. With our support, you can strengthen your operational resilience, comply with regulations, and gain the business agility you need to outstrip your competitors.

If you'd like to discuss your operational resilience journey and where our support could help, we're always happy to chat.

Contact Andrew Carr, Financial Services Director:

+44 333 101 0020

andrew@scottlogic.com

Scott Logic

6th Floor, The Lumen
St James Boulevard
Newcastle Helix
Newcastle upon Tyne
NE4 5BZ

+44 333 101 0020

scottlogic.com