The reality of operational resilience in financial services: consistency vs flexibility*

Understanding and charting your operation resilience position in a digital first world and in highly regulated industry

Monica Sasso
Global Financial Services
msasso@redhat.com

Sam Marland
Financial Services SA Lead
smarland@redhat.com

Source: ChatGPT
***Consistency vs Flexibility:** consistency involves stability and adherence to established principles, while flexibility involves adaptability and openness to change. Both have their merits, and the appropriate balance depends on the context and the goals you're trying to achieve. Finding the right balance between consistency and flexibility is often crucial. Overemphasis on one at the expense of the other can lead to problems. Too much consistency can result in resistance to change, while excessive flexibility can lead to instability and lack of direction.

Red Hat

Agenda

- What is operational resilience - in financial services
- Foundational elements of technology and cloud resilience
- Building your technology resilience story
- Op res and the financial services ecosystem

Operational resilience in financial services

Red Hat

Cloud usage is being reshaped by regulatory requirements

2018

Data Privacy (GDPR)

2024/2025

DORA, Operational Resilience, NIS 2, etc

TBD

Directive on Critical Infrastructure Resilience (CIR)

TBD

Cloud Sovereignty

https://www.whitecase.com/insight-our-thinking/financial-regulatory-observer-2022-operational-resilience-uk-eu-and-us

Red Hat

Topics from the operational resilience rules

From a tech provider's view point

- Identity & Access Management process, controls & testing
- Incident Management process, controls & testing
- Operations Management process, controls & testing
- Protecting confidentiality and data
- Data privacy rules (e.g. a client's right to access their data, GDPR, etc)
- Breach Management & Reporting
- Security and Regulatory Compliance process & controls esp. for shared responsibility such as network security and vulnerability management
- Due Diligence (that Red Hat acts how a regulated entity would w.r.t its operations
- Auditing of Red Hat's partners (i.e. our 3rd and 4th party providers)
- Business Continuity process, controls & testing
- Disaster Recovery process, controls & testing
- (3rd Party) Risk Management process, controls & testing
- Access to everything above *promptly*
- **Exit Strategy (e.g. no vendor lock-in)**
- Stronger contracts to ensure continuity of service (regardless of commerciality) & incl failure to comply
- How Red Hat builds non-functional requirements into its products & services such as security & regulatory features
- Change Management process, controls & testing

Red Hat

UK Op Res rules[1]* & DORA[2]

Pillars of the UK and EU regimes

Op Res in Financial Services

UK op res framework

- Firms must identify their **'important business services'** that could impact clients or the financial system if disrupte
- Define an **'impact tolerance'**
- Ensure delivery of those services within their impact tolerances during severe scenarios
- Takes an outcome-based approach
- Firms must manage risks to their own op res - so their 3rd parties' risk as well

However, firms cannot manage systemic risks that may arise because multiple firms have independently decided to rely on a common third party for certain services.

DORA

1. (ICT) Risk Management
2. (ICT) Incident Management (cyber security)
3. Intelligence Sharing
4. Digital Operational Resilience Testing
5. ICT third-party risk management, which includes having **exit strategies**

The powers relating to third parties will be set out in DORA's oversight framework of pan-European critical ICT service providers (CTPPs), which aims to ensure operational risks are no longer addressed exclusively through outsourcing arrangements put in place by financial institutions, ***but also directly at the CTPP level***[3]*.*

1. https://www.fca.org.uk/firms/operational-resilience, https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector#chapter-2-2
2. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1
3. https://www.whitecase.com/insight-our-thinking/financial-regulatory-observer-2022-operational-resilience-uk-eu-and-us

But really, managing critical 3rd party ICT providers is all about . . .

Bank of England plans tough new rules on IT resilience, avoiding cloud "concentration risk"

Is 'big cloud' too big to fail? What cloud concentration risk means for the future of banking

Niamh Curran
Reporter, Finextra

What is cloud concentration risk?

Cloud concentration risk can be defined as when a bank's overreliance on one cloud service provider presents operational risks and creates financial stability risks on a regional or global scale. Concentration risk also emerges if a number of banks have key operational or market infrastructure capabilities running on one cloud service provider.

As it stands, the cloud services network is concentrated with Amazon Web Services, Google Cloud and Microsoft Azure leading the pack. It could be argued that cloud services is a difficult game to get into. Comparably smaller providers and even those with solid and robust offerings, like IBM and Oracle, are picking up steam but struggle to compete on an equal level.

With a renewed interest in operational resilience because of the COVID-19 pandemic, global regulators are ramping up their evaluation of the shared responsibility model and considering whether the bank or the cloud service provider is responsible for events that put financial stability at risk.

Several vectors of cloud concentration risk that presented the most significant challenges:

- **Over-reliance**: An over-reliance on one cloud service provider (CSP) to support key banking or important business services
- **Resiliency**: A dependence on a single-cloud and single region / zone
- **Visibility:** A lack of concentration risk visibility across third- and fourth-parties upon which many financial institutions depend

1. https://thestack.technology/bank-of-england-cloud-concerns-concentration-risk/
2. www.ibm.com
3. https://www.finextra.com/the-long-read/331/is-big-cloud-too-big-to-fail-what-cloud-concentration-risk-means-for-the-future-of-banking

Red Hat

Foundational elements of technology and cloud resilience

Foundational elements of modern technology resilience

Drive Consistency

[Five foundational elements supporting Op Res]

1. Define infrastructure as code and automate everything
2. Understand your end-to-end software supply chain
3. Build security and compliance into your development process
4. Evolving working practices
5. Culture

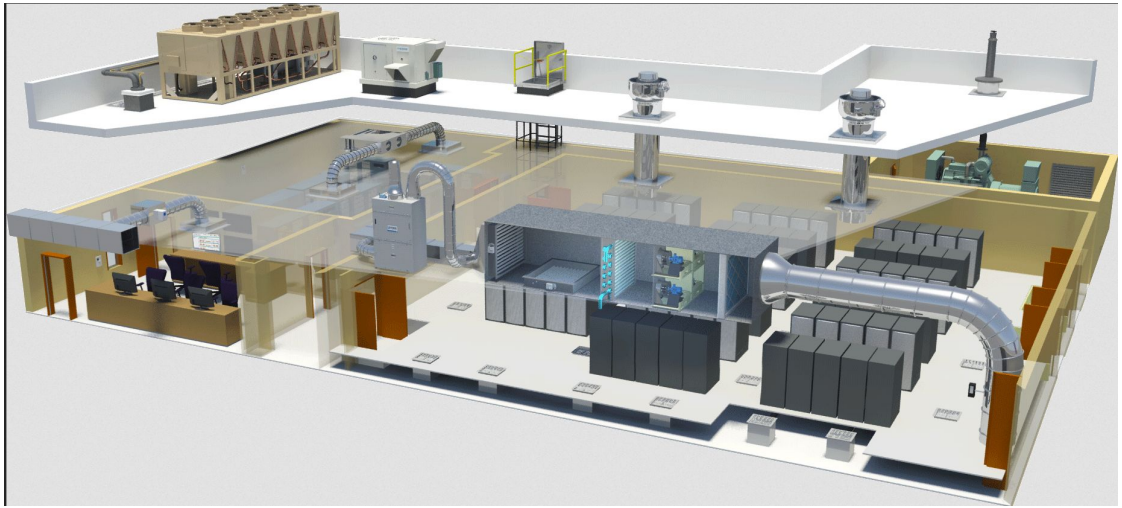
Red Hat

Building your technology resilience story

Red Hat

Assessing risk ‘the old way’

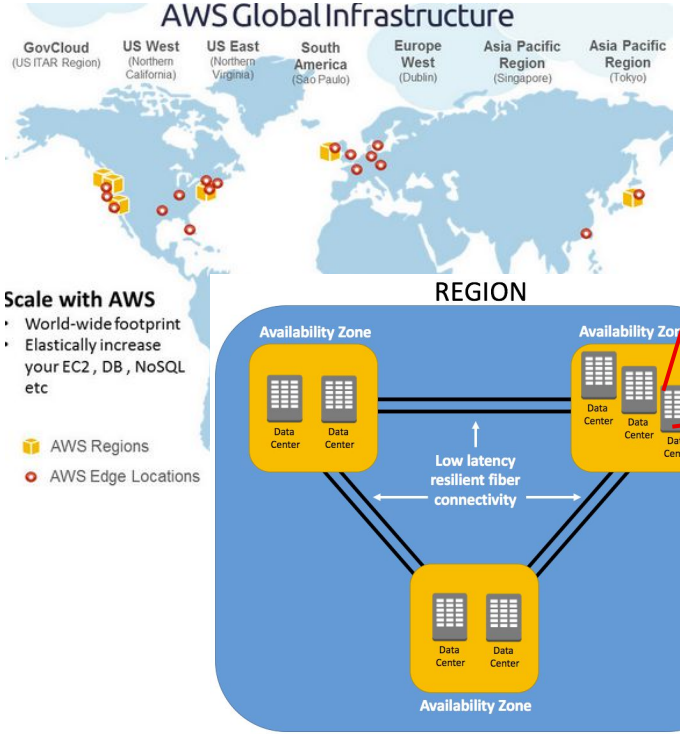
Before software was everything and everywhere

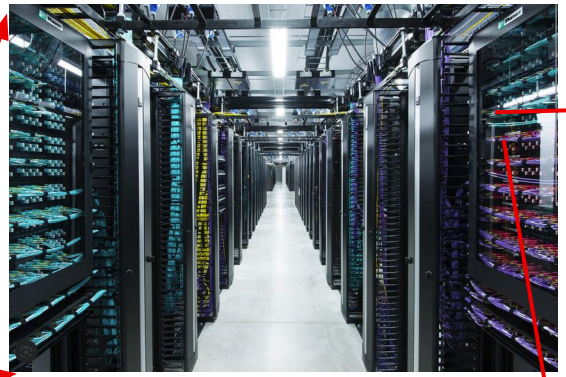


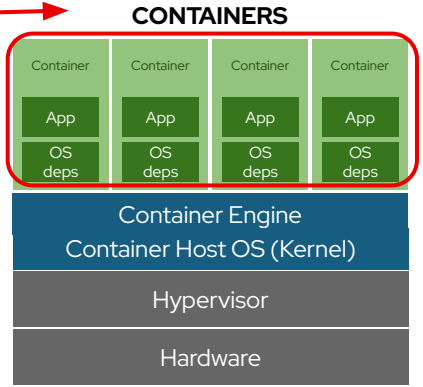
- Computing and processing infrastructure
- Storage and data management
- Network Infrastructure
- Support infrastructure

Assessing risk for in a cloud native, modern* world

It is more than outsourcing your data centre







Source: ChatGPT

***Modern technology practices** refer to contemporary approaches and methodologies that are widely adopted in the technology industry to improve software development, deployment and operations. These practices focus on increasing agility, collaboration, efficiency, and quality in software development and IT operations. Here are some key modern technology practices: Agile Development, DevOps, CI/CD, Test-Driven Development (TDD), Cloud Computing, Microservices Architecture, Automation and Infrastructure as Code, Data-Driven Decision Making

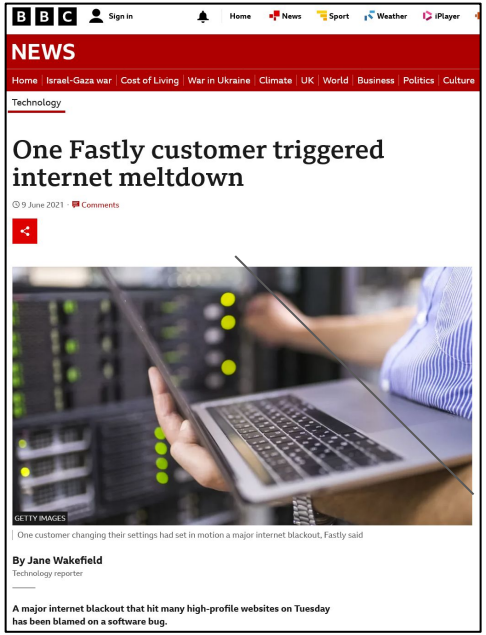
Red Hat

New risk areas to assess your own posture

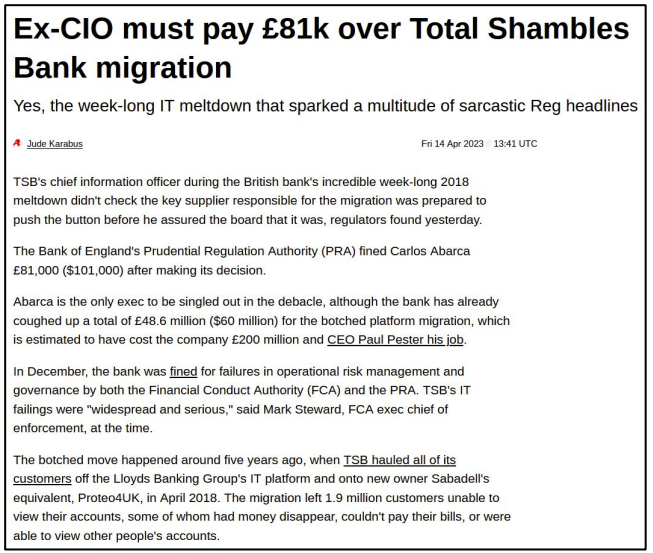
Examples of the changing(ed) risk landscape

Managing your Trusted software supply chain

Managing 4th & 5th parties risk



Managing delivery risk



Ex-CIO must pay £81k over Total Shambles Bank migration

Yes, the week-long IT meltdown that sparked a multitude of sarcastic Reg headlines

Jude Karabus — Fri 14 Apr 2023 13:41 UTC

TSB's chief information officer during the British bank's incredible week-long 2018 meltdown didn't check the key supplier responsible for the migration was prepared to push the button before he assured the board that it was, regulators found yesterday.

The Bank of England's Prudential Regulation Authority (PRA) fined Carlos Abarca £81,000 ($101,000) after making its decision.

Abarca is the only exec to be singled out in the debacle, although the bank has already coughed up a total of £48.6 million ($60 million) for the botched platform migration, which is estimated to have cost the company £200 million and CEO Paul Pester his job.

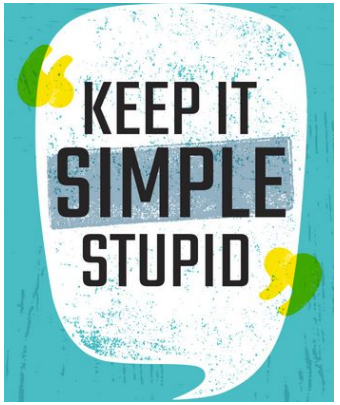
In December, the bank was fined for failures in operational risk management and governance by both the Financial Conduct Authority (FCA) and the PRA. TSB's IT failings were "widespread and serious," said Mark Steward, FCA exec chief of enforcement, at the time.

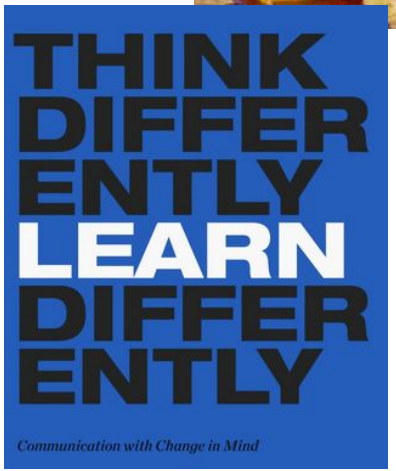
The botched move happened around five years ago, when TSB hauled all of its customers off the Lloyds Banking Group's IT platform and onto new owner Sabadell's equivalent, Proteo4UK, in April 2018. The migration left 1.9 million customers unable to view their accounts, some of whom had money disappear, couldn't pay their bills, or were able to view other people's accounts.

- https://www.bbc.co.uk/news/technology-55442732
- https://www.bbc.co.uk/news/technology-57413224
- https://www.theregister.com/2023/04/14/ex_cio_tsb_fine/

Red Hat

Tips on assessing your own posture





Red Hat

Op res and the financial services ecosystem

Red Hat

What is Red Hat up to

Our homework

Engaged a 3rd party to understand our own compliance posture

Demos . . .

Building a validated pattern and demo to prove that application portability is possible in a hybrid environment that we see most common in our FS customers around the world (e.g. in support of their exit strategy, and to demonstrate the limits of resilience)

Use cases

Developing use cases and proof points like North-South encryption, confidential compute, helping cutomrs with exit strategies, even digital sovereignty

Partnerships

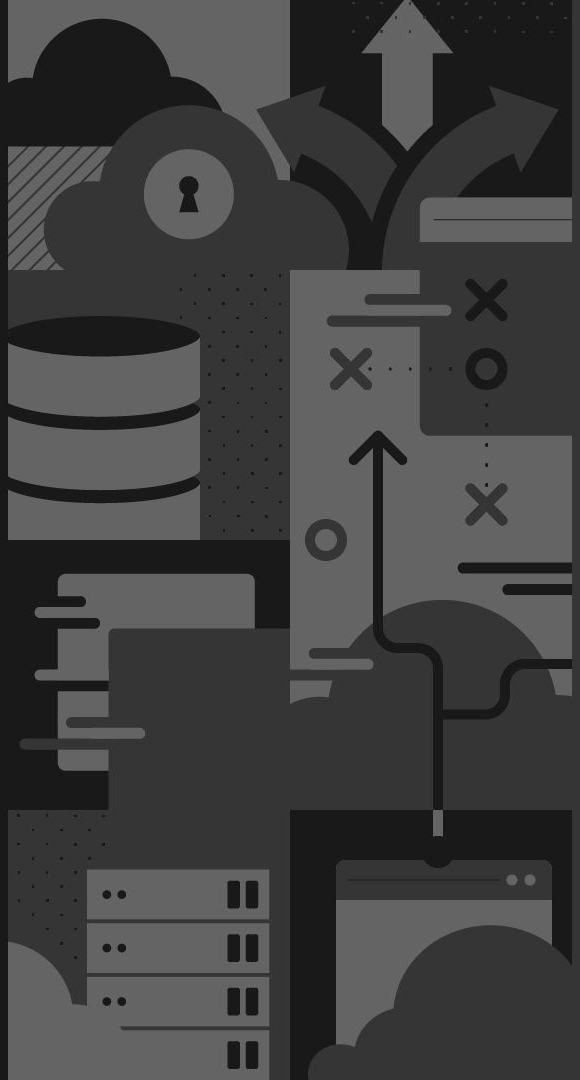
FINOS

A community minded approach to solving for it

Where we would like to work together

Join open source working groups to explore use case, prove application portability and jointly explire the limits of resilience

Red Hat



Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat