

Financial Regulators Worldwide are Getting the Legal Right to Regulate the Operational Resilience of Big Cloud Service Providers

SREcon22 Europe/Middle East/Africa
Andrew Ellam, Monzo Bank



Welcome - let's dive into the talk.

By the way, I'd like this to be a conversation, and I've allowed time at the end for that, so please do rack up some comments and questions in the Track 1 Slack channel, or raise your hand at the end.

Long title is long

Sorry

OK so my title is kind of long and not clever or witty.

Long title is long

Does give you a good overview of the topic though

But it does give you a good overview of what I'm going to talk about.



Let's get a proper overview.



- New legal powers are coming for financial regulators worldwide. New laws are being written and passed now.



- Financial regulators are being given powers to regulate the "critical" cloud service providers.



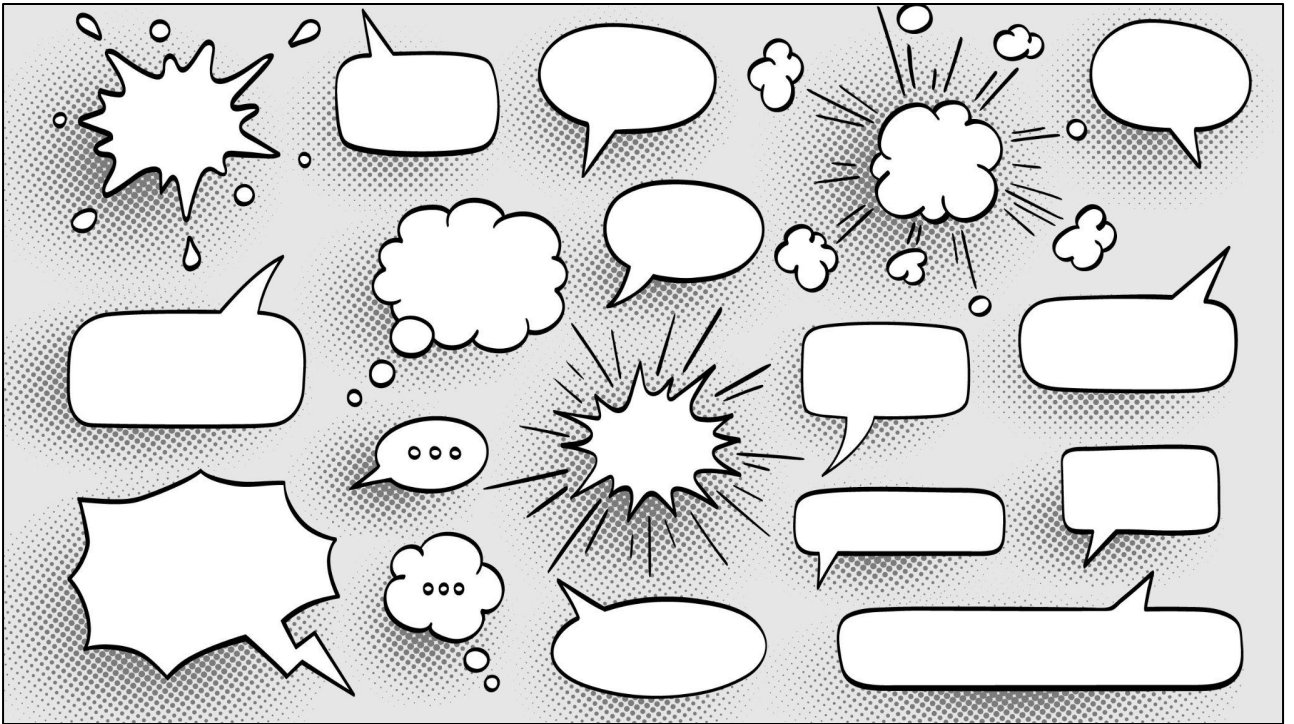
- The things on which they will enforce standards are absolutely central to the SRE discipline (e.g. availability/uptime).



- Cloud service providers could face large fines or being barred from the market, if they fail to meet required standards.



- We (the SRE discipline) will need to successfully collaborate with "risk and compliance" disciplines from the finance field.




- We need to represent to the regulators the SRE way of doing things and how effective it can be.


Agenda



 Me: The perspective from which I'm looking at this


 New laws

 Impact on cloud service providers

 So what?

 How can we contribute to the conversation?

Today I'm going to talk about:

 Myself: The perspective from which I'm looking at this

 New laws






 Impact on cloud service providers

 So what?

 How can we contribute to the conversation?

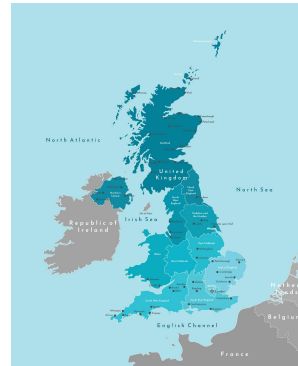
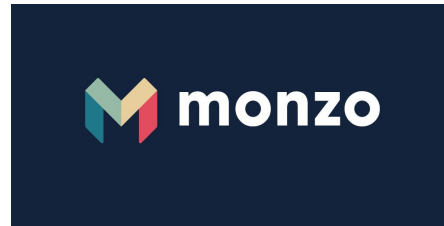
Agenda



-  Me: The perspective from which I'm looking at this
-  New laws
-  Impact on cloud service providers
-  So what?
-  How can we contribute to the conversation?

Let's start with me: a quick summary of the perspective that I'm bringing to this.

My perspective



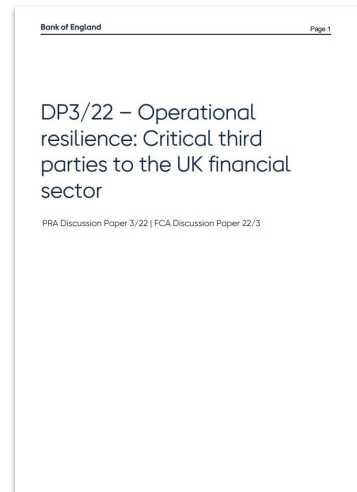
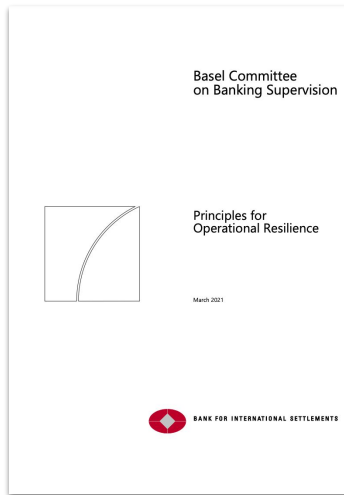
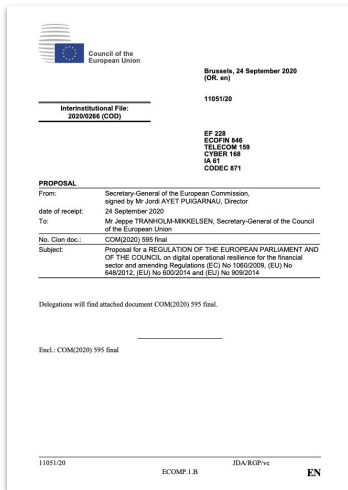
- Tech industry background (Startups / Amazon / Facebook / now Fintech).
- I'm in the UK and working for a UK-registered bank so what you're going to get from me is a UK perspective.

My perspective



- I'm new to Fintech - more accustomed to the tech world including SRE.

My perspective



- Discovering that the finance/banking world is suddenly alive to the importance of SRE concerns (although they don't call them that).

My perspective



- Importance of operational resilience is backed by regulators 'wielding big sticks' (fines, bans, etc).



- This is a new thing for the finance world. New rules/law are coming in now (some already live, some being passed by legislators now, others in the planning stages).




- Warning: a lot of what I'm talking about today hasn't been implemented yet. What you're getting is my best guess of how it might be implemented. It could play out differently from this.


Agenda



 Me: The perspective from which I'm looking at this

 **New laws**

 Impact on cloud service providers

 So what?

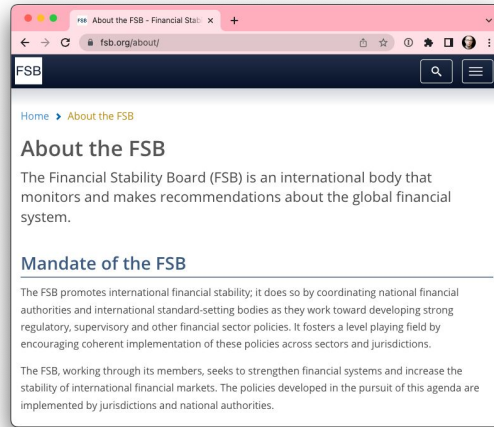
 How can we contribute to the conversation?

So let's get into detail about the new laws that are being passed.

New laws



- There is a global push for regulators to improve the “operational resilience” (meaning uptime/availability) of the financial sector’s consumer-facing software systems.



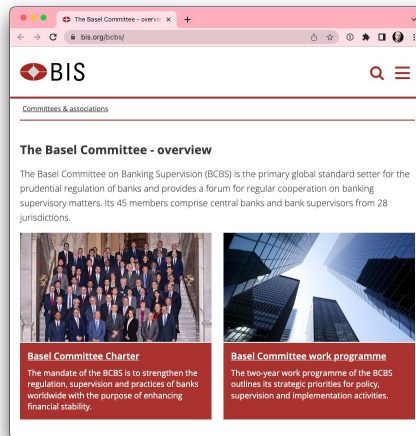
The FSB promotes **international financial stability**



Where is this push coming from?

- From global regulatory organisations such as the Financial Stability Board (FSB)...

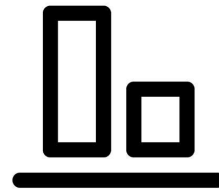
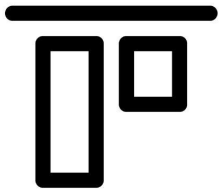
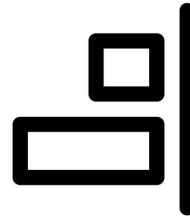
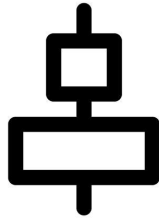
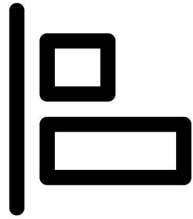
New Laws



“ primary global standard setter for the prudential regulation of banks ”

- ... and the Basel Committee on Banking Supervision.

New Laws



- Expect “global regulatory alignment” (all the large financial regulators to end up with similar laws and regulatory regimes on operational resilience).



Why introduce these new laws?

- To prevent instability in national and global financial markets which can be caused by IT failures in individual financial institutions or (worse case) in common systems used by many financial institutions.

Image: Police keep order during a run on the Adolf Mandel Bank on New York City's Lower East Side. February 16, 1912.

[Take a look at the trades and industries shown on the walls in the hall here - there's some people mining coal over there, people ploughing a field over there - none of them can effectively function without a working financial system]

New Laws



Is this a good thing? (Yes).

- Financial disasters are a very bad thing! Financial regulators are right to recognise that “availability is feature zero”.



- “Concentration risk” is real and growing. A large proportion of UK finance firms that are using cloud computing (and we’re all either on the cloud or planning to be on it) are using the three main cloud service providers (AWS/GCP/Azure). A serious problem with any one of these three could cause systemic impact on financial markets. Individual financial institutions are not in a position to deal with this systemic risk; it’s good that the regulators are doing so.

“

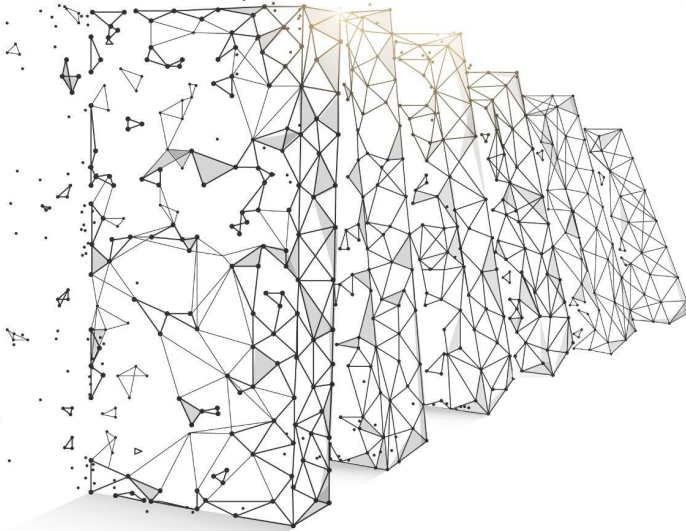
*the increasing reliance on a small number of CSPs [Cloud Service Providers] and other critical third parties for vital services could increase financial stability risks in the absence of greater **direct regulatory oversight of the resilience of the services they provide.***

”

Bank of England, Financial Policy Committee,
Financial Policy Summary and Record Q2 2021

This is how the Bank of England phrased it earlier this year.

New Laws



- Digression: worst case is a ‘domino effect’ in which failure of one cloud service provider causes capacity crunch in other cloud service providers which leads to instability across the industry (or just lack of capacity for disaster recovery).



- Legislative bodies are passing new laws imposing operational resilience obligations on systemically important vendors such as key cloud service providers.



What laws?

- EU: Digital Operational Resilience Act (DORA).
Provisional agreement was reached 11 May 2022.

Parliamentary Bills

House of Commons

UK Parliament > Business > Legislation > Parliamentary Bills > Financial Services and Markets Bill

Bill feed

Financial Services and Markets Bill

Government Bill

Originated in the House of Commons, Session 2022-23

Last updated: 8 September 2022 at 15:03

Commons Lords Final stages



[See full passage](#)

Details News Stages Publications

Long title

What laws?

- **UK: Financial Services and Markets Bill**

Background info:

- UK: Bank of England Supervisory Statements SS1/21 “Operational resilience: Impact tolerances for important business services” and SS2/21 “Outsourcing and third party risk management” established requirements for financial institutions which must be implemented by April 2025. HM Treasury June 2022 Policy Statement “Critical third parties to the finance sector“ proposes wide-ranging powers for financial regulators over IT suppliers designated “critical”.
- e.g. 1.17 “A rule-making power will allow the financial regulators to set minimum resilience standards that critical third parties will be directly required to meet in respect of any material services that they provide to the UK finance sector. It will also allow the financial regulators to require critical third parties to take part in a range of targeted forms of resilience testing, to assess whether these standards were being complied with”.
- e.g. 1.19 “The financial regulators will have a suite of statutory powers, including the power to direct critical third parties from taking or refraining from taking specific actions; and enforcement powers

- including a power to publicise failings, and (as a last resort) to prohibit a critical third party from providing future services, or continuing to provide services to firms. The financial regulators' powers in relation to CTPs will be set out in primary legislation.”

<https://bills.parliament.uk/bills/3326>

312N Power of direction

- (1) A relevant regulator may, if it appears to the regulator to be necessary or expedient for the purpose of advancing any of its objectives, **direct a critical third party to**—
- (a) **do anything** specified in the direction, or
 - (b) **refrain from doing anything** specified in the direction.

40

These powers are very broad; for example, the Financial Services and Markets Bill gives the regulator the power to direct a critical third part to **do**, or to **refrain from doing, anything**. With immunity from liability for damages.

<https://publications.parliament.uk/pa/bills/cbill/58-03/0146/20146.pdf>

New Laws



312R Disciplinary measures

- | | |
|---|----|
| (1) This section applies if a relevant regulator considers that a critical third party has contravened a requirement imposed by or under this Chapter. | 25 |
| (2) The relevant regulator may publish a notice – | |
| (a) prohibiting the critical third party from entering into arrangements, or continuing, to provide services to authorised persons, relevant service providers or FMI entities; | 30 |
| (b) prohibiting authorised persons, relevant service providers or FMI entities who receive services from the critical third party from continuing to receive those services from that party; | |
| (c) prohibiting authorised persons, relevant service providers or FMI entities from entering into arrangements for receipt of services from the critical third party; | 35 |
| (d) providing for the provision of any services by the critical third party to be subject to such conditions or limitations as are specified in the notice; | |
| (e) providing for any receipt of services by authorised persons, relevant service providers or FMI entities from the critical third party to be subject to such conditions or limitations as are specified in the notice. | 40 |

If the critical third party doesn't comply, disciplinary measures include prohibiting the critical third party from contracting with financial institutions - and preventing financial institutions from contracting with them, or from continuing to receive services currently contracted. There is a right of appeal to the relevant Tribunal, and of course these measures can't be unreasonably applied, and would only be used as "a last resort" (quoting from Bank of England discussion paper).


<https://publications.parliament.uk/pa/bills/cbill/58-03/0146/20146.pdf>


Agenda



 Me: The perspective from which I'm looking at this

 New laws

 **Impact on cloud service providers**

 So what?

 How can we contribute to the conversation?

So that's the kind of thing that's being passed into law. Let's look now at the impact of this on cloud service providers.

Impact on cloud service providers



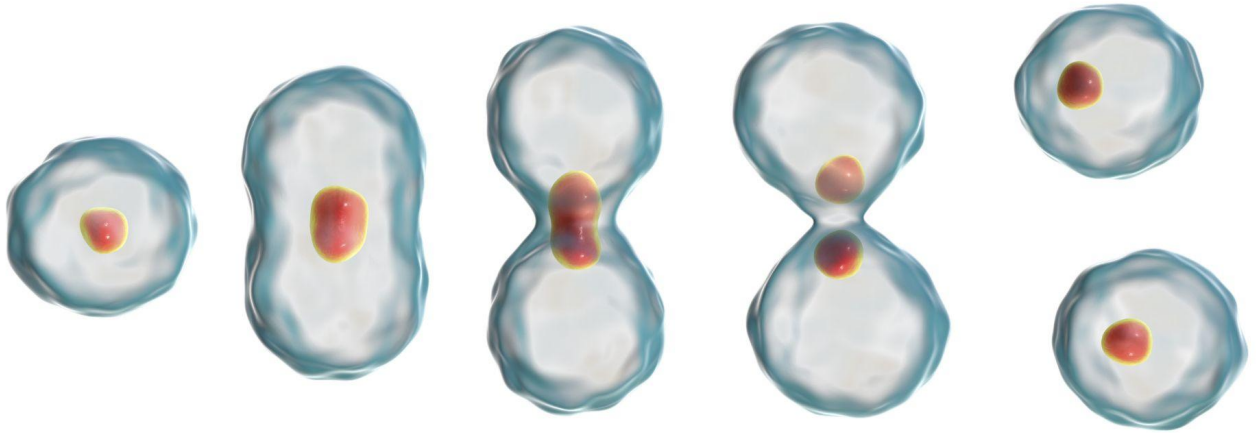
- These are my 'best guesses' at the moment; all this is far from clear. The cloud service providers are actively lobbying the regulators at the moment on what this will look like. But here's some broad brush strokes.

Impact on cloud service providers

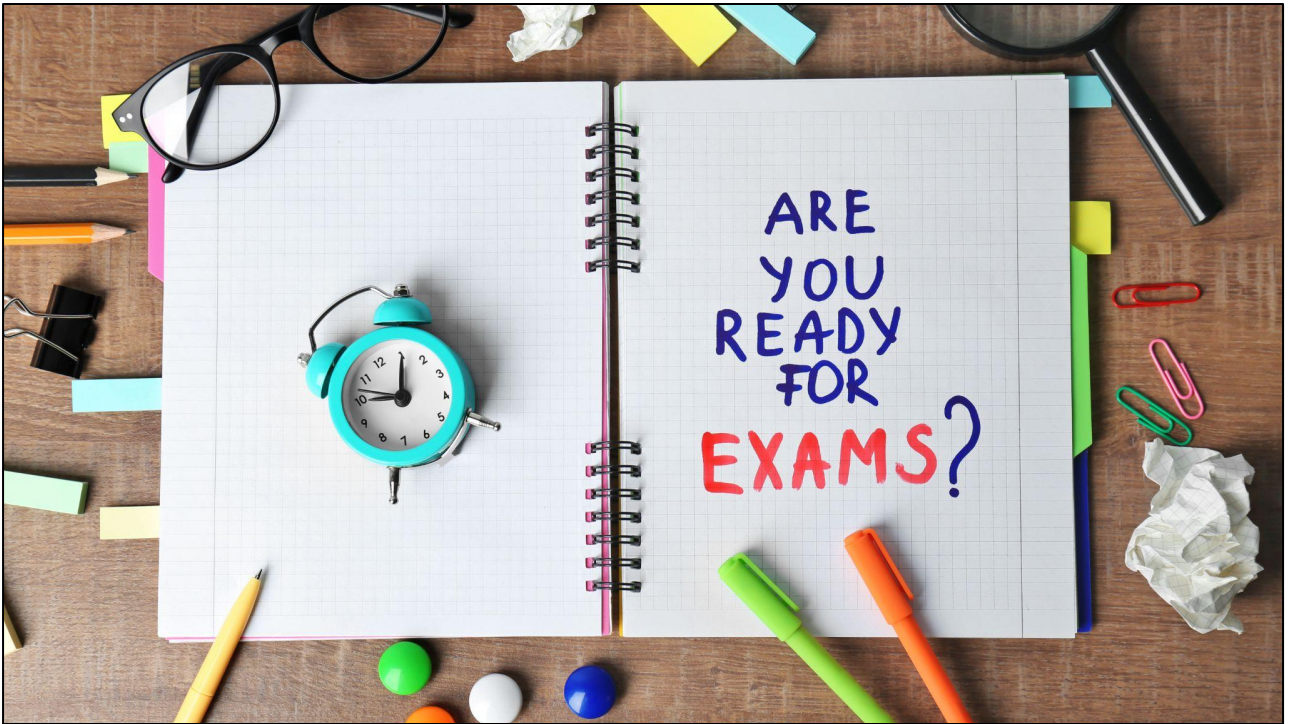


- The regulators will set resilience standards for the provision of cloud computing services to financial institutions, by 'critical third parties'.

Impact on cloud service providers



- Digression: This may produce an incentive for cloud service providers to separate out a division, or particular kinds of service, for the financial sector, in order to limit the amount of their operations that are in-scope for the regulators.



4.3. Regulators will have the ability to test cloud service providers against those resilience standards, likely using a combination of external assessment (certification by third parties) and internal assessment (robust internal processes of which the regulator has clear visibility).

Impact on cloud service providers



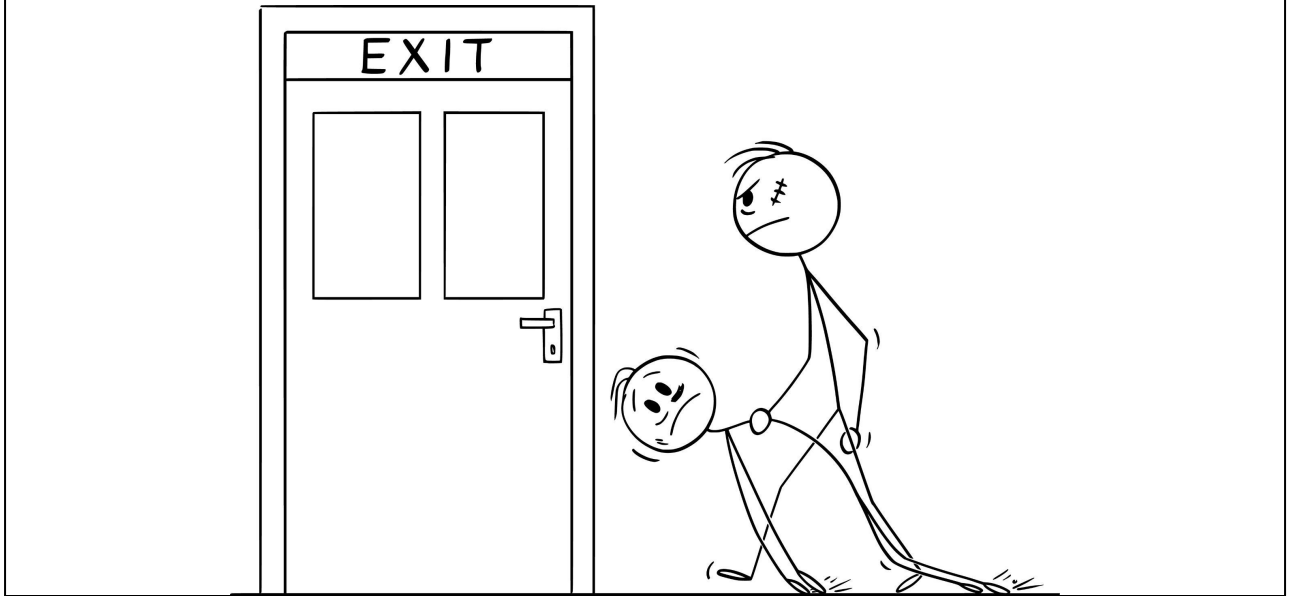
DOs



DON'Ts

- Regulators will have the legal right to insist that cloud service providers (providing service to financial institutions) take or refrain from taking specific actions.


Impact on cloud service providers




- Regulators will have the ability to bar from the market cloud service providers who don't meet the required standards or are insufficiently responsive to regulatory requests and instructions. Fines are also a possibility.


Agenda



 Me: The perspective from which I'm looking at this

 New laws

 Impact on cloud service providers

 So what?

 How can we contribute to the conversation?

So what?

So what?



- The SRE discipline has a lot to contribute here.






So what?



- The SRE discipline has a lot to lose if these new laws are implemented in a way which is counterproductive in terms of real-world outcomes for consumers (e.g. bureaucracy which does not help improve availability).

Agenda



-  Me: The perspective from which I'm looking at this
-  New laws
-  Impact on cloud service providers
-  So what?
-  How can we contribute to the conversation?

What can we contribute?

- We know all about defining standards of operational resilience. We have established best-practices for doing this. We should share them with the regulators and help to frame how standards of operational resilience are defined and tested.
- We're well-placed to be part of the conversation on what regulators should actually instruct cloud service providers to do and not to do in order to mitigate concentration risk at an operational level. E.g. could cloud providers prioritise key financial infrastructure (and other key infrastructure e.g. healthcare, transport) in a capacity crunch?

How should we contribute?

- We need to improve our collaboration with colleagues in risk/compliance and legal/regulatory, both operationally (dealing with current regulatory regime) and lobbying (influencing the future regulatory regime).
- I'm open to conversations and ideas on next steps. Existing trade bodies and professional associations might be a good place to start.



What are the key takeaways here?

Key Takeaways



#1 The stability of national and even global financial markets increasingly depends on the resilience of a small number of cloud service providers in a small number of regions.

First:

The stability of national and even global financial markets increasingly depends on the resilience of a small number of cloud service providers in a small number of regions.

#2 SRE is becoming massively important in the Finance sector (although using different vocabulary) and financial regulators are getting legal powers to enforce effective practice on the Cloud service providers (AWS/GCP/Azure).

Second:

SRE is becoming massively important in the Finance sector (although using different vocabulary) and financial regulators are getting legal powers to enforce effective practice on the Cloud service providers (AWS/GCP/Azure).

#3 There are people in "risk and compliance" roles within the Finance sector who are trying to achieve similar aims to SREs, but they speak a totally different language and have very different methods - we would benefit from improving our collaboration with them.

Third:

There are people in "risk and compliance" roles within the Finance sector who are trying to achieve similar aims to SREs, but they speak a totally different language and have very different methods - we would benefit from improving our collaboration with them.

Key Takeaways

#1

The stability of national and even global financial markets increasingly depends on the resilience of a small number of cloud service providers in a small number of regions.

SRECon22EM...

Key Takeaways

#2

SRE is becoming massively important in the Finance sector (although using different vocabulary) and financial regulators are getting legal powers to enforce effective practice on the Cloud service providers (AWS/GCP/Azure).

SRECon22EM...

Key Takeaways

#3

There are people in "risk and compliance" roles within the Finance sector who are trying to achieve similar aims to SREs, but they speak a totally different language and have very different methods - we would benefit from improving our collaboration with them.

SRECon22EM...

Q & A



LinkedIn: andrewellam

Q & A