Royalty-free stock photo ID: 1697986873.

Oct 07, 2021 13:53 BST

Spotlight on the future of outsourcing in the UAE's financial services sector

By Simon Fieldhouse, global managing director, Software Resilience

In our 'Spotlight on' series, we've been exploring operational resilience and third-party risk management within financial institutions (FIs), looking to the latest regulations and guidelines released by regulators across the globe and what they mean for businesses in the sector.

In recent years, there has been a global shift towards mitigating supplier risk for financial institutions. A wide range of guidelines have been established

across the world, including the Prudential Regulation Authority's (PRA) recommendations for outsourcing and third-party risk management in the UK, the European Digital Operational Resilience Act (DORA), and many more.

In the Middle East, the regulatory landscape is changing rapidly as businesses, particularly in the region's fintech sector, onboard new technology at pace and adopt more innovative ways of working.

This includes new regulation on outsourcing from the Central Bank of the UAE – but what does this mean for organisations?

What do the new guidelines advise?

This new regulation sets out principles and advice for financial institutions when developing innovative products and services, as well as catering to the business models of large organisations and new entrants to the financial services sector.

It aims to mitigate the risks which arise from the development and use of new technologies in order to ensure transparency and financial stability. This will in turn improve organisational efficiency and resilience within the sector, meaning that they can deliver more solutions to customers with lower risk.

Ultimately, this advice aims to promote growth and advancement in the UAE's financial services sector and encourage the adoption of innovative activities in a way that also manages risk.

What are the key guidelines that organisations should be aware of?

The regulations from the Central Bank of the UAE outline recommended minimum requirements for outsourcing agreements, including business continuity plans and certainty when it comes to how suppliers protect information. In particular, the guidelines highlight the importance of stressed exit plans and data recovery as a way for financial institutions to drive operational resilience.

- **Exit and resolution planning**

One key piece of advice set out by the Central Bank is the importance of defining and maintaining specific exit plans for each cloud computing arrangement that financial institutions have in place, accounting for developments such as new technology that may affect a planned exit. This is important to ensure that any disruption can be managed, and business continuity can be ensured in the case of a stressed exit.

This exit plan should clearly define the roles and responsibilities for the operation and management of any cloud computing arrangements, security controls and risk management controls.

A full plan should also identify and log the IT assets involved in the arrangement, based on criticality or confidentiality. Where cloud computing services are outsourced, steps should be set out within the stressed exit plan for managing and reviewing the contract between the institution and the outsourcing service provider to mitigate the risk of business disruption.

- **Data recovery**

Another important area that is highlighted in the guide is data recovery. It is important for financial institutions to establish procedures for data recovery in the case of any issues that could result in the loss of data – from natural disasters to accidental data loss.

Preventative and data controls should be used to lower the risk of business-critical or sensitive data being damaged or lost, and this should include securely backing up all data so that it's recoverable.

What should financial institutions do?

To remain compliant, financial institutions should ensure they have stressed exit plans in place and plans for data recovery in line with the new regulations, helping to ensure that sensitive and customer data is kept safe.

One way to lower risk and maintain compliance is to store business-critical information in escrow. This means that information is stored securely and can easily be retrieved in the event of any issues, ensuring continuity and availability for customers and stakeholders.

These regulations highlight the importance of ensuring financial institutions can continue to innovate soundly, and should spark further guidance from regulators across the globe.

Image: Royalty-free stock photo ID: 1697986873

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970