Cloud Infrastructure & Compliance

Navigating Regulatory Waters: D.O.R.A, SEPA Instant Payments, and the opportunities for Credit Unions

cuEngage Live saw 150+ members of the Credit Union industry come together to discuss Unlocking the Next Generation Credit Union.

There's no getting away from the fact that the regulatory demands on Credit Unions, particularly over the last 18-24 months, have been significant which can make the ability to comply in full, quite challenging.

However, it's important to emphasise that the success and scalability of Credit Unions is underpinned by compliance and regulation; and not to be constrained by it.

And that's exactly what we discussed at cuEngage Live in the breakout session "Staying Ahead of the Curve; Powering success through D.O.R.A and SEPA Instant Payments".

Operational Resilience

The ability to demonstrate Operational Resilience against the Central Bank of Ireland (CBI) Guidance that was published in 2021 could be considered as a driver for a more direct supervisory focus on the Credit Union sector, aligning closer with the expectations the regulator has on larger Irish PSPs.

Guidance, however, leads to interpretation, and a need for standards what would be appropriate and acceptable in how firms could demonstrate how prepared and mature they would be, in the face of an operational disruption.

The Wellington IT position was to bring together an internal Special Interest Group (SIG), with a specific technical skillset to represent the wider User Group, to get the value a Credit Union would need from an Operational Resilience Framework. This approach involved breaking down critical operational workflows and key dependencies within the organisation, with the purpose of shining a light on key components that ensure security and continuity of service for Credit Unions and in turn, the members.

Fundamentally it was about mapping out those workflows, and pinpointing the architecture and dependencies that support those services Wellington IT provides to the User Group. That perspective focuses on the strong control framework already in place, as well as highlighting where targeted continuity of service testing could be undertaken. Thus providing assurance to Credit Union Boards and ensuring the Credit Union member can continually avail of all services that they rely on their Credit Union for.

Risk Identification

Risk identification is key to any successful Operational Resilience Framework, and in addressing the x3 CBI Pillars directly. Risks will exist, but it is the layers of control around them that provides the much-needed assurance. They may come in the form of IT asset failures, physical infrastructure, third party dependencies, personnel risks etc.. and they're evolving, so must we.

Cyber risk is one that has become increasingly mainstream and a risk that mandates greater attention. Supervisory bodies have been tracking this closely and proposed an extension of the existing Operational Resilience Framework that we now live by, to include digital and cyber risk elements in greater focus as part of the Digital Operational Resilience Act (D.O.R.A).

D.O.R.A (Digital Operational Resilience Act)

While a reference to D.O.R.A might seem daunting as another incoming regulation, it is crucial to view its provisions as best practices that enhance a solid Operational Resilience Framework. Implementing the key components of D.O.R.A strengthens the overall resilience against cyber threats.

Currently, Credit Unions remain exempt from D.O.R.A, but this could change. Other Irish PSPs, like major retail banks, must fully comply by January 17, 2025.

It was interesting to discover that 73% of the cuEngage Live audience see D.O.R.A as a positive concept for the Credit Union industry, despite the challenges faced in meeting the baseline requirements.

Understand more about Cloud Infrastructure & Compliance.

Discover More