The implications of IT regulations for financial services organisations


pwc.ie/services/consulting/insights/it-regulation-implications-financial-service-organisations.html

07 October, 2020

The speed of regulatory change in the financial services sector is staggering. Changes in the regulatory landscape have had a profound impact on the financial services industry with a number of European Union and local regulatory requirements coming into effect.

Recent regulatory developments relating to technology risk impose various requirements for IT and cybersecurity risk management.

There are over 20 IT risk-related regulations that Irish registered entities should be aware of, with over 10 being issued during the past three years.

These regulations come from multiple sources, such as the European Banking Authority (EBA), Central Bank of Ireland, European Parliament, Houses of the Oireachtas, National Cyber Security Centre (NCSC), Basel Committee on Banking Supervision, and many others. The requirements raised by these regulations relate to various IT domains, such as IT governance and strategic planning, IT asset management, IT and cybersecurity risk management, incident management and monitoring, cloud computing and IT outsourcing. While a number of these regulations directly relate to IT, some, while not directly focussed on IT, include requirements relating to the management of IT systems and data.

As the use of technology continues to increase at staggering rates traditional governance and compliance efforts which may have had less of a focus on IT compliance will need to evolve to address IT regulatory requirements.

Key regulatory focus areas for technology risk

Technology risk has been on the regulatory agenda for years and expectations of regulators continue to evolve. While IT-specific requirements are spread across a number of IT domains we have included below some of the new IT regulations being addressed by our clients.

Payments

Payment Services Directive 2 (PSD2) went into full effect on 14 September 2019. Among other objectives, PSD2 aims for enhancing the security of payments. In support of this goal, European Banking Authority (EBA) has published sets of regulations that define the requirements around operational and security risk, the management and reporting of incidents and the mechanisms for authentication and connection security:

- Guidelines on the security measures for operational and security risks (PDF)
- Guidelines on major incident reporting (PDF)
- Regulatory technical standards on strong customer authentication and common and secure communication (PDF)

Cloud

It's expected that institutions wishing to adopt and reap the benefits of cloud computing should ensure that risks, specifically related to data security in multi-tenant, cloud environments, are appropriately identified and managed. Quite often organisations which consume cloud services and benefit from it in the constant digitalisation race do not have clear governance around it. This leads to an emergence of shadow IT (software not managed by the organisation's IT function) where organisations have limited visibility into how cloud is used, what information is collected and stored in the cloud and who has access to this data.

IT vendor or third-party risk (outsourcing)

Supervision focus on IT outsourcing has increased since outsourcing IT and data services poses security and other IT risks that still require governance by the regulated entities.

Technology risks within capital adequacy

The EBA guidelines on the assessment of Information and Communication Technology (ICT) risk establish ICT as a fundamental risk that will be examined under the Supervisory Review and Evaluation Process (SREP). Regulators may request that additional capital be held where financial institutions are unable to demonstrate how ICT risks to critical systems are identified, managed and understood. In order to prepare themselves, financial institutions should ensure ICT is robustly embedded within the operational risk management framework whilst also ensuring coverage of the associated risks within the financial institution's risk appetite and the Internal Capital Adequacy Assessment Process (ICAAP).

Challenges in the complex regulatory landscape

Due to the increased regulatory focus on IT, financial services organisations need to comply with multiple regulations, standards, and guidelines. This is often achieved without proper planning using a siloed approach where different organisational teams reactively respond (and often in isolation) to address an urgent compliance requirement for a single regulation and not ignoring existing investments in IT control often leading to duplicate efforts that may increase compliance costs unnecessarily. Managing the vast range of complex regulations, guidelines, and standards that impose IT-related requirements can be daunting. Financial services organisation face the following challenges:

- Which IT regulations are in scope for your specific organisation?

- How does IT and the various lines of defence work collaboratively to achieve compliance to IT regulations?
- How are compliance efforts evolved to include IT specific requirements?
- How does an organisation manage the diverse regulations that impose requirements for IT and cybersecurity?
- How to identify and manage overlaps between regulatory developments while reducing the costs of compliance?
- How to align regulatory requirements with international IT frameworks and standards, and integrate identified IT controls into its current control framework?
- How to derive benefit from existing IT control initiatives and marry regulatory compliance with these?

We are here to help you

PwC is helping our clients manage the overwhelming complexity of IT compliance by building a regulatory compliance framework to organise IT requirements around existing IT control initiatives based on international standards. Our team of IT regulatory compliance experts have worked with clients from the financial services industry to navigate the complexities in the IT regulatory space. We can:

- Assist with the identification of IT regulations applicable for your organisations
- Rationalising requirements for IT through aggregation and deduplication of mandates extracted from applicable regulations
- Conduct a gap analysis of your existing IT processes and regulatory requirements by mapping IT-related requirements to existing controls and practices
- Build IT and cybersecurity international standards and frameworks into your regulatory compliance framework for easy implementation, testing and monitoring and helping you derive benefit from existing IT control programmes