

ecoDa and Mazars webinar - New reporting requirements on Digital issues: What impacts for the auditor's selection?

Jan Matto - Partner IT Audit & Advisory, Forvis Mazars Netherlands

Petra Terasaho - Board Member and AC Chair

To introduce the topic, a presentation of the modern digital landscape was made.

It was explained that while digitalisation has been integrated more in the business environment due to increasing outsourcing of IT and integration of IT services and products, there has been a “loss of IT governance”. M.Matto urged that proper management of IT involves not only reporting and procedures but the construction of proper architecture. He also warned that modern cybercrime is operating at industrial scales, with non-strategic organisations being equally under threat as a vulnerability for more important organisations. In view of the massive financial damages, organisations must be fully aware of their networks to manage risks.

The discussion shifted to a presentation of the various relevant EU regulations:

- The Digital Services Act, requires relevant organisations to reduce their share of systemic risk while applying reasonable assurance.
- The DORA Act, aims at operational resilience for financial institutes and their IT providers which involves having a good organisational self-knowledge of the systems as well as tested processes for responding and recovering from attacks, as well as changing IT providers. The precise obligations scale with the strategic importance of each organisation. For boards it was emphasised that they will be liable, therefore they should have relevant understanding at board level, though not necessarily expertise. It was also claimed that they will need proper auditing and reporting channels from the IT department to the board.
- The NIS2 directive, which will come into effect in 2025, depending on national transposition, will include even more companies in its scope. Its precise requirements are unclear during transposition but it is said that it will follow DORA. The directive forms a framework that will be constantly the subject of updates to keep it relevant. It was recommended for relevant organisations to keep an eye on the work of ENISA, which will be publishing recommendations.
- The AI act will require all AI systems producers and non-private users in the EU market to conform to certain obligations. These involve not placing in the market certain prohibited systems, providing mitigation, oversight, and transparency for certain risky systems, and ensuring that all other AI systems are in fact not within the scope.

Finally, Mr Matto gave some advice on the subject of auditing. He recommended for audit teams to focus on IT issues to be multidisciplinary, with experts on technological, legal, and auditing issues. He also emphasised how the market is more demanding on assurance, an important point of value for digital systems.