DIGITAL OPERATIONAL RESILIENCE ACT

AAMCONSULTING

MANAGEMENT CONSULTING | IT CONSULTING | SECURITY CONSULTING

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

GENERAL INFORMATION

Aim of the regulation: Coordinate and synchronize the defense, risk management, data and information security against cyber threats within the EU

Entry into force: 17 January 2025 *(further technical standards will available by 17 January 2024 and 17 July 2024)*

Referred entities: The regulation applies to financial entities (credit institutions, payment institutions, insurance companies, investment companies, etc.) and ICT third-party service providers

Penalties: Member States will lay down rules establishing administrative penalties and remedial measures for breaches of the Regulation

for Critical ICT third-party service providers — up to 1% of the average daily worldwide turnover in the preceding business year

Actions defined by the DORA regulation

ICT risk management

- Continuous engagement in the monitoring of ICT risks, development of governance and control framework (incl. policies and procedures, roles and responsibilities, risk tolerance levels, KPIs, business continuity plan, business impact analysis, digital operation resilience training).
- Implement ICT incident review process (lessons learned, analysis) and introduce ICT awareness programs.

Digital operational resilience testing

- Continuous digital operational resilience testing of the financial functions, monitor preparedness, identify weaknesses and deficiencies, and implement corrective actions.
- Test the digital operational resilience by applying software solutions (Threat Lead Pen Testing (TLPT), overload tests (DDOS), data security testing, etc.)

ICT-related incident management, classification and reporting

- Harmonization of security incident monitoring and reporting processes and standardization of the reporting method.

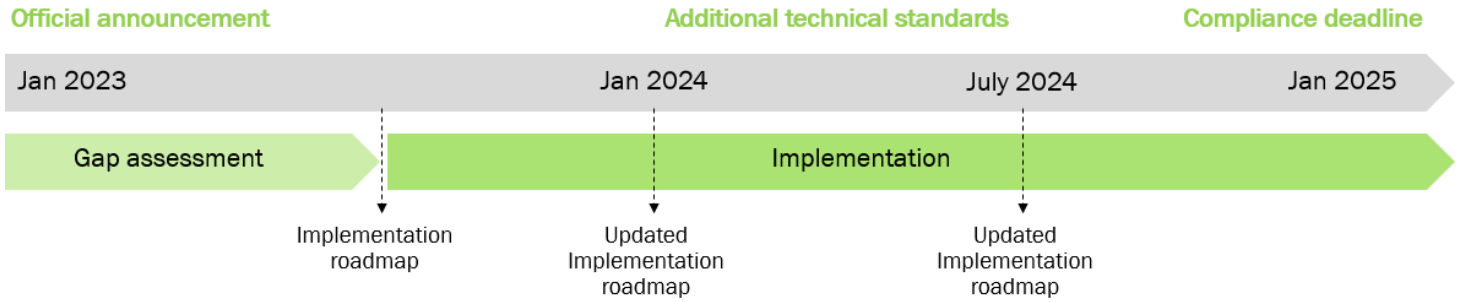
Managing of ICT third-party risk

- Supervise, measure and monitor ICT risks from third-party service providers.

Information-sharing arrangements

- Report to the competent financial authorities in a standardized format. Information shall be forwarded to an investigation team monitored by European Supervisory Authority.

AAM's approach



Gap assessment phase — AAM will perform an initial assessment of the organization's compliance against each requirement of the regulation with suggestions for necessary improvements and changes. At the end of the phase AAM will produce a comprehensive final report and a roadmap for compliance

Implementation phase — AAM will support the organization in remediating the non-compliances identified during the gap assessment. AAM will continuously update the implementation roadmap as additional technical standards are published

AAMCONSULTING

1133 Budapest, Hungary,
Capital Square Office, Váci út 76.
Telephone: +36 1 465 2070
Web: www.aam.hu

1000 Sofia, Bulgaria,
17 Moskovska St., 3rd floor
Telephone: +359 883 22 54 77
Web: www.aamconsulting.bg

DIGITAL OPERATIONAL RESILIENCE ACT

AAMCONSULTING

MANAGEMENT CONSULTING | IT CONSULTING | SECURITY CONSULTING

Tasks to be performed and AAM services

Development and customization of ICT risk management and framework

Identify, classify and document ICT-related business functions (management control, internal control, etc.) and configure the related ICT systems.

MAIN SERVICES

- Develop a strategy for digital resilience;
- Governance – Integration of IT security requirements within the organization;
- Development of risk management methodology and risk management plan;
- Development of internal and external procedures and regulations;

Test resistance due to digital operation

Test and review key ICT systems, documents and applications at least once a year. Key functions and services of the organization should be tested every three years using advanced methods like threat-based intrusion testing.

MAIN SERVICES

- Define test strategy and scenarios;
- Development of test methodologies and procedures (penetration tests, overload tests (DDOS), data security test, etc.);
- Preparation of test plans, determination of scope;
- Coordination of the testing process;
- Development of test report structures;
- Provide guidance for digital reporting to authorities;

Establish conditions for monitoring third-party ICT risks

Monitor documentations, services, risk assessments, furthermore harmonization and control of main elements of the third-party services providers from the beginning of the collaboration.

MAIN SERVICES

- Development/ revision of ICT risk strategy and regulations;
- Integration of third-party ICT risk procedures into the corporation's risk management framework;
- Assessment of compliance and third-party contracts;
- Define exit strategy and transition plan;

Support the revision of the ICT framework and Event management

Plan the regular review of the information security of ICT systems required by the regulation like coordinate the reviews, document the observations and prepare action plans. Monitor, record and report significant risks to authorities and handle feedbacks from supervisory audits.

MAIN SERVICES

- Preparation of the plan review;
- Coordination of revision process;
- Record and evaluate the results obtained;
- Identification of preventive and corrective measures;
- Identification of the incidents, follow up and manage the results obtained, log analysis and support the incident management process;

AAMCONSULTING

1133 Budapest, Hungary,
Capital Square Office, Váci út 76.
Telephone: +36 1 465 2070
Web: www.aam.hu

1000 Sofia, Bulgaria,
17 Moskovska St., 3rd floor
Telephone: +359 883 22 54 77
Web: www.aamconsulting.bg