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

The aim of the regulation:
Coordinate and synchronize the defense, risk management, data and information security against cyber threat within the European Union.

Entry into force:
It shall apply from 12 months after the date of entry into force.

Referred entities:
The regulation applies to the entities, listed in the document in Article 2, section 1.

Objectives defined by the regulation

- Address and manage IT risks and threats of the financial sector at European Community level.
- Increase the resilience of financial services to cyber threats.
- Continuous testing of the financial functions, monitor preparedness, identify weaknesses and deficiencies, and implement corrective actions.
- Harmonization of security incident reporting and standardization of the reporting method for Information and Communication Technologies (ICT).
- Supervise and monitor the services, documentations and risk assessments provided by third-party services.
- Publish data and provide information about cyber threats for supervisory authorities.
- Reduce administrative and financial burdens related to compliance.

Expectations proposed by the regulation

- Continuous engagement in the control of monitoring of the ITCs, risk management and development of the framework (survey, planning, implementation, analysis, etc.) .
- Test the digital operational resilience by applying software solutions (penetration tests, overload tests (DDOS), data security testing, etc.) .
- Enforcement of the principle of proportionality (based on organizational size, activity, business profile) in relation with ICT risk management, digital resilience testing, security incident reporting and service oversight provided by third-party services.
- Report relevant information and data to the competent financial authorities in a standardized format. Information and thus collected shall be forwarded by the authorities to an investigation team which shall be monitored by European Supervisory Authority.
- Measure and monitor ICT risks from third-party service providers.
- Share data and information on cyber security and vulnerability within the European Union.

AAMCONSULTING

1133 Budapest, Hungary
Capital Square Office, Váci út 76.

Telephone: +36 1 465 2070
Fax: +36 1 465 2078

E-mail: aam@aam.hu

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 (BCP-DRP);
- 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
Fax: +36 1 465 2078

E-mail: aam@aam.hu