Financial Supervisory Authority

Rule no. 40/2016
amending and supplementing Rule no. 6/2015 of the Financial Supervisory Authority on the management of the operational risks arising from the information systems used by entities regulated, authorized/licensed and/or supervised by the Financial Supervisory Authority

In force since December 23, 2016
Published in the Official Journal, Part I, no. 1040 of December 23, 2016.
There are no amendments until December 28, 2016.

Further to the deliberations held in the meeting of the Financial Supervisory Authority's Board of December 14, 2016,

and based on the provisions of Art. 3 Para (1) Letter b), Art.5, Art. 6 Para (2) and Art. 14 of Government Emergency Ordinance No. 93/2012 on the establishment, organization and operation of the Financial Supervisory Authority (ASF), approved as amended and supplemented by Law No. 113/2013, as subsequently amended and supplemented;

The Financial Supervisory Authority hereby issues this rule:

Art. I. - The Rule of the Financial Supervisory Authority no. 6/2015 on managing operational risks generated by information systems used by entities regulated, authorized/approved and/or supervised by the Financial Supervisory Authority, published in the Official Journal of Romania, Part I, no. 227 of 3 April 2015, shall be amended and supplemented as follows:

1. In Article 1, paragraph (1) shall be amended to read as follows:

"**Art. 1. -** **(1)** This rule sets the requirements at the level of entities authorized/licensed/registered, regulated and/or supervised by the Financial Supervisory Authority A.S.F., for the identification, prevention and mitigation of the potential adverse impact of operational risks generated by the use of information technology and communication at the level of people, processes, systems and external environment, including facts relating to cybercrime."

2. In article 2, the introductory part shall be amended to read as follows:

"**Art. 2. -** This rule shall apply to the following categories of entities authorized/licensed/registered, regulated and/or supervised by A.S.F., hereinafter referred to as entities:".

3. In article 2, the introductory part of letter b) shall be amended to read as follows:

"**b)** investment management companies (IMC), alternative investment fund managers (AIFM), as follows:".

4. In Article 2, letter f) shall be amended to read as follows:

"**f)** Investors Compensation Fund, Policyholders Guarantee Fund and Private Pension System Rights Guarantee Fund;".

5. In article 6, paragraphs (4) and (5) shall me amended and shall have the following content:

"**(4)** The classification and re-classification of the entities referred to in art. 2 letter b) shall be made in January of each calendar year, on the basis of the value of assets in the portfolio/managed in the last working day of the previous year.

(5) The classification and re-classification of the entities referred to in art. 2 letter d) shall be made in January of each calendar year, on the basis of the activity authorized by A.S.F. and holding the capacity of market maker/liquidity provider in the last working day of the previous year."

6. In article 8, after paragraph (2) a new paragraph shall be introduced, paragraph (3), with the following content:

"**(3)** Information systems providing to IMC/AIFM and their investors access to electronic platforms for the distribution of units shall ensure at least, without limitation:

a) security and integrity of data processed by using a security method, on data sent to the electronic platforms of distribution of units;

b) mechanisms ensuring the non-repudiation of data transmitted and received;

c) real-time logging of information on investors' instructions transmitted;

d) mechanisms of non-repudiation of the integrity of registration of information system operations."

7. In article 9, the introductory part of paragraph (9) shall be amended to read as follows:

"**(9)** The agreement referred to in paragraph (7) shall contain an express clause under which the auditor undertakes to notify A.S.F. in writing as soon as possible, but no later than 10 days after the finding of any fact or act in relation to the computer and communications system used by the entity and which:".

8. In article 9, the introductory part of paragraph (10) shall be amended to read as follows:

" **(10)** The agreement referred to in paragraph (7) shall contain an express clause under which, upon the written request of A.S.F., the auditor undertakes to submit to A.S.F. within 10 days from request:".

9. In article 10, the introductory part of paragraph (2) shall be amended to read as follows:

" **(2)** To obtain ASF’s approval, the external IT auditor shall submit to A.S.F. an application, in which it shall mention the sector/sectors in which entities for which it plans to provide services are authorized/licensed/registered, regulated and/or supervised by A.S.F., together with the documentation, which shall include the following, as the case may be:".

10. In Article 10, paragraph (2), point (v) of letter a) shall be amended to read as follows:

"**(v)** proof of experience and specialization in the field of external audit of information systems;".

11. In Article 10, paragraph (2), points (ii) and (iii) of letter b) shall be amended to read as follows:

"**(ii)** curriculum vitae of the IT auditor, dated and signed, with the presentation of professional experience in the external audit of information systems;

(iii) copy of the certificate of IT auditor, signed for conformity with the original, proving the experience in the field of external audit of information systems;".

12. In article 10 paragraph (9), after point (vii) of letter j), a new point shall be introduced, point (viii), with the following content:

"**(viii)** description of the way in which the audit of assessment referred to in art. 5 paragraph (1) was conducted."

13. In Article 10 paragraph (9), letter o) shall be amended to read as follows:

"**o)** affidavit of the external IT auditor regarding the fact that it is not in relationships with the audited entity, with members of the management structure or with its employees which could affect its independence or objectivity of the audit activity."

14. In Article 11 paragraph (1), letter a) shall be amended to read as follows:

"**a)** allow compliance with the entity with the provisions of this rule, so that, by outsourcing the activity, no avoidance of compliance with the provisions of the rule is registered;".

15. In Article 11, paragraph (4), the introductory part and points (i) and (iv) of letter c) shall be amended to read as follows:

"**c)** supporting documents depending on the type of service or activity carried out, as follows:

(i) for all suppliers - SR ISO/IEC 27001 or certifications for equivalent standards;

. . . . . .

(iv) for providing hosting or outsourcing services through datacenters - compliance with technical conditions under TIA-942 Level 2 or equivalent;".

16. In article 14, after paragraph (5) a new paragraph shall be introduced, paragraph (6), with the following content:

(6) The reports referred to in paragraph (3) shall be submitted to A.S.F. according to the reporting system communicated by each organizational structure within A.S.F. with responsibilities of supervision of the respective entity."

17. Article 15 shall be amended to read as follows:

"**Art. 15. -** Failure to comply with the provisions of this rule by entities referred to in art. 2 constitutes an offense according to the provisions of art. 39 paragraph (2) letter a) of Law no. 32/2000 on the activity and supervision of insurance and reinsurance intermediaries, with subsequent amendments and additions, of art. 163 paragraph (1) letter a) of Law no. 237/2015 on the authorization and supervision of the insurance and reinsurance business, of art. 272 paragraph1 (1), letter a) point 6, letter b) point 5, letter c) point 4, letter d) point 4, letter e) point 7, letter f) point 3, letter h) point 8, letter i) point 3, letter j) point 17 and letter k) point 3 of Law no. 297/2004, with subsequent amendments and additions, of art. 141 paragraph (1) letter g) of Law no. 411/2004 on privately managed pension funds, with subsequent amendments and additions, and, respectively, of art. 121 paragraph (1) letter k) of Law no. 204/2006 on voluntary pensions, with subsequent amendments and additions, depending on the type of the entity."

18. In Article 16, paragraph (4) shall be amended to read as follows:

"**(4)** For all entities, the first IT audit shall be conducted so that the report of the external IT auditor be submitted to A.S.F. by no later than 31 December 2016."

19. In article 16, after paragraph (4) a new paragraph shall be introduced, paragraph (5), with the following content:

"**(5)** By way of derogation from the provisions of paragraphs (1)-(4), the Policyholders Guarantee Fund and the Private Pension System Rights Guarantee Fund shall make the first reports starting with 2018, for 2017, within the deadlines referred to in art. 14."

Art. II. - **(1)** External IT auditors that have submitted the documentation for licensing before the entry into force of this rule shall be licensed according to the provisions of the rule in force on the date of submission of the application. External IT auditors licensed and registered in the Public Register of the Financial Supervisory Authority (A.S.F.) before the entry into force of this rule may provide services for entities supervised by A.S.F.

(2) The external IT auditor that is licensed by A.S.F. and shows an intention to also provide services for entities within other sector/sectors than that/those for which it is registered in the Public Register of A.S.F. is required to send a notification to A.S.F., mentioning the sector/sectors in which the respective entities are authorized/licensed/registered, regulated and/or supervised by A.S.F.

(3) Based on the notification referred to in paragraph (2), the external IT auditor shall be able to provide services only after its registration in the Public Register of A.S.F. in the section related to the sector/sectors mentioned in the notification.

Art. III. - This rule shall be published in the Official Journal of Romania, Part I, and in A.S.F. Bulletin, and shall enter into force on the date of its publication.

President of the Financial Supervisory Authority,
Mişu Negriţoiu

Bucharest, 16 December 2016.
No. 40.