Rule no. 4/2018 on the management of operational risks generated by information systems used by authorized / licensed / registered entities, regulated and / or supervised by the Financial Supervisory Authority

In force starting April 15, 2018

Published in the Official Gazette, Part I no. 233 of March 16, 2018. There are no changes until April 15, 2018.

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, organisation and operation of the Financial Supervisory Authority, approved as amended and supplemented by Law No. 113/2013, as subsequently amended and supplemented;
further to the deliberations held in the meeting of the Financial Supervisory Authority's Board of February 28, 2018,
The Financial Supervisory Authority hereby issues this rule:

CHAPTER I
General Provisions

Art. 1. - (1) This rule lays down the requirements at the level of the entities authorised/licensed/registered, regulated and/or supervised by the Financial Supervisory Authority, hereinafter referred to as *ASF,* for the identification, prevention and reduction of the potentially adverse impact of the operational risks arising from the use of the information and communications technology in terms of persons, processes, system and external environments, including cybercrime acts.

(2) This rule lays down activities and operations for the assessment, supervision and control of the operational risks arising from the use of information systems and information security, as well as management of the risks related to the security of the major information systems in order to ensure the IT security of the entities stipulated in paragraph (1).

Art. 2. - This rule applies to the following categories of entities authorised/licensed/registered, regulated and/or supervised by ASF, hereinafter referred to as *entities:*

a) market operators/system operators;

b) investment management companies (IMCs), alternative investment fund managers (AIFM), respectively:

1. Companies with net assets in portfolio/managed with a total, aggregate value for all managed funds exceeding EUR 250 million, the RON equivalent;

2. Companies with net assets in portfolio/managed with a total, aggregate value for all managed funds of up to EUR 250 million, the

RON equivalent;

c) central depositories, clearing houses/central counterparties;

d) intermediaries - investment firms (SSIFs), branches of intermediaries of other non-member States and credit institutions of Romania authorised by the National Bank of Romania in accordance with the bank legislation and registered in ASF's public registry as intermediary, i.e.:

1. intermediaries as independent operator;
2. SSIFs significant in terms of size, internal organization and nature, expansion and complexity of activity, according to specific regulations;
3. intermediaries providing related safe custody and management services of financial instruments on behalf of clients, including custody and related services, such as the administration of funds or guarantees;
4. intermediaries using trading facilities through the Internet (ADP/AS) - platforms through which clients' orders are taken and sent;
5. intermediaries as market makers and/or liquidity providers;
6. intermediaries dealing on own account and not covered by the categories referred to in Items 1-5;
7. intermediaries not dealing on own account and not covered by the categories referred to in Items 1-5;

e) traders;

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

g) insurance/reinsurance undertakings;

h) insurance/reinsurance brokers;

i) The Motor Vehicle Insurance Bureau in Romania

j) entities carrying out depository activities of the units of undertakings for collective investment and the assets of private pension funds;

k) private pension funds management companies.

Art. 3. - (1) The entities referred to in art. 2 have the obligation to identify all the major information systems used on both components, namely the hardware and software infrastructure, which are essential in the work carried out by them.

(2) The major information systems referred to in paragraph (1) shall include, but are not limited to, the following, depending on the type of the entity:

a) information systems necessary for the smooth running of the activity authorized / approved by ASF:

1. trading systems / alternative trading systems;

2. clearing, settlement, depositary and custody systems;

3. platforms / applications for trading or distribution by internet or telephone;

4. management systems of policyholders;

5. management and underwriting systems of insurance contracts;

6. recording and management systems for claim files;

7. platforms for the issuance of insurance contracts;

8. systems for the calculation of fees;

9. reinsurance contracts management systems;

10. management systems for participants in private pension funds;

11. portfolio management systems for financial instruments of private pension funds;

12. call-center systems;

13. online applications used for dissemination and to inform customers, such as accessing online accounts;

14. back-office information systems other than those falling under points 1 to 13 ;

b) internal systems to ensure reporting to ASF and other financial market institutions / entities;

c) information systems used in the entity's financial-accounting activity, such as accounting programs;

d) electronic voting systems and other IT systems with significant implications for the entity's governance system, such as teleconferencing / videoconferencing systems used in remote meetings of the Board of Directors / Supervisory Board;

e) information systems with impact on the business continuity and disaster recovery plan;

f) central business applications other than those falling letters under a) -e);

g) computer infrastructure used for major IT systems hosted at data center locations.

(3) Entities are required to compile and update permanently a register with the major information systems identified in accordance with paragraphs (1) and (2) .

(4) The register, prepared in accordance with the provisions of paragraph (3) shall be subject to verification by the IT auditor.

Art. 4. - Entities shall extend the scope of the IT audit to other systems in the situations referred to in Art. 29 para. (1).

Art. 5. - (1) The provisions of this rule shall be applied by the entities according to the risk category established by ASF in accordance with Art. 10 and 11 and in relation to the internal risk assessment based of the best practices in the field.

(2) The risk category corresponding to each type of entity shall be established by ASF depending on the nature, size and complexity of such entity’s activity, as well as on the risks they may pose, and the impact on the activity.

Art. 6. - (1) Entities shall annually assess and continuously monitor the operational risks arising from the use of major information systems, prioritize resources, implement information security measures and monitor their effectiveness through the application of risk management.

(2) The manner of implementation of the information security measures provided for in par. (1) shall be determined by each entity, depending on the risk profile, risks identified, incidents occurred, in accordance with the applicable legal requirements.

Art. 7. - Entities shall participate in the collection, analysis, monitoring and reporting of IT security events within the system to be developed by ASF

Art. 8. - The terms and expressions used in this Rule shall have the meaning given in Annex no. 1.

CHAPTER II
Classification of Entities in Risk Categories

Art. 9.- (1) For the purposes of this rule, each of the entities referred to in Art. 2 shall be classified in one of the following risk categories:

a) "major risk",
b) "significant risk",
c) "medium risk",
d) "low risk".

Art. 10. - The classification of the entities referred to in art. 2 letters a) - j) in the risk categories mentioned in art. 9 is done as follows:

a) in the category of major risk the entities referred to in art. 2 letter a) , letter c) , letter d) pt. 1 and letter i) ;

b) in the important risk category the entities referred to in art. 2. letter d) pt. 2, 4 and 5 , letters g) and j) ;

c) in the category of medium risk the entities referred to in art. 2 letter b) point 1 , letter d) pt. 3 and pt. 6 and letter f) ;

d) in the low risk category the entities referred to in art. 2 letter b) point 2 , letter d) pt. 7 , letters e) and h) .

Art. 11. - The classification of the entities referred to in art. 2 letter k) shall be carried out individually in the risk categories provided under art. 9, according to the provisions of art. 44 par. (4) letter e) and Art. 51 of Rule no. 3/2014 on the internal control, internal audit and risk management in the private pension system issued by the Financial Supervisory Authority's Board.

Art. 12. The classification and re-classification of the entities referred to in Art. 2 letter b) shall be made in January of each calendar year, based on the total value of the assets in the portfolio/managed on the last working day of the previous year.

Art. 13. 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 authorised by ASF and possession of status of market maker/liquidity provider on the last working day of the previous year.

Art. 14. An entity that carries out several types of activities authorized by ASF and falls into several risk categories of those specified in art. 9 comply with the highest risk category obligations established by this rule.

CHAPTER III
Provisions on mandatory activities carried out by entities

Art. 15. - (1) Entities shall carry out at least the mandatory activities corresponding to each risk category as referred to in Art. 9, as listed in the table

of Annex No. 2.

(2) Entities are required to conduct a vulnerability scan every year.

(3) The penetration tests found in the table of annex no. 2 to letter B) point 8 letter c) have the objective of testing the security of the applications included in the audit, testing the security of the operating systems used within the entity, and testing the network infrastructure security, as well as testing the vulnerabilities identified by the security scan.

(4) Entities are required to ensure that the following are conducted in the IT audit period, without limitation to: external penetration tests, internal penetration tests, and social engineering tests.

(5) ASF will publish on its website a guide that contains details and parameters on how to implement the mandatory activities provided for in paragraph (1). The guide is indicative and can be updated by ASF according to good practice in the field.

Art. 16. - (1) With respect to the activity carried out, the entities shall ensure that the information systems meet at least the following requirements:

a) ensure the integrity, confidentiality, authenticity and availability of data in accordance with the risk category of the information system defined internally by the entity, and the processing thereof in accordance with ASF's regulations, taking into account the possibility to update the same according to the changes in the applicable law;
b) ensure that the contents of the information indicated in the reporting forms, as provided for in the specific legislation, as well as other reports required by ASF's regulations, are complied with;
c) ensure the storage and retention of the data recorded and logged by the trading systems, corresponding to issuing insurance contracts/approval of claims files and back-office systems for a period of time in accordance with the applicable laws in force. The data storage system shall ensure that these data may be transmitted or made available to ASF, upon request;
d) ensure particulars of the data subject to processing or verification and precise identification of the time when entries were made and the identification of the system users at that moment;
e) ensure the confidentiality and protection of information and programs through passwords, identification codes for access to information, as well as back-ups for the programs and information held;
f) ensure security and control mechanisms of major information systems, to preserve the safety of stored data and information, files and databases, including in the case of the risk events.
g) ensure the reconstruction of the reports and information subject to verification;
h) ensure the possibility of restoring data archived on external digital media such as, but not limited to, information, input data, financial statements.

(2) Entities are required to ensure that the following requirements are met:

a) multiple people cannot be multiple-logged on the same application

account.

b) non-disclosure of credentials, passwords or any other authentication system by their users;

c) use of personalized credentials only for authorized / registered staff;

d) logging, monitoring and archiving in accordance with specific regulations in the field so as to ensure control of users' access, place of access and accessed data, including personal data;

e) using authentication systems that use at least two factors;

f) ensure that authorized users do not provide authentication items to third parties.

Art. 17. - (1) Entities are required to annually test the IT security incident response plan.

(2) The IT security incident response plan must provide for simulation of a computer security incident and cover all IT systems and networks used by the entity.

Art. 18. - (1) Entities have the obligation, within maximum 45 days after the completion of the testing provided for in art. 17, to draw up a test report containing, but not limited to, the following information:

a) the implementation method of each stage of the IT security incident response plan;

b) how to manage internal and external communication throughout testing;

c) the causes and the real / potential impact of the IT security incident on the data of the entity;

d) suggestions to improve security measures for IT incidents;

e) suggestions to improve the IT security incident response plan.

(2) The test report provided in paragraph (1) shall be kept at the office of the entity that is required to present it to the IT auditor and to ASF at the request of the latter.

Art. 19. - Major IT systems that provide intermediaries and their customers with access to electronic trading platforms as well as major IT systems that highlight clearing, settlement and registry operations for financial instruments and operations with these instruments shall ensure, without limitation to:

a) the security and integrity of the data processed by using a way of securing of both data sent to electronic trading platforms and to clearing, settlement and registry platforms as well as the data received from these platforms;

b) mechanisms to ensure non-repudiation of the data sent and received;

c) real-time logging of information about orders sent for execution, the status of these orders, and the changes that are brought to these orders in the course of their existence by customers and intermediaries using these major information systems;

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

Art. 20. - Information systems that provide access to IMCs and AIFMs and their investors access to electronic platforms of distribution of shares shall ensure at least, but not limited to:

a) the security and integrity of the data processed through the use of a security

method, on the data sent to electronic platforms of distribution of shares;
b) mechanisms to guarantee non-repudiation of the data sent and received;
c) the real-time logging of information on the instructions of investors sent to IMC/AIFM;
d) mechanisms for non-repudiation of the integrity of the registration of information system operations.

CHAPTER IV
Auditing and Testing Major Information Systems

Section 1
Provisions on the IT Audit

Art. 21. - (1) The entities have the obligation to audit major information system, as follows:

a) the entities in the high risk category have the obligation to externally audit major IT systems used, with annual frequency so that the audit period is a calendar year, starting with the first month of January following the end of the period previously under IT audit;

b) entities in the important risk category have the obligation to audit, externally or with internal certified resources, the major information systems used every 2 years so that the period under audit is 2 consecutive calendar years starting with the first month of January after the end date of the period previously under IT audit;

c) entities in the medium risk category have the obligation to audit, externally or with internal certified resources, the major information systems used every 3 years so that the period under audit is 3 consecutive calendar years starting with the first month of January after the end date of the period previously under IT audit;

d) entities in the low risk category have the obligation to audit, externally or with internal certified resources, the major information systems used every 4 years so that the period under audit is 4 consecutive calendar years starting with the first month of January after the end date of the period previously under IT audit

(2) The IT audit period is the period between two successive audits.

Art. 22. – The entities which carry out the audit with certified internal resources have the obligation to use certified IT auditing personnel employed within the entity or within a company within the same financial group, in compliance with the provisions of this rule and with internationally certified methodologies.

Art. 23. The external audit shall be carried out on the basis of an IT audit contract concluded between the entity that requested the auditing and an external auditor registered the List of external IT auditors kept by ASF according to Art. 38.

(2) Entities may not contract the IT audit with the same external IT auditor for more than 3 consecutive audits of those referred to in art. 21.

Art. 24. The entity has the obligation to ensure that the IT audit contract

includes mandatorily the clauses relating to the fact that the external IT auditor is required to meet the requirements necessary to carry out the audit of major information systems, in accordance with the provisions of this rule and with the good practices in the field.

Art. 25. The external IT auditor shall notify in writing to ASF in the shortest time possible, however, not later than 10 days starting the finding, of any fact or act in connection with the major information systems used by the entity, which:

a) is likely to affect the continuity of the business of the entity being audited;

b) may lead to a qualified audit opinion, to the impossibility of expressing a professional opinion or a negative opinion.

Art. 26. - At the written request of ASF, the external IT shall provide ASF, within maximum days as of the request, with the following:

a) any report or document which has been brought to the attention of the audited entity;

b) a statement of the reasons for the termination of the IT audit contract, regardless of their nature;

c) any other information or documents required in connection with the external IT audit work.

Art. 27. - The IT auditor carrying out the IT audit activity to the entities referred to in Art. 2 has the obligation to prepare and present to the management of the entity a situation of the deficiencies and vulnerabilities identified.

Art. 28. - Upon completion of the IT audit, IT auditors are required to prepare an IT audit report accompanied by annexes covering at least the elements set out in the reporting model set out in Annex no. 3, without limitation to those.

Art. 29. - (1) ASF may impose on the entity an obligation to audit any IT systems if:

a) following the findings it results that the entity did not carry out all the minimum required activities for the risk category in which it was classified, according to the provisions of art. 10 or 11, or the activities carried out are of a formal nature;

b) believes that additional investigations are needed at the level of IT systems.

(2) The establishment by the ASF of the obligation to audit other IT systems according to par. (1) also includes the deadline by which the entity is required to send to ASF the audit report and this deadline may not exceed 90 days from the date of the requirement to audit other information systems by ASF.

Art. 30. - Entities, including those performing IT audit with certified internal resources, are required to take all necessary measures to avoid conflicts of interest that may arise in conducting IT auditing.

Art. 31. - Entities, including those performing IT audit with certified internal resources, are required to ensure that the IT audit activity is independent of the audited activity in order not to compromise its objectivity, and that IT auditors are independent and objective in all aspects of the IT audit activity.

Art. 32. - In applying the provisions of art. 31, the entities performing the IT

audit with certified internal resources are obliged to:

a) ensure that the IT auditor notifies ASF in writing as soon as possible, but not later than 10 days after the finding, of any fact or act relating to the major information systems uses by the latter and which is likely to affect continuity of the activity of the audited entity or may lead to a qualified audit opinion, to the inability to express an audit opinion or to a negative audit opinion;

b) present at the request of ASF within 10 days, any report or document that has been brought to the attention of the audited entity or any other information or documents requested in connection with the IT audit activity.

Art. 33. - Entities, including those performing IT audit with certified internal resource, are required to provide the IT auditor with integral, appropriate, relevant and timely information in order to enable the IT auditing to be carried out in good working order.

Art. 34. - Compliance with the provisions of art. 25 and 26 is not contrary to the ethical and professional provisions, does not constitute a breach of professional secrecy imposed by contractual clauses or legal provisions and shall not entail any liability of the natural person/entity concerned.

Section 2
Testing major information systems

Art. 35. - (1) The entity has the obligation to keep track of the following major changes to major information systems:

a) the complete change of major information systems / programs;

b) outsourcing IT services;

c) changing electronic archiving, restoring or synchronizing processes of databases.

(2) In the event of decommissioning of a major information system, the entity is required to request an IT audit with certified internal or external resources addressing the systems to be decommissioned.

Art. 36. - (1) The entity has the obligation to test major information systems prior to first use and during any changes in their lifecycle, regardless of whether they are made with internal resources or by external suppliers.

(2) The result of the tests provided for in paragraph (1) is recorded in an IT test report that includes, but is not limited to, the following:

a) testing team;

b) the purpose of testing;

c) the testing period;

d) description of the computer program tested;

e) identifying used applications and people involved;

f) analysis of the risks involved in acquiring or modifying the computer program, possible vulnerabilities and associated risk mitigation measures, by system or computer program controls;

g) a description of the manner in which the tests, test scenarios were carried out, the relevant rules or standards applied and the result of the test;

h) the conclusion of the test team;

i) signature of test team members.

Art. 37. - The entity is required to maintain the IT test reports for at least 5 years after the decommissioning of the major IT system and to make them available to ASF or the IT auditor upon request.

CHAPTER V
Registration of the external IT auditor

Art. 38. - The external IT auditor, seeking to provide IT services to the entities to which the provisions of this rule apply is required to be listed in the List of external IT auditors maintained by ASF.

Art. 39. In order to be included in the list provided for in art. 38, the external IT auditor shall submit to ASF a request stating the sector(s) in which the entities for which it intends to provide IT audit services operate, together with the documentation that should include the following, as applicable:

a) the external IT auditor's identification data:

1) the full name/name and address/office (full address);

2) the address where it pursues its business;

3) the telephone/fax, email, website address;

b) in the case of the IT certified auditor who is a natural person and of the representative of the external IT audit company, who will sign the audit report, the following documents shall be submitted, as applicable:

1. the copy of the IT auditor's identity card;
2. the IT auditor's curriculum vitae, dated and signed, including the professional experience with the presentation of professional experience in IT external auditing of information systems;
3. the copy of the IT auditor certification, signed as true to the original, which will include the expertise in external IT auditing of information systems;
4. proof of experience and expertise in the field of external IT auditing of information systems;
5. a certificate of good standing issued by the National Trade Register Office, with the up-to-date status of the legal entity, in original copy;
6. the valid criminal record certificate and fiscal record certificate – in original copies;
7. the external IT auditor's professional liability insurance contract, for the minimum insured amount of EUR 100,000 valid on the date of submission of the documentation, in copy;
8. the copy of the payment document of the registration fee in ASF's Public Registry.

Art. 40. - Registering the external IT auditor in ASF's List of external IT auditors or the reasoned refusal of registration, shall be carried out no later than 30 calendar days after receipt of the applicant's complete file.

Art. 41 - Any modification to the documentation referred to in art. 39 letter b) points 1, 3, 5, 6 and 7 shall be notified to ASF no later than 30 calendar days from the date of the modification.

Art. 42 - ASF shall deregister from the list provided for in art. 38 the external IT auditors in any of the following cases:
a) upon their request;
b) in the case of liquidation or initiation or insolvency;
c) in the case of breach of provisions of Art. 25, 26, 28 and 41;
d) in the case of breach of the provisions of this rule.
Art. 43. - For all situations referred to in Art. 42 letters c) and e), ASF shall send the external IT auditor a prior notice informing the latter of the facts leading to his deregistration by ASF from the List of external IT auditors.

CHAPTER VI

Requirements for External Providers and Outsourced IT Service Providers for Major Information Systems

Art. 44 - Any outsourcing is carried out in compliance with the laws applicable to the relevant entity.
Art. 45. - Where there are no other legal provisions applicable to the entity regarding the outsourcing of IT services, and in all cases where the services of external providers are used, for all the major information systems, the entity is required to notify ASF on the external provider or the outsourced IT service provider within 14 days after the conclusion of the agreement with the latter.
Art. 46. – (1) The notification referred to in art. 45 shall include the following information and documents, as applicable:
a) the description of the services provided/outsourced;
b) the provider's identification data:
1. the company's office - full address
2. the telephone/fax number, email, Website;
c) a certificate of good standing issued by the National Trade Register Office, with the up-to-date status of the legal entity, or its equivalent for foreign providers registered in other states, in original or certified true copies;
d) documents according to the type of service or activity carried out, as follows:
1. SR ISO/IEC 27001 or certifications for equivalent standards – for all the providers;
2. certifications for the provision and development of computer software;
3. certifications for the provision of outsourced services;
4. proof of compliance with TIA-942 level 2 technical requirements or equivalent for the provision of hosting or outsourcing services through data centers;
5. authorization for the provision of electronic archiving services through data centers;
6. certificates specific to the outsourced activities for the provision of outsourced cloud computing public services.
(2) The certifications provided for in paragraph (1) letter d) points 1, 2, 3 and 6

must be issued by nationally and / or internationally recognized entities / bodies.

Art. 47. - The entity has the obligation, in case of modification of certain information and / or documents provided under art. 46, which may lead to impairment of outsourced services under the contract, to notify ASF and submit the original or copy of the modified documents within 90 days as of the change.

Art. 48. - For major information systems, the entity is required to ensure that outsourced IT service providers, including in the case of chain outsourcing, with the exception of communications, hardware, or software licensing providers, with strict regard to the outsourced activity :

a) allow the entity to comply with the provisions of this rule so that the outsourcing of certain activities does not violate the applicable laws;

b) submit at the request of ASF the manner in which the entity complies with the provisions of this rule;

c) allow ASF and the IT auditor to verify and / or audit its information systems in the context of the application of the provisions of this rule or provide the IT auditor an audit report prepared in accordance with ISAE 3402 or equivalent for the information systems made available to the entity.

CHAPTER VII
Reporting Requirements

Art. 49. - The entity is required to prepare in accordance with the provisions of this rule and other relevant regulations and send the following reports to ASF:

a) the annual report on the internal assessment of operational risks carried out in accordance with the provisions of Art. 6 par. (1) until March, 31st of the current year;

b) the IT audit report prepared for the audited period for the IT audit carried out in accordance with Art. 21 until June 30th, of the current year, after the last year of the audit period, accompanied by the copy of the IT auditor's certificate signed for compliance with the original, valid at the time of the audit report;

c) annual electronic reporting with the indicators listed in annex no. 4, if these indicators are applicable and relevant to major information systems, by March 31st of the current year, for the previous year.

Art. 50. - Where deficiencies / vulnerabilities are identified in accordance with the provisions of Art. 27 , the IT audit report provided for by art. 49 letter b) shall be sent to ASF together with the action plan showing how to remedy the deficiencies / vulnerabilities identified by the IT auditor.

Art. 51. - The reports referred to in art. 49 shall be sent to ASF in accordance with the reporting system communicated to them by each ASF organizational structure with supervisory responsibilities, on paper or in electronic format with extended electronic signature, as applicable.

CHAPTER VIII

Transitional and Final Provisions

Art. 52. - The non **-** observance of the provisions of this rule by the entities provided in art. 2 represents a contravention according to the provisions of Law no. 32/2000 on the activity and supervision of intermediaries in insurance and reinsurance, with the subsequent amendments and completions, Law no. 237/2015 on the authorization and supervision of insurance and reinsurance activity, as subsequently amended, Law no. 297/2004 on the capital market, with the subsequent amendments and completions, Law no. 411/2004 on privately managed pension funds, republished, with the subsequent amendments and completions, Law no. 204/2006 on voluntary pensions, with the subsequent modifications and completions, according to the type of entity, of Law no. 187/2011 on the establishment, organization and operation of the Private Pension System Rights Guarantee Fund, Law no. 213/2015 on the Policyholder Guarantee Fund and Law no. 132/2017 on the compulsory insurance against civil liability for the damage to third parties caused by vehicle and tram accidents.

Art. 53. - (1) Starting 2018, the entities have the obligation to observe the reporting deadlines provided for in art. 49 .

(2) The Romanian Motor Insurers' Bureau shall make the first reports for the year 2018 starting with 2019, within the deadlines provided for in art. 49 .

Art. 54. - (1) The provisions of this rule shall apply to entities that do not have an ongoing IT audit on the date of publication of this rule in the Official Gazette of Romania, Part I.

(2) The IT audit in progress at the date of entry into force of this rule shall continue in accordance with the regulations in force at the time of the commencement of the IT audit.

Art. 55. - Annexes no. 1 - 4 are an integral part of this rule.

Art. 56. - This rule shall be published in the Official Gazette of Romania, Part I, and shall enter into force within 30 days from the date of its publication.

Art. 57. - On the date of entry into force of this rule, the Rule of the Financial Supervision Authority no. 6/2015 on the management of operational risks arising from the information systems used by the entities regulated, authorised/licensed and/or supervised by the ASF, published in the Official Gazette of Romania, Part I, no. 227 of April 3, 2015, as amended and supplemented, shall be repealed.

Chairman of the Financial Supervisory Authority,

Leonardo Badea

Bucharest, February 28, 2018
No. 4

Annex no. 1

DEFINITIONS AND ABBREVIATIONS

1. electronic archiving - means the document storage in digital format;
2. risk analysis - means the analysis of significant threat scenarios, in order to assess the probability of materialisation thereof and the potential impact that such event would have on the entity and its operations;
3. ethical hacking/penetration test - means the assessment of the information systems by simulating actual attacks in real life conditions on networks, information systems and computer programs used by the entity assessed or audited, as appropriate;
4. IT audit - means the collection and evaluation of samples to determine whether the information system meets the performance and working parameters according to the design requirements, if it ensures the functionalities necessary for the business requirements and compliance with the laws in the field, if it is secured, if it maintains the integrity of the processed and stored data, if it allows the achievement of the entity's strategic objectives and efficient use of IT resources;
5. IT auditor - means the authorised natural person holding an IT auditor certification or the legal person with certified staff, carrying out an auditing activity of information systems, according to the regulations and best practices in the field;
6. database - means the structure of organisation of information in one or more fields of application, in order to make it accessible at all times to users via the computer programs as a whole;
7. data centre - means a secured space, equipped with computers and communications equipment by means of which data in electronic form are received, stored and sent, which shall be implemented in compliance with specific standards, using the level concept or an equivalent thereof, including, but not limited to, the standards SR EN 50600 (European Standard - means Data Centres Facilities and Infrastructures) or TIA-942 (Telecommunications Industry Association);
8. level 2 data centre - means a data centre meeting the requirements of TIA-942 tier 2 or equivalent and the infrastructure of which has 99.741% availability characteristics, a dedicated circuit for cooling and power supply, redundant components, raised floor, uninterruptible power sources, a generator and maximum 22 hours of non-functioning per year.
9. life cycle - means all stages of a life cycle of an IT service, configuration element, incident, problem or change, without limitation thereto;
10. public cloud computing - means the IT infrastructure, with configurable computing resources that allow for the provision of IT services on request and is provided through public data centres, other than the entity's own IT infrastructure, through an external provider, as a distributed package of

computing services, computer software, access to information and data storage;

11. communications/telecommunications - means transmission systems, and any other resources which permit the conveyance of signals by wire, radio, optical fibre or other electromagnetic means, and the technologies used in the communication processes, which presume the existence of an IT environment consisting of computer hardware, specialised software, and data transmission/reception electronic devices;

12. IT controls - means all the policies, procedures, practices and organisational information structures designed to provide reasonable assurance that the business objectives shall be achieved and unwanted events shall be prevented or detected and corrected;

13. (computer) data - means any representation of facts, information or concepts in a form suitable for processing in an information system, including any software program that can cause a similar function to be performed by a information system;

14. availability - means the ability of an IT service or of an IT configuration item to perform the agreed functions when necessary;

15. double validation - means the validation of an action by two users or the existence of a double information validation involving a program that verifies a specific action by different methods;

16. IT services outsourcing - means the use by an entity of an external IT services provider for the provision, on a contractual basis and on a continuing basis or for a limited period, of the operations related to the technical support or processing, required for the performance of such entity's normal course of business;

17. chain outsourcing - means the outsourcing where the external provider subcontracts with other external providers components of the services provided to the entity;

18. external provider - means the authorised natural or legal person providing goods (such as hardware, software licences, components, etc.) and IT solutions, which has expertise in specialised areas, in compliance with the applicable legal framework;

19. outsourced IT service provider - means the authorised natural or legal person with their object of activity and expertise in the field of IT services, IT service provider in compliance with the applicable legal framework and authorisation received;

20. hardware - means the collection of physical and technical elements with the help of which data may be collected, verified, processed, sent, displayed and stored, including the data storage media and auxiliary computer hardware;

21. security incident - means any event recorded and reported at the level of the entity on the information security or information systems with a high probability of compromising operations and threatening the IT security and

the consequence of which compromises or is likely to lead to compromise information or information systems;

22. key performance indicators (KPI) - means the representative analytical parameters selected for monitoring key activities and processes for entities, providing an overview of the performance;

23. key risk indicators (KRI) - means the parameters that actually measure the risks related to the entity's procedures and activities, timely providing proper alerts of the negative consequences, which may result in direct or indirect potential losses;

24. unavailability (as time duration) - means the time within the availability period of the service when an IT service or critical/significant component of the service is not available;

25. information - means the result of the processing of data through an information system representing the basis for knowledge through some new elements in relation to previous knowledge and constitutes a resource that must be protected;

26. IT infrastructure - elements of the technical and material basis, by components or as a system, supporting data collection, storage and management, and also data integration, search and viewing, and other calculations and processing services of information by using information technologies, owned or externally contracted by the entity and required for its proper operation;

27. integrity - means preserving computer data, digitized, unaltered during communication between correspondents or during the data storage period;

28. ISACA - means the Information Systems Audit and Control Association;

29. ISAE 3402 – means the audit standard used to obtain insurance reports on controls within a service organization;

30. SR ISO/IEC 27001 - means a standard that establishes the requirements for an information security management system;

31. change management - means the process responsible for checking the life cycle of all changes to allow implementation of beneficial changes with minimal disruption of IT services;

32. non-repudiation - attribute to prevent the possibility of an entity to deny an action taken in the information context;

33. Cooperation Plan in the field of information and network security - means a plan that establishes the organisational roles, obligations and responsibilities within the cooperation, and the procedures for maintaining or restoring the functioning of networks and information systems where these are affected by a cyber-risk or incident with a significant impact;

34. computer program (application) - means the set of instructions that may be executed by an information system to obtain the envisaged result;

35. information resources - means all information and documents, in accordance with the requirements laid down by the laws in the field, used only in the definition of IT audit;

36. network - means the equipment interconnected through transmission channels, including, but not limited to, computer network;

37. security risk - means any circumstance or event that has a potentially negative effect on the security of information systems;

38. systemic risk - means the risk of damage to an important area of the financial system or any financial market, which has the potential to result in serious negative consequences for the internal market and the real economy, instability of the financial system, potentially catastrophic, caused or accentuated by idiosyncratic events or conditions of entities;

39. significant risks - means the risks with serious impact on the enteritis' financial, pecuniary and/or reputational situation;

40. IT audit report - means the tool by which the purpose of the audit, targeted objectives, applied rules/standards, period, nature, scope, procedures, findings and conclusions of the audit and any reservation of the IT auditor on the audited information system are communicated;

41. IT test report - means the tool by which the purpose of the test, targeted objectives, applied rules/standards, period, nature, scope, procedures, findings and conclusions of the test, and any reservation of the testing team on the tested information system are communicated;

42. (IT) information technology risk - means the subcomponent of the operational risk which refers to the actual or future risk of negatively affecting the entities' or investors' gains and capital, on the one hand, and participants and policyholders, on the other hand, caused by the inadequacy of the IT strategy and policy, information technology and processing thereof, in terms of management capacity, integrity, controllability and continuity, or improper use of the information technology;

43. (cyber) security - means the ability of a network or an information system, resulting from the application of a set of reactive and proactive measures, to withstand, at a given level of confidence, accidental or malicious actions that compromise the availability, authenticity, integrity or confidentiality of the data stored or transmitted, or of the related services offered by the network or the information system or accessible through them;

44. (digital) electronic signature - means the indispensable attribute of the electronic document, obtained as a result of its cryptographic transformation, using the private key in accordance with Law No. 455/2001 on the electronic signature, republished;

45. IT service - means the combination of persons, processes and technologies provided within the entity or by an IT service provider, which is based on the use of information technology and providing the technical support necessary to carry out the entity's activity, and which should be defined in an SLA;

46. information system - means the group of functionally inter-connected devices for the purposes of the automated obtaining of the information necessary for the entity's operational and managerial activities, through the

IT services, hardware equipment and software products, manual procedures, databases and mathematical models for analysis, planning, control and decision-making, using components for entering and processing data, processing components such as servers, computers, basic operating software system, computer programs, computer networks and telecommunications, storage components and users, without being limitative;

47. software - means the entire program product range, consisting of at least the following elements: operating systems, drivers or computer programs;

48. (IT) information technology or information and communications technology - means the technology required for processing (obtaining, processing, storing, converting and transmitting) the information, in particular by using electronic computers and corresponding programs;

49. TIA-942 - means the standard that defines the infrastructure of a data centre, in particular in terms of cabling system and network design, but it also covers its location, cooling, power supply and equipping, and also any environmental aspects;

50. vulnerability - means the facts, processes and/or phenomena diminishing the information systems' response capacity to existing or potential risks, or favoring their occurrence and development, with an impact on functionality and utility.

Annex no. 2

Mandatory activities carried out by entities

The entities shall carry out the activities indicated in the table below, in accordance with the corresponding risk categories.

Mandatory activities of the entities, by risk categories.

	Activity	Entity's risk category			
		Major	Significant	Medium	Low
A) Internal assessment of the operational risk and risk register		x	x	x	x
B) Organisation by processes					
1	Availability Management	x	x	x	
2	User Management	x	x	x	x
3	Incident Management	x	x	x	
4 Change Management					
a)	Computer Program Life Cycle Management	x	x	x	x
b)	Version Management	x	x	x	x
c)	Test Management	x	x	x	x
5	Capacity Management	x	x	x	
6	Configuration Management	x	x		
7	Service-level Management (SLA)	x	x	x	
8 Security Management					
a)	General requirements	x	x	x	x
b)	Vulnerability scanning	x	x		
c)	Penetration Tests				
9	Continuity Management	x	x	x	
C) Control and measuring points					
1	General controls	x	x	x	
2	Computer programs controls	x	x		
3	Financial flow controls	x	x	x	x

	Activity	Entity's risk category			
		Major	Significant	Medium	Low
D) Implementation of key performance indicators (KPI)		x			
E) Implementation of key risk indicators (KRI)		x	x		
F) Information System Security Management					
1	Organisational Measures	x	x		
2	Security procedures	x	x	x	x
3	Security assessment	x			
4	Cooperation Plan	x	x	x	x

[1] For reporting, the penetration test will be performed during the audited period.

ANNEX No. 3

Reporting template

I. IT Audit Report
II. Annexes to the IT audit report:
1. Summary of observations
2. Internal Operational Risk Analysis and Risk Register
3. Requirements related to external suppliers and outsourced IT service providers for major IT systems
4. Process organization
5. Conclusions of the audit team on compliance with requirements
6. Own-account statement of the external IT auditor
7. Own-account statement of the legal representative of the IT audited entity with internal resources

I. IT Audit Report

#	Chapter	Comments / Explanations
A	Title of report	
B	Recipients of the report and any restrictions on the content and circulation of the report	
C	Introductory paragraph	Identification of the audited entity (Name / Registration number with the National Trade Register / Office Address) Inclusion of the statement that information systems were audited as a result of the legal obligation imposed by this regulation
D	Assumption of responsibility by the management of the entity regarding the audit of information systems.	
E	Responsibility of the IT auditor	The IT audit report shall at least include the following assertions : "It is the responsibility of the IT auditor to express an opinion on the compliance of the IT systems with the provisions of this rule"; - the IT audit report was prepared in accordance with the audit standard used, respectively. . . (to be mentioned)
F	Identification data of the IT audit team certified coordinator / IT auditor natural person / IT certified internal auditor	Name, surname, telephone number, fax number, e-mail address and business address
G	The signature of the IT audit team certified coordinator and the signature of the legal representative of the IT auditor legal entity / the signature of the IT auditor natural person / signature of the IT certified internal auditor	
H	The objectives of the IT audit activity, the audited period	

<table>
<tr><td>I</td><td>The office where the IT audit activity takes place, the date of preparation of the IT audit report</td><td>Address of the office where the IT audit activity (main office / branch / subsidiary) took place, the date of preparation of the IT audit report</td></tr>
<tr><td>J</td><td>Description of the IT audit scope</td><td>Identification of important information systems used by the entity and their reporting in accordance with the table below:
<table>
<tr><th>Nr.</th><th>Major information system *</th><th>Function fulfilled</th><th>Management of the major IT system (internal / external)</th><th>Included in the IT audit scope</th></tr>
<tr><td colspan="5">For the major IT systems included in the IT audit scope, the following shall be mentioned:
- description of the hardware components of the major information systems used;
- organizational measures: applicable policies and procedures implemented;
- a summary containing the analysis of the risks related to the activity, the possible deficiencies of the major audited information system and the associated risk mitigation measures based on the general or specific controls implemented according to the provisions of this rule</td></tr>
</table></td></tr>
<tr><td>K</td><td>References to the implementation of the entity's action plan resulting from the previous IT audit activity, if any</td><td rowspan="2">Verification of the implementation method of the measures, and observance of the assumed deadlines.</td></tr>
<tr><td>IT</td><td>References concerning the veracity of indicators reported in accordance with the provisions of art. 49 par. (1) of this rule, relating to the period between two IT audits and the compliance of reporting made to ASF</td></tr>
<tr><td>M</td><td>References on how the entity performs the annual assessment of operational risks arising from the use of important information systems as provided in Art. 6 par. (1) of this Rule</td><td>Opinion on the plausibility of the methodology/techniques used and on the control measures implemented to address identified operational risks</td></tr>
<tr><td>N</td><td>The result obtained after the penetration test, as applicable</td><td>When the IT auditor performs the penetration test, the following should be mentioned:
- description of the methodology / techniques used;
- mentioning the results of the test;
- the recommendations addressed to the entity and the entity's management response.
In the case where the penetration test was not performed by the IT auditor, the latter will check:
- the methodology / techniques used;
- the results obtained from the test,
- the recommendations addressed to the entity and the entity's management response.</td></tr>
<tr><td>A</td><td>The affirmation of compliance, reflected in the opinion of the IT auditor</td><td>Positive opinion, qualified opinion, negative opinion, as the case may be</td></tr>
</table>

II. Annexes to the IT audit report

1. Summary of the observations

The annex is assumed by the audited entity when signed by the legal representative and includes, without limitation to:

a) description of nonconformity / finding

b) the importance of nonconformity / finding;

c) associated risks;

d) the likelihood that these findings will have a significant impact; the IT auditor's recommendations for corrective actions and the management response of the audited entity for each finding in the report (including after the penetration test);

e) the action plan assumed by the audited entity containing the actual measures, the implementation deadline and the persons responsible for the implementation.

2. Internal Operational Risk Analysis and Risk Register

The annex contains the following information, but is not limited to:

a) the description of the policy / methodology used by the entity;

b) the results of the review of risks arising from the use of IT systems;

c) the results of the IT auditor's assessment of the control measures implemented to address identified operational risks (for significant risks).

3. Requirements related to external suppliers and outsourced IT service providers for major IT systems

Reporting is done by filling in the table below

Major information system	Function of the major information system - description of the services provided	Supplier - identification data (name, company office, fiscal registration data, telephone / fax / website)	SR ISO / IEC 27001 or equivalent (issuer, certification number, date of issue, period of validity)	Other certifications in accordance with the provisions of this rule (issuer, certification number, date of issue, period of validity)	Conclusion - Compliance Yes / No / Partial	Comments

4. Organization by processes

The appendix contains information on availability management, namely:

a) measuring the availability of important information systems (complying with TIA-942 Tier 2 requirements);

b) major information systems for which measurements have been made regarding their availability;

c) a description of how the availability of major information systems has been measured.

Reporting is done by filling in the table below

Major information system	The availability of the major information system in the measured period	Period under test	Conclusion - Compliance Yes / No	Comments

5. Conclusions of the audit team on compliance with requirements

No.	Item under review	Compliance YES / NO / PARTIAL / NOT APPLICABLE	Comments / Motivations in the event of non-compliance
1.	Article 3 (3)		
2.	Article 6 (1)		
3.	Article 6 (2)		
4.	Article 15 (1)		
5.	Article 15 (2)		
6.	Article 15 (3)		
7.	Article 15 (4)		
8.	Article 16 (1) - (a)		
9.	Article 16 (1) - (b)		
10.	Article 16 (1) - (c)		
11.	Article 16 (1) - (d)		
12.	Article 16 (1) - (e)		
13.	Article 16 (1) - (f)		
14.	Article 16 (1) - (g)		
15.	Article 16 (1) - (h)		
16.	Article 16 (2)		
17.	Article 17 (1)		
18.	Article 17 (2)		
19.	Article 18 (1) - (a)		
20.	Article 18 (1) - (b)		
21.	Article 18 (1) - (c)		
22.	Article 18 (1) - (d)		
23.	Article 18 (1) - (e)		
24.	Article 19 - (a)		
25.	Article 19 - (b)		
26.	Art. 19 - c)		

27.	Article 19 - (d)		
28.	Article 20 - a)		
29.	Article 20 - b)		
30.	Article 20 - c)		
31.	Article 20 - d)		
32.	Article 35 (1) - (a)		
33.	Article 35 (1) - (b)		
34.	Article 35 (1) - (c)		
35.	Article 35 (2)		
36.	Article 36 (1)		
37.	Article 36 (2) - (a)		
38.	Article 36 (2) - (b)		
39.	Article 36 (2) - (c)		
40.	Article 36 (2) - (d)		
41.	Article 36 (2) - (e)		
42.	Article 36 (2) - (f)		
43.	Article 36 (2) - (g)		
44.	Article 36 (2) - (h)		
45.	Article 36 (2) - (i)		
46.	Article 37		
47.	Article 45		
48.	Article 46 (1) - (a)		
49.	Article 46 (1) - (b)		
50.	Article 46 (1) - (c)		
51.	Article 46 (1) - (d)		
52.	Article 46 (2)		
53.	Article 47		
54.	Article 48 - a)		
55.	Article 48 - b)		
56.	Article 48 - c)		

6. Own-account statement of the external IT auditor

The annex contains information according to which the external IT auditor is not related to the audited entity, members of the management structure or its employees, that could affect the independence or objectivity of the IT audit activity.

7. Own-account statement of the legal representative of the IT audited entity

with internal resources

The annex contains information on the performance of the IT audit with certified internal resources that are independent of the audited activity and a copy of the certified IT auditor certificate, signed for compliance with the original.

Annual Electronic Reporting Indicators

To report indicators in the table below, entities will report:

a) in accordance with the provisions of Art. 49 letter c) of this rule;

b) 0 “zero” - if there are no values of the relevant indicator for the period being reported or, where appropriate, at the end of the reporting period;

c) the value of the indicator - if the indicator’s values are other than zero for the period being reported or, where appropriate, at the end of the reporting period.

Indicators to be reported:

Objective during the reporting period	Indicator
1	2
Indicators relating to accessing online the services provided by the entity	
	Number of clients (total users) accessing the online services offered by the entity
Indicators relating to persons who may make modifications to the major information systems/computer programs	
	Number of persons (total users) who have direct access to the entity’s databases (referring to portfolios, transactions and assets) with rights to modify the same, administrator role or equivalent privileges
	Number of persons (total users) who have the rights to modify the entity’s major computer programs (internal/external/online computer programs accessed via the Internet)
Indicators relating to the double validation principle through operations in major information systems	
	Number of operations INITIATED requiring double validation
	Number of operations CONFIRMED requiring double validation
	Number of operations CANCELLED requiring double validation
Indicators relating to the access to major information systems	
	Number of persons (total users) who have access to major information systems which contain information relating to portfolios, transactions and assets
	Number of system administrators (total users) who have access to

	the credentials of the clients' access accounts
Indicators relating to the internal information security incidents, reported	
	Total number of internal information security incidents
	Total number of external information incidents
	Number of breaches of security policies and procedures
	Number of data losses due to actions not approved
	Number of reported incidents related to data loss (electronic data)
	Number of reported incidents resulting in accidental or deliberate destruction of documents/records/ folders
	Number of reported incidents of serious breach of rules/frauds/ deceptions
	Number of reported incidents of destruction in the data centre
	Average number of days between the identification of a security incident and its resolution
Agreed service-levels, internally and for clients	
	Number of hours of unscheduled downtime of major information systems to which clients have access (including, but not limited to, online trading applications, online applications for subscription of insurance policies)
	Number of hours of unscheduled downtime of outsourced IT services that affect the services provided to entities' clients
Change management	
	Number of major computer programs
	Number of changes to major computer programs
	Number of operational errors caused by deficiencies in the design of major information systems
	Number of unidentified operational errors in testing major information systems
Continuity management indicators	
	Number of tests conducted in accordance with the business continuity plan
	Number of tests conducted in accordance with the disaster recovery plan
Audits and tests	
	Number of annual internal audits