BANKING AGENCY OF REPUBLIKA SRPSKA

INSTRUCTION

FOR AUDITING INFORMATION SYSTEM IN BANKS BY AN EXTERNAL AUDITOR

Banja Luka, November 2019

Content

Introduction

Instruction for auditing information system in banks by an external auditor shall be issued pursuant to Article 22, Paragraph 1, Item f of the Law on the Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska" No. 59/13 and 4/17), and Article 6, Paragraph 1, Item b and Article 22, Paragraph 4, Item m of the Statute of the Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska" No. 63/17).

1. Subject

1) The Instruction for auditing the information system in banks by an external auditor (hereinafter: the Instruction) provides detailed guidelines, as well as the expectations of the Banking Agency of Republika Srpska (hereinafter: the Agency) related to performing the external audit of information systems in banks, in accordance with the obligations arising from the Banking law of Republika Srpska (hereinafter: the Law), the Decision on information system management in banks, the Decision on outsourcing management, the Decision on performing external audit in banks, the Decision on licensing conditions and procedure, approvals and consents to banks operating in Republika Srpska, and in accordance with good practices.

2) In accordance with the laws and bylaws referred to in Paragraph 1 of this Article, the auditing company (hereinafter: the external auditor) is obliged to prepare a report on the audit of the information system for the needs of the Agency, which, inter alia, should contain information on the performed audit of the information system, assessment of the condition and adequacy of the management of that system, and should provide the bank and the Agency with quality and complete information on the risks to which that information system is exposed.

3) The Instruction refers to banks and external auditors, which perform audit of the information systems in banks, and aim to improve the quality of information systems audit, and better understand the roles and responsibilities of the bank and the external auditor in this process.

4) The Agency expects that the performance of the audit, as well as the report on the performed audit shall be in accordance with the following in this document, whereby this document cannot be considered as a methodology for performing the audit of information systems. In the procedure of giving consent for performing the external audit of the information system, the Agency shall assess the quality of work and actions of the external auditor, as well as the compliance of previous audit reports with the requirements from this document.

2. Appointment of an external auditor

1) The method of selecting the external auditor for the purpose of auditing the information system is determined by the Decision on information system management in banks, the Decision on performing the external audit in banks and the Decision on licensing conditions and procedure, approvals and consents to banks operating in Republika Srpska.

2) Conditions and criteria that must be met by the external auditor in order to audit the bank's information system are defined by the Decision on licensing conditions and procedure, approvals and consents to banks operating in Republika Srpska and the Decision on information system management in banks.

3) When performing the external audit of the information system, the bank and the external auditor are expected to apply the standards set by the provisions of the Law on accounting and auditing of Republika

Srpska, to the extent applicable (contract, contractual relation, assignment, signing of reports, time period of engagement, number of employees, working documentation, data confidentiality, conflict of interest, etc.).

4) The general assembly of the bank, with the prior consent of the Agency, no later than September 30 of the current year, shall appoint the external auditor who will audit the information system for that year. If there is a change in the data on the basis of which the external auditor obtained the consent of the Agency, he/she is obliged to immediately notify the Agency of the change.

5) The external auditor is obliged to submit to the Agency for each bank with which he/she has concluded an information system audit contract, an audit plan for that business year, at least 30 days before the audit, from which the areas subject to audit are indicated, as well as the names of the persons who will perform the audit and their engagement, and the duration of the audit.

6) The report on the performed audit of the information system as of December 31 of the previous year is a special report, which the bank is obliged to submit to the Agency no later than May 31 of the current year. The bank is obliged to submit to the Agency an original copy of the report in one of the languages in official use in Republika Srpska and in electronic form.

7) When performing the audit of the information system, the external auditor should apply international auditing standards, the Code of professional ethics of auditors and the rules of the auditing profession, as well as other rules and regulations governing this area.

3. Competences of persons performing audit

1) Persons who operationally perform information system audit must have the appropriate knowledge, skills and experience necessary to perform audit tasks, which are acquired through continuous education (e.g. formal education, and professional development and certification in areas related to information system audit and information systems), and appropriate work experience, in order to ensure quality and professional audit of the information system. The key members of the team that will perform the operational part of the audit should have at least two years of work experience in tasks of auditing information systems in banks.

2) In his/her work, the external auditor should apply standards for auditing information systems, then other appropriate professional or industry standards, as well as regulatory requirements, which would provide the ability to assess the condition of the information system and the adequacy of information system management.

3) If the external auditor does not have employees who have the appropriate knowledge and skills necessary to perform the audit of the information system, the external auditor may hire third parties, who have adequate professional qualifications (e.g. internationally recognized certificates for auditing the information system). The responsibility of the external auditor towards the bank and the Agency cannot be transferred to the persons hired by the external auditor.

4) The external auditor and the engaged third parties should be independent, which means that during the engagement by the bank they cannot have:

1. any direct or indirect financial interest in the bank or in any related person to the bank and

2. any other relation that may compromise his/her independent assessment, i.e. consulting services, audit of his/her own work (e.g. internal audit), audit of work for which they were previously responsible, etc.

4. Responsibility of an external auditor and a bank

1) In the process of performing the audit of the information system, the bank should acquaint the external auditor with all the systems and applications it uses in its activities. The bank is also responsible for submitting complete documentation related to its information system, information and documentation required by the external auditor, which relates to the bank's information system, as well as for authorized bank staff to provide the external auditor with access to information system resources.

2) The external auditor is responsible, based on the performed audit process and collected audit evidence, to provide a report containing an objective and realistic opinion, as well as an assessment of the condition of the information system and the adequacy of information system management.

3) If the external auditor during the engagement notices deficiencies, weaknesses or irregularities that pose a very high risk and which are at the same time critical for the security of the bank's information system, he/she is obliged to immediately notify the Agency.

5. Contractual relation between a bank and an external auditor

1) The contract between the bank and the external auditor should clearly define all relevant conditions, rights and obligations, and responsibilities of the contracting parties, and should at least contain the following provisions:

1. detailed description of services that are the subject of the contract,

2. areas to be covered by the audit,

3. if the external auditor hires a subcontractor, it is necessary to provide information on the subcontractor and/or individuals who participate in the performance of the operational part of the audit,

4. methodologies and procedures to be used by the external auditor,

5. responsibility of the bank and the external auditor,

6. limitation of liability and compensation for damages and

7. obligation to protect banking and business secrets.

6. Exchange of information between an external auditor and the Agency

1) The exchange of information and data between the Agency and the external auditor shall be performed in writing, by holding meetings or, if necessary, in another manner agreed between the Agency and the external auditor.

2) The exchange of information and data is usually performed during the preparation and planning of the audit, during the audit and after signing the report on the audit, and in cases where the Agency needs additional information and data for the purposes of bank supervision.

3) Auditors are obliged to improve their reports in accordance with the Agency's recommendations, and review specific areas of the information system, if the Agency has assessed them as critical or of special importance.

7. Information system audit

1) When performing the audit of the information system, the external auditor shall provide an assessment of the condition and adequacy of the information system management, where he/she is obliged to:

1. use methods and procedures for audit of information systems based on risk assessment,

2. define the scope and plan of the audit, based on the risk assessment, before the start of the audit of the information system,

3. define the depth of the audit, depending on the current condition of the information system,

4. review and assess the condition of the information system and

5. check whether the bank complies with the applicable laws and bylaws, which relate to information systems.

2) Based on the audit of the information system, the external auditor is obliged to point out the significant risks to which the bank is exposed.

8. Information system audit planning

1) In order to efficiently perform the audit of the bank's information system, it is necessary for the external auditor to perform audit planning, taking into account at least the following:

1. the size of the bank (market and financial position, etc.),

2. risk profile of the bank, and risk appetite,

3. scope and complexity of business processes,

4. organization of the bank (number of employees, organizational structure, number of organizational units, etc.),

5. characteristics of the information system (organizational and technological complexity, heterogeneity of software and hardware resources, scope and complexity of the network infrastructure, etc.),

6. level of outsourced activities related to the bank's information system (number of service providers and level of significance of services they perform, dependence on service providers, etc.),

7. reports of control functions from the aspect of information system, committee for information system management, persons in charge of the information system security and head of organizational unit for information technology,

8. reports on previously performed audits of the information system by external auditors,

9. current trends related to technological progress (e.g. cyber threats, etc.) and

10. compliance with regulatory requirements.

2) The scope of the information system audit should be defined on the basis of the conducted risk assessment. It is necessary to rank the areas according to the criterion of their risk, and accordingly pay attention to those parts and resources of the information system that are necessary for the functioning of critical/key business processes of the bank.

3) The scope of the audit may change during the audit in accordance with new knowledge about risks or other facts relevant to the subject of the audit.

9. Information system audit performance

1) During the audit of the information system, the external auditor should at least:

1. determine the adequacy of the information system management process,

2. review the work and activities of control functions (especially internal audit of the information system, the person responsible for the security of the information system, the committee for the management of the information system, etc.),

3. assess the operational efficiency of the process and the established system of internal controls and

4. check the status of the findings of previously performed audits by external auditors.

2) The external auditor should verify that the processes related to information systems (incident and user requirement management, information system documentation management, development and change management, access control management, malicious code protection management, backup data management, cyber security, etc.) are adequately established, which includes checking the level of documentation of these processes by internal acts.

3) It is necessary to emphasize that the existence of internal acts, as well as their adequacy, does not mean that the processes that regulate them are adequately established. Therefore, the external auditor should check the level of implementation of these processes in practice, and their operational efficiency, and provide an objective and realistic assessment (opinion) about them.

10. Assessment of information system condition

1) In order to form an objective and realistic assessment (opinion) on the condition of the information system and the adequacy of its management, the external auditor should analyze the architecture of the information system, technological characteristics and configuration of significant information system resources.

2) Previously stated in Paragraph 1 of this Article includes analysis of network infrastructure design, technological characteristics and configurations of network components, architecture and configuration of servers, databases, analysis of backup systems, etc. In accordance with the above, the external auditor should identify those information system resources that are important for the performance of critical/key processes of the bank, as well as those resources that are important from the aspect of information system security.

11. Use of audit tools

1) When performing an audit of the information system, the external auditor may use appropriate audit tools in order to check the effectiveness of controls built into the information system, assess the quality of data and similar.

2) The use of audit tools, as well as the scope and method of their application, should be agreed in advance with the bank (before concluding a contractual relation on the audit of the information system), given the possible negative consequences of the application of these tools.

12. Report on performed information system audit

1) The external auditor should prepare a report upon completion of the audit, which should be comprehensive, objective, fact-based, precise and clear.

2) The report should indicate the name of the bank and the recipients, scope, objectives, period of audit coverage, and the nature and period of the audit. The report should include findings, risks and recommendations, and if there is a reluctance on the part of the external auditor, the qualifications or limitations to the extent observed by the external auditor during the audit should be stated.

3) The external auditor must state in the report on the performed audit of the information system the names of the persons who have operatively conducted the audit of the information system of the bank, and their overall engagement in these tasks.

4) The report should contain at least the following:

1. report summary

2. defining the scope of reports and methodologies

    - audit methodology(s) (for risk assessment and information system audit)

    - initial risk assessment to determine the scope of the audit

    - areas of the information system that have been subject to control testing

    - review of the previous report on the audit of the information system (status of recommendations)

3. risk assessment results

    - overview of the bank's information system (system architecture)

    - applied risk assessment procedures

    - key components of the information system included in the scope of the audit

4. findings on controls in the information system

    - area of information system

    - observations and risks

    - risk assessment

- recommendations

- recommended deadlines for implementation of recommendations

5. compliance of the bank's operations with individual articles of the Decision on information system management in banks and the Decision on outsourcing management; and

6. assessments of the level of maturity by areas of the information system.

5) In the summary of the report on the conducted audit of the information system, the most significant findings with the corresponding risk levels and the overall assessment of the condition and adequacy of the information system management should be singled out.

13. Findings, risks and recommendations

1) The report on the performed audit of the information system should clearly state the findings, risks and recommendations for each area or part of the information system that was the subject of the audit.

2) The auditor's finding is a written explanation of irregularities, weaknesses, deficiencies, mistakes or needs for improvements and changes identified during the audit. The finding is a constructive critical comment on a particular action or unprocessed activity, which in the opinion of the external auditor is an obstacle in achieving the desired objectives in an efficient and effective manner.

3) The findings stated by the external auditor in the report should meet the following:

1. problems and shortcomings determined during the audit of the information system are clearly and precisely identified,

2. contain information to which part of the information system they refer (software, hardware, business process, etc.),

3. contain the name of the standard or good practice, specific policy, procedure or regulation to which the finding relates,

4. are based on the factual situation established during the audit of the information system,

5. are reasoned in an objective manner and fully supported by audit evidence and

6. are precise, sufficiently understandable and convincing.

4) The external auditor should, wherever possible, consider the cumulative impact of weaknesses or absences of controls relating to the same business processes or resources that affect the overall level of risk of the information system. Such findings should be interlinked and grouped, and the overall risk arising from them should be stated.

5) If the external auditor determines that there are no deficiencies for a certain area of audit or that identified deficiencies are of such importance that they should not be stated in the report, the information that no significant deficiencies have been identified should be stated in the report. Such findings should be adequately supported by audit evidence, just as in the case of identifying weaknesses. In situations where the external auditor has not gathered sufficient evidence to examine and evaluate a particular area of the information system, the external auditor should state that fact.

6) If there are relevant reports for specific areas of the information system (e.g. penetration tests, audit report of the service provider, etc.), the external auditor may take them into account when assessing these areas.

7) The external auditor should identify and state the risks arising from the identified findings and explain them in such a manner that the bank can adequately assess the possible impact of the identified deficiencies on the bank's operations.

8) The external auditor should state the causes of the existing situation, in order to sufficiently clarify the identified shortcomings. The description and level of risks to which the information system is exposed should clearly indicate possible negative consequences for the information system and the bank's operations.

9) Consequences most often reflect potential financial loss, non-compliance, disruption of business continuity, endangered security, etc. The external auditor should explain the meaning of the level of risk used in the report.

10) The recommendations should state the expert opinion of the external auditor on the activities that the bank should carry out in order to mitigate the risks arising from the identified deficiencies (findings). The basic guidelines for writing recommendations are as follows:

1. the recommendation is professional and constructive, and aimed at mitigating risks,

2. represents a logical sequence of what is presented in the finding, and does not introduce new information that is not presented within the stated factual situation,

3. does not contain a description of activities already undertaken,

4. does not indicate specific organizational and/or technological solutions and

5. an adequate deadline for the implementation of the recommendation is proposed.

11) If the proposed activities for the implementation of recommendations have already been discussed with the bank's management, the external auditor should include the management's response and explanations in the report on the performed audit of the information system.

12) The external auditor is obliged to make a report on the performed audit for the needs of the Agency, which includes an overall assessment of the condition of the information system and the adequacy of information system management, and to indicate significant risks to which the bank is exposed. The overall assessment is given in the summary of the report.

13) The assessment referred to in Paragraph 1 of this Article is descriptive and may have one of the following values:

1. completely satisfactory,

2. satisfactory,

3. unsatisfactory and

4. completely unsatisfactory.

14) When giving an assessment, the external auditor is obliged to take into account the compliance of the bank's operations with the Banking Law, bylaws related to the information system (the Decision on information system management in banks and the Decision on outsourcing management), as well as other relevant legal regulations (e.g. the Law on personal data protection, etc.). When explaining the assessment, the external auditor is obliged to state the facts that most influenced the assessment of the condition of the information system and the adequacy of the information system management.

15) For each area of the information system that has been audited, the external auditor should provide an individual descriptive assessment in accordance with the methodology used (e.g. assessment of the level of maturity according to the *COBIT* methodology).

16) The Agency may request additional information from the external auditor in connection with the performed audit.

14. Reasons for rejecting data and information from the audit report

1) The Agency may reject the report on the performed audit of the information system if it finds that the external auditor in the report on the audit of the information system did not submit data and information and did not give an assessment for the needs of the Agency in accordance with the Banking Law, the Law on accounting and auditing, regulations adopted based on these laws and rules of the profession or if by performing supervision over the bank or in any other manner it is determined that the data are not based on true and objective facts. In this case, the Agency may require:

1. from the external auditor to supplement or amend the data or

2. from the bank to appoint another external auditor or for the Agency to directly appoint an external auditor at the expense of the bank who will perform the audit of the information system.

15. Bank role

1) The competent bodies of the bank should review the report on the performed audit of the information system and state their opinion on the identified findings. In doing so, they can comment on the recommendations and risks identified by the external auditor.

2) The bank should, based on the findings stated in the report on the audit of the information system, assess how these risks fit into its risk profile and determine how to mitigate these risks.

3) If the bank assesses that it can mitigate the stated risks by carrying out further activities, it is necessary to determine which activities (measures) are to be carried out, and to define deadlines and persons responsible for carrying out these activities.

16. Transitional and final provisions

This Instruction shall enter into force on the eighth day from the day of its publication in the "Official Gazette of Republika Srpska".

Number: D-14/19

Director

Date: 15 November, 2019

_____

Rade Rastoka