Syrian Arab Republic
The Monetary and Credit Council

The Monetary and Credit Council Decision (115/M.C.C)

Date: 23 May 2022

The Monetary and Credit Council, pursuant to the provisions of the Central Bank of Syria Law and Basic Monetary System No. 23 of 2002 and its amendments, as well as the letter of the Banking Supervision Department No. 1268/16 dated 10 March 2022, and its memorandum concluded following its session held on 19 May 2022, hereby **decides the following:**

First: Approval of the Standard Framework for External Information Systems Audit Tasks at the Banks and financial Institutions operating in the Syrian Arab Republic:

Article 1: Definitions:

- **An Institution:** A Financial banking institution.
- **External Information Systems Auditor:** A Legal person or a Syrian company registered in the Companies Register at the Ministry of Internal Trade and Consumer Protection, in accordance with the applicable laws and regulations, and accredited by the National Network Services Authority to provide information security services.
- **Sensitive Data:** All data and information related to systems and technologies invested in institutions, as well as all customer data, including electronic details and storage media.
- **Information Systems Audit:** Review and evaluation of administrative, legal, investment, and operational controls of information technology systems and structures invested in an institution, all executed operations, and all policies and procedures related to them. The opinion and results are based on an analysis of associated risks according to the relevant standards and guidelines approved by The Monetary and Credit Council and the Central Bank of Syria, assessing the institution's achievement of the objectives specified in item **3.2** of this decision.

Article 2: An institution is obliged to make a contract with an external auditor to audit information systems for the following purposes:

2.1. Ensuring the confidentiality, security, and protection of sensitive information and data from unauthorized disclosure due to internal and external factors.
2.2. Verifying the accuracy, adequacy, efficiency, effectiveness, reliability, and credibility of data for decision-making.
2.3. Ensuring the availability, integrity, and comprehensiveness of information upon request, protecting associated resources, and ensuring continuity of work and recovery when necessary.
2.4. Verifying the reliability, independence, and ability of technical structures and information systems to execute all types of investment functions under various

operational conditions, as well as the sufficiency of their continuity requirements and independence.

2.5. Evaluating compliance with the controls, regulations, circulars, and legal and regulatory obligations approved by The Monetary and Credit Council and the Central Bank of Syria, as well as national and international standards.

Article 3: Regulatory and Administrative Procedures for Information Systems Audit:

3.1. The external information systems auditor must have practical experience in the field of auditing, work with a specialized team, have previous experience, and maintain a good reputation in this field. Additionally, they must have a permanent address in Syria, considering the institution's approved contracting principles.

3.2. Syrian law shall govern the relationship between the institution and the external auditor.

3.3. The company must hold valid accreditation from the National Network Services Authority for information security services, following the applicable guidelines.

3.4. The external information systems auditor shall sign a non-disclosure agreement and maintain confidentiality, documented with reference numbers and dates, before initiating any discussions or negotiations regarding the task with the institution.

3.5. The external information systems auditor shall provide the institution with the following information (*at a minimum*):

3.5.1. A copy of the organizational structure of the auditor, including job titles.

3.5.2. Identification of all parties involved in implementing the information systems audit task, their activities, results, and reports.

3.5.3. Identification of the control mechanism for obtaining, preserving, and disclosing data and information.

3.5.4. Proof of experience with duly authenticated supporting documents.

3.6. All documents and correspondence related to the external information systems auditor that occurred before signing the contract shall be documented at the beginning of that contract, with reference numbers and dates.

3.7. Evaluation of the competence of the external auditor and their selection shall be based on the minimum following criteria:

3.7.1. The competence of the staff, from the practical, professional, and the specialized scientific aspects, in addition to relevant experiences and skills.

3.7.2. The adequacy of the staff for completing the task in proportion to the necessary workload for information systems audit.

3.7.3. The existence of a methodology and a standardized guide[1], that includes audit mechanisms and techniques, quality assessment procedures and policies, a

[1] It is preferable to utilize the methodologies based on a standardized framework such as COBIT2019, CISA, or other relevant standards issued by the ***Information Systems Audit and Control Association (ISACA)***.

rotation policy for external information systems auditor staff, requirements of independence, objectivity, and adherence to professional conduct standards.

3.7.4. Achieving Independence criteria and the following Professional Conduct Standards:

3.7.4.1. An external information systems auditor must not be a member of the institution's board of directors, nor should there be any family relationship up to the third degree between any of the external information systems audit team members and any head of any management within the institution or any members of the institution's board of directors.

3.7.4.2. None of the external information systems audit team members may work permanently in any technical, administrative, or consulting capacity for the institution.

3.7.4.3. An external information systems auditor may not perform more than two consecutive information systems audit tasks for the same banking institution.

3.7.4.4. An external information systems auditor, members of an auditing staff, and their immediate family members (spouses and children) are prohibited from directly or indirectly benefiting from credit facilities granted by an institution they are serving, during the audit period and for two subsequent years after the services are terminated. These provisions also apply to their guarantees for others based on facilities granted by the institution. However, they may benefit from credit facilities for personal (consumption) purposes without any discriminatory treatment, provided they obtain prior approval from the institution's audit committee.

3.7.4.5. An external information systems auditor and their team members may not be partners with any of the institution's managers, members of the board of directors, or an agent thereof.

3.7.4.6. An external information systems auditor and their team members may not collectively own an influential share exceeding 5% of the institution's shares.

3.7.4.7. An external information systems auditor and their team members may not hold a consultancy relationship regarding the scope of the task with the institution, its executive departments, or any members of its board of directors.

3.7.4.8. An external auditor may not receive any additional financial compensation beyond what is stipulated in the contract regarding the assigned task.

3.7.4.9. None of the external information systems audit team members may combine audit work with any additional services[2] provided to the institution beyond the scope of the assigned audit task.

[2] This applies on the works that are beyond the scope of the auditing task, that is defined by this resolution.

3.7.5. Providing the external information systems auditor with policies and procedures that shows the minimum requirements regarding the competencies of their staff, provided that they meet the following conditions:

3.7.5.1. An external information systems auditor must have good character, behavior, and a positive professional reputation.

3.7.5.2. They must not have been convicted of a felony or misdemeanor related to honor or integrity.

3.7.5.3. They should hold an academically recognized degree of no less than a university bachelor's degree in communications or information technology. Preference will be given to those with a professional certification in information systems audit from one of the internationally recognized bodies.

3.7.5.4. They must have scientific experience in information systems audit for a minimum of two years.

3.7.5.5. They should possess sufficient knowledge of banking information systems, services, technologies, and risks (both conventional and Islamic), as well as relevant laws and regulations.

3.7.5.6. They should be familiar with international information systems audit standards, in addition to professional codes of conduct and their updates.

3.7.5.7. They must not be disqualified from practicing their profession or have received a definitive criminal judgment due to a professional misconduct or a legal violation related to their profession.

3.7.6. Setting a policy for providing continuous training for the team of the external information systems auditor.

3.7.7. Ensuring the availability, adequacy, and competence of the tools and equipment necessary to carry out the activities of the task.

3.7.8. The ability to prepare task outputs and present them in Arabic (without translation).

3.7.9. A financial institution must inform the Banking Supervision Department (Information Systems Audit Division) of the name of the approved external information systems auditor within a maximum of one week from the date of signing the contract with them. This should be done through a written letter that includes detailed information about the external auditor and their team. The contract should be written in Arabic.

3.7.10. A financial banking institution may contract with an external information systems auditor with whom they have previously contracted for the same purpose, taking into account the provisions related to the rotation policy for auditors, independence, and professional conduct standards in this decision.

3.7.11. The institution's board of directors and audit committee must verify that the external information systems auditor complies with the standards specified in this

decision before contracting with them. They should ensure that nothing affects the quality and performance of the audit.

3.7.12. An institution's board of directors or audit committee must monitor the work of the external information systems auditor during task execution to ensure at least the following:

3.7.12.1. The effectiveness of audit activities throughout all stages of the task, which shall be done by means of evaluating the suitability and adequacy of audit methods, the level of importance, risks, and activities that may potentially impact all of the information systems and technical infrastructure invested in by the concerned institution.

3.7.12.2. The independence and objectivity of the external information systems auditor, as well as their adherence to the professional conduct standards and codes of conduct.

3.7.12.3. An external information systems auditor's commitment to the scope of the task and the work plan, in addition to scrutinizing the reasons leading to any changes or deviations.

3.7.12.4. Seeking input from relevant institution employees regarding the external information systems auditor's performance.

Article 4:

4.1. The scope of the task of external information system auditing and the required reports:

4.1.1. The task must be comprehensive in a way that covers all pieces of infrastructure and information technology systems invested in by the concerned institution. The minimum scope of this task shall include:

4.1.1.1. The basic system of the bank, its banking services systems, and all of the relevant ancillaries connected to it, whether technically or functionally.

4.1.1.2. Administrative, financial, security, and any other systems that are supplementary or connected to it, whether technically or functionally.

4.1.1.3. Infrastructure, communications, main and back-up data centers, continuity plans, disaster response, and emergencies.

4.1.2. The task activities and assignments must include reviewing, auditing, and comprehensively evaluating all of the operations related to the infrastructure and information technology systems invested in by the concerned institution, in accordance with the objectives stated in /**Article 1**/ of this decision. This is linked, at the minimum, to the following:

4.1.2.1. The strategies and policies that are written and adopted at the level of the institution on the one hand, and at the level of information technology on the other.

4.1.2.2. Adopted standards, procedures, regulations, rules of working, operations, and job functions.

4.1.2.3. The mechanisms used for employing human resources working with information systems, their performances, monitoring methods, qualification, and development.

4.1.2.4. Overseeing the infrastructure and information technology systems invested in by the concerned institution.

4.1.2.5. The risks facing the infrastructure and information technology systems invested in by the concerned institution, whether internally or externally generated.

4.1.2.6. The acquisition of the infrastructure and information technology systems invested in by the concerned institution, developing them, and managing their change.

4.1.2.7. Licenses and contracts of technical support services and technological systems maintenance, whether owned by the concerned institution or operated by it.

4.1.2.8. Managing the services of the infrastructure and information technology systems invested in by the concerned institution.

4.1.2.9. Achieving the credibility of the infrastructure and information technology systems invested in by the concerned institution, their continuity and recoverability.

4.1.2.10. Cybersecurity, encryption, authorities, authorizations, and access control.

4.1.2.11. Electronic banking services and the security and protection of payments instruments and channels.

4.1.2.12. Testing the security of the technological systems and reviewing the source code, if available.

4.1.2.13. The flexibility of the storage system and its media and planning its capacity.

4.1.2.14. Protection from blocking the service and the risks posed in a similar event.

4.1.2.15. Online information systems (electronic service systems) and relevant security procedures.

4.1.2.16. The activities of raising awareness and client protection.

4.1.2.17. The regulations and procedures for protecting data centers alongside their physical and software components.

4.1.2.18. The server room and the equipment it contains (servers, computer network equipment, devices for an uninterruptible power supply (UPS), fire protection devices, surveillance cameras, etc.) and the security procedures taken to protect it.

4.1.3. The activities of the task must include comprehensive internal and external penetration tests of all infrastructure and information technology systems invested in by the concerned institution in addition to all associated electronic services, with

an audit of settings, classification of information assets, and analysis of risks according to importance and treatment priority.

4.1.4. The task activities must include reviewing, auditing, and comprehensively evaluating the results of the latest internal and/or external information systems audit report.

4.1.5. The task activities should involve risk analysis and classification based on importance using a globally standardized methodology. Optimal corrective solutions should be proposed in detail, along with the expected time required for implementation, retesting, verification, and quality assurance.

4.1.6. The task activities and assignments must include the following tools and standards, at the very least:

4.1.6.1. Syrian laws, decisions issued by the Council of Ministers, The Monetary and Credit Council, the Central Bank of Syria, and relevant circulars, considering their applicability and subsequent amendments.

4.1.6.2. The task activities should involve analyzing the current gap in scope against applicable standards, laws, and effective decisions. It should evaluate weaknesses and propose optimal corrective solutions in detail, along with the expected time required for implementation, retesting, verification, and quality assurance.

4.1.6.3. A unified and comprehensive report for the task should be submitted in Arabic (**with no translation**), categorized according to the lines of approach and items specified in item /**4.1**/ stated above. The report should thoroughly document information sources, documents, and all tools used in task execution. It should also explain all symbols, meanings, and abbreviations used in the report and accompanying documents.

4.2. Evaluation of Reports and Results Handling:

4.2.1. The institution's board of directors and/or audit committee are responsible for evaluating the performance of the contracted external information systems auditor in accordance with the standards specified in this decision.

4.2.2. The institution's board of directors and/or audit committee are responsible for monitoring the handling of outputs and results of the information systems audit task. This is done through an executive action plan that entails detailed corrective and remedial measures, classified by priority and importance, according to a specified timeline. The Banking Supervision Department should be provided with this program, along with the monitoring and follow-up results.

Article 5:

5.1. Audit Deadline: An institution commits to auditing information systems by contracting with an external information systems auditor according to the provisions of this decision (at least once every two years). However, internal and external penetration

tests mentioned in item /**4.1.3**/ are an exception, an institution must conduct these tests annually (at least once a year) for all invested systems and associated services. Additionally, these tests should be performed when launching any new electronic banking service, focusing solely on the service level.

5.2. An institution must provide the Banking Supervision Department with the information systems audit report, along with the corrective or remedial action plan and the specified timeline mentioned in item /**4.2.2**/. This must be done within no longer that one month after the task's completion.

Second: Banks and financial institutions operating in the Syrian Arab Republic are obligated to conduct their first external information systems audit task according to the referenced standard framework in the "First" section of this decision as of January 2023.

Third: The Banking Supervision Department is responsible for evaluating external information systems audit reports and preparing a comprehensive report of the results for presentation to The Monetary and Credit Council.

Fourth: This decision shall be communicated to whom it may concern for implementation.

Chairperson of The Monetary and Credit Council
Mhd.Issam Hazime