

By the Banking Regulation and Supervision Agency:

**COMMUNIQUE ON THE REPORT RELATING TO INFORMATION
SYSTEMS AND BANKING PROCESSES AUDIT TO BE PERFORMED BY
EXTERNAL AUDIT INSTITUTIONS**

(Published in the Official Gazette dated January 13, 2010, Nr. 27461)

**SECTION ONE
General Provisions**

Objective and Scope

ARTICLE 1 — (1) The purpose of this Communiqué is to lay down the principles and procedures governing the scope and form of the audit report to be prepared according to the Regulation on Bank Information Systems and Banking Processes Audit to be performed by External Audit Institutions

Basis

ARTICLE 2 — (1) This Communiqué has been prepared on the basis of Article 40(2) of the Regulation on Regulation on Bank Information Systems and Banking Processes Audit to be performed by External Audit Institutions.

Definitions and abbreviations

ARTICLE 3— (1) Following terms used in this Regulation shall have the meanings expressly designated to them below:

- a) Banking processes audit: Audit referred in article 25 of the regulation,
- b) Information systems audit: Audit referred in article 24 of the regulation,

- c) IT: Information Technologies,
- ç) COBIT: Current version of Control Objectives Information and Related Technologies (CEBIT) which was published by Information Systems Audit and Control Association (ISACA) Information Technologies Governance Institute (ITGI),
- d) Auditor: Auditor defined in article 4 of the regulation,
- e) Auditee: Auditee defined in article 4 of the regulation,
- 1) Detailed control target: Detail control targets defined in COBIT under control targets,
- g) Noteworthy lack of control: Noteworthy lack of control defined in article 6 of the regulation,
- ğ) Control: Control defined in article 4 of the regulation,
- h) Control areas: General control areas which COBIT defined as a general process model by distributing IT activities into 4 areas,
- ı) Control target: Control targets in COBIT which actualized a desired result or an objective by establishing control procedures in a specific IT activity,
- i) Control weakness: Control weakness defined in article 6 of the regulation,
- j) Board: Banking Regulation and Supervision Board,
- k) Agency: Banking Regulation and Supervision Agency,
- 1) Significant lack of control: Significant lack of defined in article 6 of the regulation,
- m) Regulation: Regulation on Bank Information Systems and Banking Processes Audit to be performed by External Audit Institutions.

Principles to be complied with while preparing the report

ARTICLE 4 —(1) The auditor pays attention to the report to be complete, accurate, objective, persuasive as well as clear and brief to the extent the subject permits.

(2) The auditor ensures that the report is complete by giving the information meeting the entire audit targets in the report; by presenting the reported subjects in a way that these subjects are understood accurately and by providing the requirements expressed in this Communiqué relating to the content of the report.

(3) The auditor that the report is complete by actual existence of the findings presented and presenting these findings properly. Accuracy and reliability of the report is provided by delivering all findings to the reader properly. Only the information, findings and judgments supported by sufficient evidence related to the subject in the working papers of the auditor is given in the report. In cases where some of data deemed significant in respect of audit is or cannot be audited, the auditor shall express this in his report, if any, includes the restrictions of data in the report and makes no judgments in the report relating to this subject.

(4) The auditor provides the report to be objective by presenting the components in the content of the report in a balanced way and by displaying an objective attitude in presentation approach. In respect of persuasiveness of the report, the evidence in the report should be presented objectively and the reader shall be persuaded with the realities. The auditor is obliged to provide the report to be objective and not misleading. The auditor presents his report in an approach which decision-makers may act according to the findings in the report. The auditor pay attention not to use a language intended to defense or accusation.

(5) The auditor provides his report to be persuasive when audit results meets audit targets, findings are presented persuasively and judgments in the report are supported by the realities finely. The auditor presents sufficient and persuasive information in his report on validity of his findings and rationality of his judgments.

(6) The auditor ensures his report to be clear by using fluent and clear expressions. A clear, simple and as non-technical as possible language is used in the report. In cases where technical terms or abbreviations are used in the report, these terms are explained additionally and information on the abbreviations used is given in a separate part of the report. Attention must be paid to using short and active verbs in the report. The auditor, when deems necessary,

benefits from visual instruments in the report such as charts, tables and pictures in order to provide the subject is better understood.

(7) The auditor expresses what he wants to express in his report as short and to the point as possible, avoids unnecessary details and repetitions which might overshadow the message he wants to give.

SECTION TWO

General Conceptions

Findings

ARTICLE 5 — (1) The auditor mentions in his report the noteworthy lack of control and significant lack of control by classifying them in a way to be supported with sufficient and appropriate audit proofs and by coding them according to the principles set forth by the Agency.

(2) The auditor gives the information on criteria and states of his findings to the extent the audit targets require.

a) Criteria: Relating to the area/activity with which the finding is related, state in which the area/activity should be or what is expected from this area/activity,

b) State: Indicates the fundamental reasons of differences between the current implementation way or state of the area/activity which the finding is related with and the criteria and this situation.

(3) Findings defined as control weakness are submitted by the auditor to the authorities of the auditee in writing. Thus, the auditor states in his report the expression that such letter has been submitted to the authorities of the auditee and the number of control weaknesses he detected in the basis of control targets in information systems audit and processes in banking processes audit.

(4) In his report, the auditor evaluates all findings which were detected in the past periods and which have not been still removed in the previous period report; mentions the final situation of these findings and whether they continue, and explanations relating to compliance with the action plan committed by the auditee.

(5) If the auditor reached the conclusion that one or more conditions existed such as forgery, illegal practices, contract violation, abuse, double record system or repeated information systems depending on the audit proofs he collected, he expresses them in the report as finding.

(6) The auditor submits all findings he gave in his report to the Agency in the way of which procedures and principles to be set forth by the Agency.

Opinions of the auditee

ARTICLE 6 — (1) The auditor reports the opinions of the auditee about the findings, results and if any, correction studies made.

(2) The auditor gives in his report opinions of the auditee about findings which were detected in the past periods and which have not been still removed in the previous period report and studies the auditee conducted relating to removing the finding.

(3) Cases where the auditee can deliver no opinion or decline to deliver opinion are given in his report along with justifications.

Outcome assessment about the findings

ARTICLE 7 — (1) The auditor makes evaluation in the report in line with his own inferences and opinions by commenting on audit objectives, audit findings and if any, opinions of the auditee. In these evaluations, he makes comments on how these findings should be understood by adding his own observations to the findings arise in the audit and by avoiding exact repetitions of the findings.

(2) In case he disagrees with the auditee's opinion or he thinks that the correction studies are not appropriate, the auditor states this separately in the final evaluation. The auditor makes the necessary corrections in the report in case he recognized the opinions of the auditee.

(3) In case where a statement reached to the auditor by the auditee before the date of report that any finding has been corrected, the auditor analyzes the final condition of this finding so as to verify the statement of the auditee, on condition that it is once for each for all detected finding, and in case he reaches the conclusion that the finding has been removed, he expresses his judgment that the finding has been corrected in the result evaluation section of the report relating to the finding

(4) In the result evaluation section on the findings expressed to be detected in the past periods and which have not been still removed in the previous period report, as well as the compliance with the action plan by the auditee relating to the solution of findings, the auditor states in his report the continuation status of the findings as:

a) Continues,

b) Partially corrected or

c) Corrected.

SECTION THREE

Report Content

Content

ARTICLE 8 — (1) Report which the auditor shall prepare is drawn up in a way to contain the elements:

- a) Title,
- b) Competent authority to which the report is submitted,
- c) Audit letter prepared within the scope of article 34 of the regulation,
- ç) Executive summary,
- d) Table of contents,
- e) Information on audit study,
- f) General information on information systems of the auditee,
- g) Evaluation on internal control and internal audit of the auditee,
- ğ) Banking processes audit section,
- h) Bank information systems audit section,
- ı) Abbreviations,
- i) Dictionary.

Executive summary

ARTICLE 9— (1) Executive summary is prepared as described below:

a) In this section, the auditor defines the objectives of the audit and explains in summary the scope and methodology of the audit he implemented so as to fulfill these audit objectives.

1) The auditor expresses clearly his audit objectives in a way to indicate why he took on this duty as well as the preparation target of this report.

2) The auditor expresses clearly the scope of audit study determined within the scope of materiality concept. If there is any limitation forcing the auditor to select this scope while expressing the scope of the audit, these limitations are expressed clearly.

b) A general evaluation is made relating to the audit study carried out.

c) A table in which the findings detected in current and past periods are summarized is filled out as per the sample defined in annex-1.

ç) Those stand out among the findings the auditor detected and business risks these findings bear are stated.

d) Having considered the findings arise as a result of banking processes and if any, information systems audit, a general evaluation is made on the condition of the auditee.

e) If an information system audit has been carried out during audit period, a maturity degree chart is prepared and included in this section for each of control areas in comparison with maturity degrees determined in the audit of the auditee belonging to previous year and as defined in annex-2.

Information about audit study

ARTICLE 10 — (1) Concerning the audit study concerning the audit study to be carried out to conduct audit targets, the auditor gives the following in the information section:

a) Important assumptions taken into consideration while carrying out audit study,

b) Bank units of branches in which he conducted the audit,

c) Title and access information of his responsibilities relating to the processes within the scope of audit and

d) Information on audit team and beginning/ending date of audit.

General information on information systems of the auditee

ARTICLE 11 —(1) Evaluation of information systems includes the following:

a) Information on IT department employee profile,

b) Information on organization structure of IT department,

c) General information on implementations/systems used in conducting primary banking activities,

ç) Summary info on information system architecture of the auditee,

d) Explaining the web structure of the auditee and web topography,

e) Demonstration of software and instruments primary banking activities on information system architecture,

f) If information systems audit has been carried out, summary info supporting critical control targets such as change management, security management etc. .

Evaluation concerning the internal control and internal audit structures of the auditee

ARTICLE 12— (1) The Auditor shall give place to the following in this part of the report:

- a) Evaluation of the planning, activities and monitoring of the audit results realized by the internal audit unit within the scope of internal controls audit concerning the financial reporting systems,
- b) Importance given by the management to the establishment and reliable execution of the internal controls concerning the financial reporting systems, evaluation of its performance in measuring the adequacy and the effectiveness of these controls,
- c) Evaluation of the risk assessment processes of managers, related to the internal controls concerning the financial reporting systems.

(2) The Auditor shall specify in his/her report the following concerning the IT audit team:

- a) Team's profile,
- b) Team's activities,
- c) Audit studies they have realized,
- ç) Their place within the organization.

(3) In the end of this section, the Auditor shall fill the table within the Annex-3 for each finding he/she detected within the scope of this section. The findings detected in previous periods but expressed in the report of the present period because they have not been corrected shall also be presented within the same table.

Banking processes audit

ARTICLE 13 — (1) The Auditor shall specify clearly the materiality evaluation he/she used during the audit he/she have conducted relating to the efficiency, adequacy and consistency of the controls upon the banking processes, the processes he/she chose as a result of this evaluation as well as the reasons for this choice and the reasons for which he/she did not choose the other processes.

(2) The Auditor shall fill the table summarizing the work flow diagrams concerning the processes relating to banking activities presented by the auditee and his/her own study about the controls upon the processes taking place within these diagrams, as it is specified within the annex—5 and shall add these to his/her report within a CD.

(3) The Auditor shall fill the table within the annex-3 for each finding he/she has detected during the audit and shall give place to these findings under the related process according to their priority. For the findings detected previously but expressed within present report because they have not been corrected, the table within the annex-3 is filled also.

(4) The Auditor shall deliver his/her evaluations questioning how the controls upon the process are fulfilling the functions expected from them and also his/her evaluations concerning the efficiency, adequacy and consistency of the process as a whole, in the end of this section.

Preparation of risk matrix concerning the applications

ARTICLE 14 — (1) The Auditor shall establish a risk matrix to rate the risks belonging to the applications used by the auditee in its activities and to specify net risk emanated from these activities. In this matrix belonging to the risks emanated from the applications, the importance rate of the applications, risks integrated in the applications, efficiency, adequacy and maturity level of the general controls of information systems and controls upon the banking processes, and the net risk of the auditee emanated from these applications are evaluated. The principles and procedures concerning the preparation of the risk matrix explained in this article are determined by the Board.

Bank information systems audit

ARTICLE 15 — (1) The Auditor shall express clearly the importance evaluation he/she has used in the bank information systems audit as well as the control targets he/she has chosen as a result of this evaluation, the reasons of this choice and the reasons for which he/she did not choose the others.

(2) The Auditor shall give place to a general evaluation in his/her report as to include the comparison of each control field within COBIT with their level within the previous periods.

(3) The Auditor shall fill the table within the annex-4 for each information systems finding detected during the audit; and shall give place to these findings under the related control fields, according to the control target they are related to and to their priority. For the findings detected in previous periods but still expresses because they have not been corrected, the table within the annex-4 is filled also.

(4) The Auditor shall give place in his/her report the following elements for each control target under the control fields and that he/she have chosen according to the criteria of priority:

a) Name of the control target chosen,

b) Responsible of the control target,

c) Maturity level relating to the control target, obtained by evaluating the process or all of the processes formed to provide the control target,

ç) How and with which criteria did the auditee provide the maturity level determined by the Auditor and/or which criterion are missing.

SECTION FOUR
Miscellaneous and Final Provisions

Consolidated Audit Report

ARTICLE 16 — (1) The consolidated audit report concerning banks' partners subject to consolidation and which is within the scope of the bank information systems and banking processes audit realized by external audit institutions pursuant to the article 2 and the sub-paragraph (i) of the first paragraph of article 4 of the Regulation, shall be composed as follows:

- a) Audit letter formed within the scope of the article 34 of the Regulation,

- b) Executive summary,

- c) Contents,

- ç) Table concerning the bank affiliates prepared as defined within the annex-6,

- d) Information concerning the audit and

- e) Evaluations of the bank and its partners by their effect on the consolidated financial statement.

(2) In the executive summary part, the information specified within the sub-paragraphs (a) and (b) of the first paragraph of the article 9 of this Communiqué, findings considerable for their effects on the consolidated financial statement in the bank and its partners and the evaluations of these findings for the consolidated financial statement shall take place. A

general evaluation shall be made about the information system producing the financial data to be consolidated and/or the process and the financial data flow between the bank and the partners.

(3) In the part of evaluation of the bank and its partners by their effect on the consolidated financial statement:

a) The findings detected in the bank shall be evaluated and classified by the consolidated financial statement. The findings classified as significant control weakness and important control weakness shall be presented after that they are filled with the appropriate table under the annex-3 and annex-4.

b) For each partner who is included to the information systems audit, the following information shall be presented:

1) Name of the partnership, structure of the partnership (if it's an affiliate, subsidiary or jointly controlled partnership), its activities and the reasons for which it is included to consolidated audit,

2) The scope of the audit specifying which of the information systems and working processes audits have been realized in the partnership, which processes/control targets have been audited and the evaluation of the importance used in the choice of these processes/control targets,

3) As a result of the audit realized, a general evaluation in the subjects of defining, producing, using the consolidated financial information and ensuring its accuracy, completeness and confidentiality, as well as the effect of the partner made subject to the audit,

4) Findings detected in the partners, prepared by choosing and filling the appropriate table among the table within the annex-3 and annex-4 after that they are evaluated by the consolidated financial statement and classified as significant control weakness and important control weakness.

Annulled regulations

ARTICLE 17 — (1) The Communiqué on Report Format Concerning Information Systems to be performed in Banks by External Audit Institutions published in the Official Gazette dated December 5, 2006 Nr. 26367 is annulled.

Entry into Force

ARTICLE 18 — (1) This Communiqué enters into force on the date of its publication to be valid as of the date of December 31, 2009.

Enforcement

ARTICLE 19 — (1) The provisions of this Communiqué are enforced by the Chairman of the Banking Regulation and Supervision Agency.

Annex 1 – Summary Finding Table

Audit Field (1)	Level of Importance of the Finding	Current Period (2)		Previous Periods (3)			
		Number of Findings Corrected	Number of Findings Corrected Partially (4)	Number of Findings Continuing	Total Number of Findings of Previous Periods		
	ICD (5)						
...	SCD (6)						
	CW (7)						
Banking Processes Total	ICD SCD CW						
	ICD						
•..	SCD						
	CW						
Information Systems Total	ICD SCD						

	CW						
Internal Control/ Audit	ICD SCD CW						

1) Implies the names of the processes defined within the second paragraph of the article 25 of the Regulation for the Banking Processes Audit, and the general control field defined in the COBIT for Information Systems Audit.

2) Implies the finding detected in current period only.

3) Implies the findings detected by the auditor within previous audit periods but did not express that they are corrected within the previous periods.

4) If as a result of the studies conducted by the auditor, the risk carried by the finding is reduced, the finding is included in this class. The partially corrected findings shall not be included into the continuing findings within the aim of avoiding the repetitions.

5) Important Control Deficiency

6) Significant Control Deficiency

7) Control Weakness

Annex 2 – Control Targets Maturity Level Chart Comparative with Previous Periods

Maturity	Levels	Evaluated
5—		
4—		
3—		
2—		

- 1- The Auditor shall draw this table separately for each of four control fields.
- 2- The Column concerning the control target chosen by evaluating the criteria of importance among control fields shall be added to the table.
- 3- If the related control target was not audited in the previous audits, the auditor shall give place only to the column concerning the current period.



Annex 3 — Table of Findings Related to Banking Processes, Internal Control Audit Structure

Code of Finding (1)	Process
Number of Control (2)	
Finding (3) (*)	
Risk of the Job (4) (*)	
Opinion of the Auditee (5) (*)	

Result Evaluation (6) (*)	
----------------------------------	--

In the rows specified with (), if there are any differences between the previous and current periods, the evaluations concerning both periods are written separately.*

- 1 Finding code compatible with the format determined by the Agency
- 2 Related control number and/or numbers determined within the Annex-2
- 3 Findings as defined within the article 5 of this Communiqué
- 4 Job risks which may be emanated from the mal-functioning of the control
- 5 The auditee’s opinion as defined within the article 6 of this Communiqué
- 6 Result evaluation as defined within the article 7 of this Communiqué

Annex 4 — Findings Table for Information Systems General Controls

Code of Finding (1)	Control Target
Detailed Control Target	
Finding (2) (*)	
Risk (3) (*)	
Opinion of the Auditee (4) (*)	
Result Evaluation (5) (*)	

In the rows specified with (), if there are any differences between the previous and current periods, the evaluations concerning both periods are written separately.*

- 1 Finding code compatible with the format determined by the Agency
- 2 Findings as defined within the article 5 of this Communiqué
- 3 IT and job risks emanated by the mal-functioning of the control
- 4 Auditee’s opinion as defined within the article 6 of this Communiqué
- 5 Result evaluation as defined within the article 7 of this Communiqué

Annex 5 – Table of Application Controls upon the Processes Concerning Banking Activities
 (*)

Process:

Number of Control: Application: Definition of Control: Test:

Table Explanations

Process: Name of process chosen and audited by the criteria of priority

Name of Application: Name of application supporting/realizing upon the process concerning the related banking activity. Shall be left empty for controls not realized with an application.

Number of Control: Number belonging to the control shown on the job flow diagram and which is upon the process. A meaningful number providing to detect the spot to which the control corresponds.

Definition of Control: A brief definition in which the function of the control is defined.

Test: Whether or not the auditor had realized a test upon this control (Tested/Not Tested). If tested, as to give the number of samples used in this test. For example “*Tested-25*”, or “*Not Tested*”.

(*) Given within a CD attached to the report.

Annex 6- Table Concerning the Institution Owned by the Bank

Nr	Institution	If It Is a Financial Institution (*)	Subject to Consolidated Financial Audit (*)	Subject to Information Systems and Banking Processes Audit (*)
1				
2				

(*) Filled with a Check sign in positive situations, left empty in negative ones.

