Title: BANKING AUDIT SYSTEM AND METHOD

Abstract: This invention relates banking audit method enabling the audit of the bank employees working in the banking sector in terms of competence/qualification, the audit of the banking transaction’s conformity to the in-bank and legal regulations and the audit of the efficiency of the systems, the realizations of the supervisions over live screens differently from classic supervision, after the audit, the correction of the finding in the audit report according to the audit report within the targeted periods and simple tracking of the related correction actions, and to the system enabling the application of this method.
BANKING AUDIT SYSTEM AND METHOD

Technical Field
This invention relates to the supervision of the bank employees working in the banking sector in terms of competence/qualification, the supervision of the banking transaction's conformity to the in-bank and legal regulations and the supervision of the efficiency of the systems; and after the audit, providing corrections on the finding of the audit report according to the audit report within the targeted period.

State of the Art
At the present time, the internal audit of the banks are firstly performed by internal auditors and also auditors (i) affiliated with the banks are employed. Banks are responsible for building a risk control and management system with an internal audit system to be determined via a regulation, the principles and procedures of which are issued by competent bodies, which is in accordance with the scope and structure of the activities thereof in order to monitor the risks encountered during the transactions and to provide control. Moreover, the banks are obliged to employ a sufficient number of auditors in order to audit the transactions in terms of conformity for the banking principles and regulations.

In the existing practices, the audit reports are principally generated on a Microsoft Office media or in a separate interface within the banking system with the data inputs which are directly entered into this interface. Collecting said data, measuring the tendency of the audited department/branch to perform risky transactions or identifying the business processes with relatively high risk rate are performed manually. Besides, the departments/branches are audited pursuant to the subjective criteria which are created substantially with a subjective risk perception. The audit focuses mainly on whether the transactions completed within the audit period were executed duly, however the conformity of the system with the banking policy and the competence of the employees cannot be assessed.

In the existing practices, after the audit is completed, it is especially controlled whether the finding in the audit reports are corrected.

In the prior art research, a patent application with No. TR201109917 was encountered. In this application, operating systems and the platform thereof are described, which are designed in order to improve and optimize the processes relating to the banking services. It is aimed that
transactions in the bank or in a bank branch are performed in real-time within a narrowed time-period by a computer media and the results are displayed by obtaining the information such as variations in the activity processes, uncertainties, the number of the employees, customer behaviors and external factors from the branch/bank system and using them as a data. A system is described, where a close-range communication performed by a barcode reading method is used.

As a result, because of the disadvantages mentioned above and that the existing solutions are insufficient for the case, it is necessary to make an improvement in this technical field.

Object of the Invention

The object of the invention is to provide a audit system and method which provides an objective audit of the files over a system minimizing the subjective risk perception of the auditor.

The object of the invention is to enable the auditor to audit over the live screens used by the bank employees during the audit and to enable preparing the related reports for the supervision during audit.

The object of the invention is to control the competence/qualification of the bank employees, conformity of the transaction with the in-bank and legal regulations and the efficiency of the system.

The object of the invention is to approach all the customers as a whole by providing the audit system as a structure parallel to the customer-oriented banking system and to assess the reflections of the product-specific risks specific to the customers.

The object of the invention is to provide a dynamic structure for the audit points varying according to the audited department/branch, customer segment and products and to provide an easy integration to the corrections within the possible in/out bank legal regulations, enforcements, principals and methods.

The object of the invention is to provide an action for the findings in the audit reports after the audit.

The object of the invention is to transmit the findings to the related departments after the completion of the audit reports and to use them for the processes of the next administrative decisions.
The object of the invention is to rank the departments/branches/bank employees regarding to their risky transaction tendencies, to measure findings concentrations on the basis of bank transaction process and to go to the customer where the finding is noted in the related audit report by showing that reporting does not only consist of compiling the findings from the audited branch/department audit reports.

The object of the invention is to track the correction actions from the branches more efficiently within the correction periods added to the finding by generating a finding tracking systems.

The object of the invention is to provide access to the audit reports recorded by generating a virtual archive module and to facilitate tracking of the previous reports.

The invention aims to overcome the disadvantages mentioned above by inspiring from the existing situations.

The structural and characteristic features and all the advantages of the invention will be understood more clearly thanks to the detailed description thanks to the drawings given below and the references to these drawings, and thus the examination should be performed by taking these drawings and detailed description into account.

**Drawings Which Helps Understanding of the Invention**

- **Figure 1** - Schematic block diagram of the banking audit system
- **Figure 2** - Flow diagram of the banking audit method
- **Figure 3** - Flow diagram of the risky user tracking method
- **Figure 4** - Flow diagram of the finding tracking system
- **Figure 5** - Flow diagram of the reporting method
- **Figure 6** - Flow diagram of the integration method of the virtual archive and electronic signature

**Descriptions of the References**

1. Banking supervision system
10. Risky user detection module
   11. Working index module
   12. Audit process module
   13. In-report finding tracking system
20. Finding tracking module
30. Reporting module
   31. Audit report monitoring module
   32. Audit and finding reporting module

40. Virtual archive and electronic signature integration module

50. Finding

60. User list to be audited (Index)

1000. Banking supervision method

1001. Controlling whether the user (K) is detected by the risky user detection module

1002. If the user (K) is detected by the risky user detection module, adding this user (K) to the user list to be audited by the risky user detection module

1003. Auditing the user (K) as a whole over the live screens integrated into the main banking platform of the bank

1004. Controlling whether the auditor (D) has any finding for the user (K) by the finding tracking system

1005. If the auditor (D) has any finding for the user (K), controlling whether the finding is corrected during the audit

1006. If the finding is corrected during the audit, recording it as corrected during the audit

1007. Recording the report to the virtual archive module by electronic signature integration

1008. Collecting the completed reports within the reporting module

1009. Presenting the report results to the administrative units in a department and finding based way

1010. Controlling whether the auditor (D) thinks that the user (K) is risky

1011. If the auditor (D) thinks that the user (K) is risky, adding the user (K) to the user list to be audited by the auditor (D)

1012. If the auditor (D) does not think that the user (K) is risky, excluding the user (K) from the audit

1013. If the finding is not corrected during the audit, determining a target correction period for the finding

1014. Controlling whether the finding is corrected within the target correction period

1015. Recording the correction after confirmed by the auditor (D)

1016. If the finding is not corrected within the target correction period, granting an extension of time

1017. Controlling whether the finding is corrected within the time extension

1018. If the finding is not corrected within the time extension, sending warning messages periodically to the parties and managers until the finding is corrected.
1019. If the auditor (D) has no finding (D) for the user (K), presence of the user (K) with no noted finding by the auditor (D) as a user (K) having been audited and having no finding in the audit report.

2000. Risky user detection method

2001. Approaching all users (K) of all departments subject to the audit

2002. Controlling whether the user (K) has non-performing loan accounts

2003. Automatic ranking of all users (K) in accordance with risk criteria determined by the internal audit department

2004. Selection of at least 20 and at most 80 users (K) from the ordered list automatically such that it will form at least 20% of the credit risk of the audited department

2005. Controlling whether the user (K) is among the selected users (K)

2006. Formation of the list of users to be audited

2007. Controlling whether there are at least 5 users (K) in portfolio of each portfolio manager in the department subjected to the audit in the user list to be audited

2008. Direct acceptation of the user list to be audited without any addition

2009. Existence of the user list to be audited in audit transaction module as a tab

2010. One by one auditing of the users (K) in the user list to be audited by the auditor (D)

2011. Controlling whether there is finding for the user (K) in the user list to be audited by the auditor (D)

2012. Marking of the user (K) as automatically audited

2013. Controlling whether the auditor (D) thinks that the user (K) is risky during the audit

2014. Exclusion of the user (K) from the audit

2015. Adding automatic user (K) from the ranking formed according to determined criteria such that there will be at least 5 users (K) of each portfolio manager in the user list to be audited

2016. Marking of the user (K) as audited in the user list to be audited by the auditor (D)

2017. Controlling whether the credits of the users (K) are transferred to the non-performing loan accounts before the previous audit date

2018. Controlling whether the credit balance is among the highest 10 users (K)

3000. Finding tracking method

3001. Controlling whether there is finding for the user (K) by the auditor (D)

3002. If the auditor (D) has any finding for the user (K); controlling whether the correction record is before the completion of the audit for the finding

3003. If the correction record is prepared before the completion of the audit for the finding;
controlling whether the auditor (D) confirms the correction transaction with information and documents

3004. If the auditor (D) confirms the correction transaction with the information and the documents; reporting of the finding to the report as being corrected during the audit

3005. Recording of the report to the virtual archive module via electronic signature

3006. If the auditor (D) has no finding for the user (K); finding tracking will not operate for this user (K) as there is no finding input

3007. If the correction report is not prepared for the finding before the completion of the audit; determination of the target correction period by negotiating of the auditor (D) with the auditee (Y) for correction of the data

3008. Controlling whether the correction record is prepared for the finding within target correction period by the branch

3009. If the correction record is prepared for the finding within target correction period by the branch; controlling whether the auditor (D) confirms correction transaction with the information and the documents

3010. If the correction record is not prepared for the data within target correction period by the branch; requesting a time extension by the auditee (Y)

3011. Controlling whether the auditor (D) confirms time extension request

3012. If the auditor (D) confirms time extension request; controlling whether correction action is taken for the finding within the time extension

3013. If the auditor (D) does not confirm time extension request or the correction action is not taken for the data within the time extension; transmittance of warning messages to the auditor (D) and the auditee (Y) and managers of the auditee (Y)

4000. Reporting method

4001. Controlling whether the audit report is completed

4002. If the audit report is completed; tracking of the report and all the finding in the report by both the audited department and all managers of the audited department by the audit report monitoring module

4003. If the audit report is completed; tracking of all assessments written in all departments on the basis of the data with audit detection and reporting module

4004. If the audit report is completed; the classification of the data on the basis of bank-wise/coordinatorship/regional directorate/branch and portfolio with audit detection and reporting module

4005. Monitoring the number of the finding detected on the basis of the audited user (K) within the frame of the classifications
4006. Monitoring the data risk detected on the basis of the audited user (K) risk within the frame of the classifications
4007. Use of the audit results obtained from the reporting module in the following administrative decisions by the managers
4008. If the audit report is not completed; monitoring of the stage of the uncompleted reports with audit report monitoring module
5000. Virtual archive and electronic signature integration method
5001. Tracking of the audit report by the auditee (Y) from the moment it was started to be written, interactive correction of the finding during the audit
5002. Controlling whether the auditee (Y) thinks that the finding is a correct/truth-reflecting data while the audit report is being written
5003. Finalization of the finding as a result of the negotiations
5004. Inclusion of the finding within the audit report
5005. Transmittance of the audit report to the auditee (Y) for replying of the finding
5006. Re-transmittance of the finding to the auditor (D) as being replied by the auditee (Y)
5007. Making comments for the finding replies by the auditor (D)
5008. Completion of the report
5009. Recording to the virtual archive module with the completion record automatically
5010. Signing of the reports recorded in the virtual archive module electronic signature and the subjective electronic signature by the auditor (D)
5011. Negotiation between the auditor (D) and the auditee (Y)
5012. Controlling whether the auditor (D) thinks that the finding is a correct/truth-reflecting data finding, removal of the finding from the audit report

K: User (customer)
D: Auditor (supervisor)
Y: Auditee (portfolio manager)

The drawings do not need to be scaled and details that are not required for a full understanding of the present invention may have been disregarded. Apart from this, elements which are at least substantially identical or which has at least substantially identical functions are exhibited with the same numbers.

**Detailed Description of the Invention**

In this detailed description, preferred embodiments of the system of the invention are merely explained for a better understanding of the subject.

Components and features of the banking audit system (1) of the invention is as follows:
In Figure 1, the departments constituting the banking audit system (1) are shown as schematic block diagram. The system (1) comprises: risky user detection module (10), working index module (11), audit process module (12), in-report detection tracking module (13), audit tracking module (20), reporting module (30), audit report monitoring module (31), audit and detection reporting module (32), virtual archive and electronic signature integration module (40) departments.

**Risky user detection module (10):** With the risky user detection module (10), it is enabled to minimize the subjective risk perception in the audit by enabling the preparation of the user lists (60), forming a basis for the audit and to be audited, using certain risk parameters. The audit is realized over the live screens with a module integrated into the basic banking platform of the audit, thereby enabling the domination of the system by the auditors (D), and the analysis of the system activity becomes a part of the audit. In-bank and legal regulations that may be required by the auditor (D) are maximally integrated into the audit system (1). Thus, time loss due to regulation search is prevented and an instructional system (1) is structured. It is enabled that transactions for update of the system is conducted before the Board of Auditors independent of the technology company. Thus, it is enabled that the audit is constantly up to date, and audit is performed within the framework of the most recent dated regulations and policies. Issuing of the data (50) included in the audit reports in the related user (K) panel after the completion of the report and presentation to the attention of those concerned are enabled.

**Working index module (11):** It is the list of the users (K) taken into precision sampling by the working index module (11) risky user detection module (10). In this list, there is information of affiliated segment of the user (K), portfolio responsible, limit and risk information, and segment of the user (K), method of inclusion of the user (K) into the user list to be audited (60) (automatically or by the auditor), information of the auditor (D) audit the user (K) and last time of audit of the user (K). Working index module (11) filtrates this information and provides only desired information to the user (K).

**Audit transaction module (12):** Audit transaction module (12) contains tag information of the audit. In this module, there is information such as the auditor (D) conducting the audit, if present, other auditors (D) in the team, confirmation finding of the report, the dates between which the audit was conducted, branch where the audit was conducted, and affiliated regional directorate/coordinatorship.

**In-report detection monitoring module (13):** In-report detection monitoring module (13) enables the
display of the related audit point explanation of each user (K) for whom the auditor (D) performs finding input during the audit along with the branch reply.

finding tracking module (20): finding tracking module (20) enables systematically tracking of all correction processes relating to risky transactions about the audit report. It enables the enhancement of awareness of the bank workers and managers for the correction of the finding (50) specific for the related users (K) right after the completion of the determined target correction period.

Reporting module (30): Reporting module (30) renders work processes and their concentrations on the basis of the sub-processes and audit points of the audit finding (50) reportable without any manual transaction. It enables the evaluation and ranking of risky transaction tendencies of work departments and department workers on the basis of the related risk criteria. Reporting module (30) enables the tracking of the audit reports as a whole as well as the tracking for subject title, work process and sub-processes with the determined selection criteria.

Audit report monitoring module (31): With the audit report monitoring module (31), filtering is performed in accordance with the preferred search criteria and access is granted into the reports arranged within the scope of new audit model, spot audit or investigation. Current statuses of the reports are tracked.

Audit and detection reporting module (32): The audit and detection reporting module (32) detects the finding (50) with a concentrations by filtering among various criteria (such as regional directorate/coordinatorship, branch segment, branch scale) between the determined dates and informs the user (K) with graphics simultaneously.

Virtual archive and electronic signature integration module (40): The virtual archive and electronic signature integration module (40) enables the recording of the audit report as electronically signed after the completion of the audit. With the recording of the audit report in the virtual archive (40) as electronically signed, both the related article of the internal systems regulation is fulfilled and waste of thousands of papers spent each year for archiving of the audit reports are prevented. The audit reports formed by the auditors (D) the investigation/inspection documents and information notes are recorded into the virtual archive and electronic signature integration module (40), thereby providing opportunity for the improvement of the audit process from different perspectives.
A banking audit system (1) enabling the supervision of the bank employees working in the banking sector in terms of competence/qualification, the supervision of the banking transaction's conformity to the in-bank and legal regulations and the supervision of the efficiency of the systems; and after the audit, the elimination of the manual action tracking processes for the finding (50) within the audit reports and the tracking of the related regulations within the targeted period according to the audit report, comprising:

- At least one risky user detection module (10) enabling the preparation of the user lists (60) to be audited, forming a basis for the audit and to be audited, using certain risk parameters and enabling the realization of the audit over the live screens,

- At least one working index module (11) comprising the user lists to be audited (60) to which the users (K) are added by the risky user detection module (10) by means of precision sampling and/or added manually in a situation arising during the audit,

- At least one audit process module (12) containing all information of the audit and the auditor (D),

- At least one in-report detection tracking module (13) enabling the display of the related audit point explanation of each user (K) whose input is made to the audit points during the audit along with the branch reply,

- At least one data tracking module (20) systematically tracking the correction processes relating to the risky transactions subject to the audit report,

- At least one reporting module (30) rendering the work processes and their concentrations on the basis of the sub-processes and audit points of the audit finding (50) reportable without any manual transaction,

- At least one audit report monitoring module (31) enabling the tracking of the all conducted audits by filtering,

- At least one audit and detection reporting module (32) enabling the tracking of the problems encountered in the banking processes and the tracking of the areas of concentration of the audit points,

- At least one virtual archive module (40) enabling the tracking of the audit reports recorded as electronically signed,

- At least one finding (50) expressing incompleteness/error/violation to bank regulation or law detected on works and transactions of the users (K) audited by the auditor (D),

- At least one the user list to be audited (60) comprising the list of user (K) to be audited during the audit (Figure-1).

In the banking audit method (1000), initially controlling of whether the user (K) is caught by the
risky user detection module (10) is performed. If the user (K) is caught by the risky user detection module (10), the user (K) is added to the user list to be audited (60) by the risky user detection module (10). If the user (K) is not caught by the risky user detection module (10), it is controlled whether the auditor (D) thinks that the user (K) is risky.

In inquiry of whether the auditor (D) thinks that the user (K) is risky, if the auditor (D) does not think that the user (K) is risky; the user (K) is excluded from the audit, if the auditor (D) thinks that the user (K) is risky; the user (K) is added to the user list to be audited (60) by the auditor (D).

The user (K) is audited as a whole over the live screens integrated into the main banking platform of the bank. It is controlled whether the auditor (D) has any finding (50) for the user (K) by the finding tracking module (20). If the auditor (D) has any finding (50) for the user (K), it is controlled whether the finding (50) is corrected during the audit. If the auditor (D) has no finding (50) for the user (K), the user (K) is included into the audit report as a user (K) having been audited and having no finding (50).

In inquiry of whether the finding (50) is corrected during the audit, if the finding (50) is corrected during the audit, the finding (50) is recorded as being corrected during the audit; if the finding (50) is not corrected during the audit, the parties determine a target correction period for the finding (50).

Report is recorded to the virtual archive module (40) with the electronic signature integration. Completed reports are included within the scope of the reporting module (30). The report results on the basis of the department and the finding (50) are presented to the use of the administrative departments.

After the parties determine a target correction date for the finding (50), it is controlled whether the finding (50) is corrected within the target correction period. If the finding (50) is corrected within the target correction period, correction is recorded as being confirmed by the auditor (D). If the finding (50) is not corrected within the target correction period, time extension is granted and it is controlled whether the finding (50) is corrected within the time extension.

In inquiry of whether the finding (50) is corrected within the time extension, if the finding (50) is corrected within the time extension, correction is recorded as being confirmed by the auditor (D). If the finding (50) is not corrected within the time extension, automatic messages are sent
periodically to the parties and managers until the finding (50) is corrected.

The banking audit system (1000) enabling supervision of the bank employees working in the banking sector in terms of competence/qualification, the audit of the banking transaction's conformity to the in-bank and legal regulations and the supervision of the efficiency of the systems; and after the audit, the tracking of the related regulations of the finding (50) within the audit reports within the targeted period in accordance with the audit report, comprising the steps of:

- Controlling whether the user (K) is caught by the risky user detection module (10) (1001),
- If the user (K) is caught by the risky user detection module (10), adding the user (K) to the user list to be audited (60) by the risky user detection module (10) (1002),
- Auditing of the user (K) as a whole over the live screens integrated into the main banking platform of the bank (1003),
- Controlling whether the auditor (D) has any finding (50) for the user (K) by the finding tracking module (20) (1004),
- If the auditor (D) has any finding (50) for the user (K), controlling whether the finding is corrected during the audit (1005),
- If the finding (50) is corrected during the audit, recording of the finding (50) as being corrected during the audit (1006),
- Recording of the report to the virtual archive module (40) with the electronic signature integration (1007),
- Including the completed reports within the scope of the reporting module (30) (1008),
- Presenting the report results on the basis of the department and the finding (50) to the use of the administrative departments (1009),
- Controlling whether the auditor (D) thinks that the user (K) is risky (1010),
- If the auditor (D) thinks that the user (K) is risky, adding the user (K) to the user list to be audited (60) by the auditor (D) (1011),
- If the auditor (D) does not think that the user (K) is risky, excluding the user (K) from the audit (1012)
- Determining of the target correction period for the finding by the parties (1013),
- Controlling whether the finding is corrected within the target correction period (1014),
- Confirming and recording of the correction by the auditor (D) (1015),
- Granting a time extension if the finding is not corrected within the target correction period (1016),
- Controlling whether the finding is corrected within the time extension (1017),
- If the finding is not corrected within the time extension, sending warning messages
periodically to the parties and managers until the finding is corrected (1018),
- Presence of the user (K) with no detected finding by the auditor (D) as a user (K) having been audited and having no finding in the audit report (1019) (Figure-2).

In the risky user detection method (2000), initially all users (K) of the department are handled and it is controlled whether the user (K) has any credits being tracked in non-performing loan accounts. If the user (K) has no credits being tracked in non-performing loan accounts; all users (K) are ranked in accordance with risk criteria determined by the internal audit department. If the user (K) has a credit being tracked in non-performing loan accounts; it is controlled whether the credits of the user (K) are transferred to the non-performing loan accounts before a previous audit date.

At least 20 and at most 80 users (K) from the ordered list are selected automatically such that it will form at least 20% of the credit risk of the audited department. It is controlled whether the user (K) is among the selected users (K). If the user (K) is among the selected users (K); the user list to be audited (60) is formed. If the user (K) is not among the selected users (K); it is controlled whether the auditor (D) thinks that the user (K) is risky during the audit.

It is controlled whether there are at least 5 users (K) in portfolio of each portfolio manager in the department subjected to the audit in the user list to be audited (60). If there are at least 5 users (K) in portfolio of each portfolio manager in the department subjected to the audit in the user list to be audited (60), the user list to be audited (60) is accepted without further addition. If there are not at least 5 users (K) in portfolio of each portfolio manager in the department subjected to the audit in the user list to be audited (60); automatic user (K) is added from the ranking formed according to determined criteria such that there will be at least 5 users (K) of each portfolio manager in the user list to be audited (60).

The user list to be audited (60) exists in the audit transaction module (12) as a tab. The auditor (D) audits all users (K) in the user list to be audited (60) one by one, and it is controlled whether there is finding for the user (K) in the user list to be audited (60). If the auditor (D) has any finding for the user (K) in the user list to be audited (60); the user (K) is marked as automatically audited. If the auditor (D) has no finding for the user (K) in the user list to be audited (60); the user (K) is marked as audited in the user list to be audited (60) by the auditor (D).

In inquiry of whether the auditor (D) thinks that the user (K) is risky during the audit, if the auditor
(D) does not think that the user (K) is risky; the user (K) is excluded from the audit. If the auditor (D) thinks that the user (K) is risky; user list to be audited (60) is formed.

In inquiry of whether the credits of the user (K) are transferred to the non-performing loan accounts before a previous audit date, if the credits of the user (K) are transferred to the non-performing loan accounts before a previous audit date; it is controlled whether the credit balance is among the highest 10 users (K). If the credits of the user (K) are not transferred to the tracking accounts before a previous audit date; the user list to be audited (60) is formed.

In inquiry of whether the credit balance is among the highest 10 users (K), if the credit balance is among the highest 10 users (K); the user list to be audited (60) is formed. If the credit balance is not among the highest 10 users (K); it is controlled whether the auditor (D) thinks that the user (K) is risky during the audit.

The risky user detection method (2000) forming the user lists to be audited (60) constituting a basis for the audit using certain risk parameters by a system and enabling the realization of the audit over live screens, comprising the steps of:

- Handling all users (K) of the department subject to the audit (2001),
- Controlling whether the users (K) has any credits being tracked in non-performing loan accounts (2002),
- Ranking of all users (K) automatically in accordance with risk criteria determined by the internal audit department (2003),
- Selecting at least 20 and at most 80 users (K) from the ordered list automatically such that it will form at least 20% of the credit risk of the audited department (2004),
- Controlling whether the user (K) is among the selected users (K) (2005),
- Formation of the list of user to be audited (60) (2006),
- Controlling whether there are at least 5 users (K) in portfolio of each portfolio manager in the department subjected to the audit in the user list to be audited (60) (2007),
- Directly accepting the user list to be audited (60) without further addition (2008),
- Existence of the user list to be audited (60) as a tab in the audit transaction module (12) (2009),
- One by one auditing of the users (K) in the user list to be audited (60) by the auditor (D) (2010),
- Controlling whether the auditor (D) has any finding for the user (K) in the user list to be audited (60) (2011),
- Marking of the user (K) as automatically audited (2012),
- Controlling of whether the auditor (D) thinks that the user (K) is risky during the audit (2013),
- Excluding the user (K) from the audit (2014),
- Adding automatic user from the ranking formed according to determined criteria such that there will be at least 5 users of each portfolio manager in the user list to be audited (60) (2015),
- Marking of the user (K) as audited in the user list to be audited (60) by the auditor (D) (2016),
- Controlling whether the credits of the users (K) are transferred to the non-performing loan accounts before the previous audit date (2017),
- Controlling whether the credit balance is among the highest 10 users (K) (2018) (Figure-3).

In the finding tracking method (3000), initially it is controlled whether the auditor (D) has any finding (50) for the user (K). If the auditor (D) has any finding (50) for the user (K); it is controlled whether the correction record is made before the completion of the audit for the finding (50). If the auditor (D) has no finding (50) for the user (K); finding tracking module (20) will not operate for this user (K) as no finding (50) input is made for the user (K).

In inquiry of whether the correction record is made before the completion of the audit for the finding (50), if the correction record is made before the completion of the audit for the finding (50), it is controlled whether the auditor (D) confirms the correction transaction with the information and the documents. If the correction record is not made before the completion of the audit for the finding (50); the auditor (D) and the auditee (Y) determine, by negotiation, a target correction date for correction of the finding (50).

In inquiry of whether the auditor (D) confirms the correction transaction with the information and the documents, if the auditor (D) confirms the correction transaction with the information and the documents; the finding (50) is recorded to the report as being corrected during the audit and the report is recorded to the virtual archive module (40) with electronic signature integration. If the auditor (D) does not confirm the correction transaction with the information and the documents; the auditor (D) and the auditee (Y) determine, by negotiation, a target correction date for correction of the finding (50) and it is controlled whether the correction record is made for the finding (50) within the target correction period by the branch.
In inquiry of whether the correction record is made for the finding (50) within the target correction period by the branch, it is controlled whether the auditor (D) confirms the correction transaction with the information and the documents. If the correction record is not made for the finding (50) within the target correction period by the branch; time extension is requested by the auditee (Y).

In inquiry of whether the auditor (D) confirms the correction transaction with the information and the documents, if the auditor (D) confirms the correction transaction with the information and the documents; the report is recorded to the virtual archive module (40) with the electronic signature integration. If the auditor (D) does not confirm the correction transaction with the information and the documents; time extension is requested by the auditee (Y).

After the time extension request by the auditee (Y), it is controlled whether the auditor (D) confirms the time extension request. If the auditor (D) confirms the time extension request; it is controlled whether the corrected report is prepared for the finding (50) within the time extension. If the auditor (D) does not confirm the time extension request; warning messages are sent periodically to the auditor (D) and the auditee (Y) and affiliated manager of the auditee (Y) until the finding (50) is corrected.

In inquiry of whether the amended report is prepared for the data (50) within the time extension, if the correction action is taken for the finding (50) within the time extension; it is controlled whether the auditor (D) confirms the correction transaction with the information and the documents. If the correction action is not taken for the finding (50) within the time extension; warning messages are sent periodically to the auditor (D) and the auditee (Y) and affiliated manager of the auditee (Y) until the finding (50) is corrected.

The finding tracking method (3000) enabling systematical tracking of the correction processes relating to the risky transactions of the audit report and, after the completion of the audit, the enhancement of awareness for the correction of the finding (50) specific for the related users (K) within the determined target correction period, comprising the steps of:

- Controlling whether the auditor (D) has any finding (50) for the user (K) (3001),
- Controlling whether the correction record is made before the completion of the audit for the finding (50) (3002),
- Controlling whether the auditor (D) confirms the correction transaction with the information and the documents (3003),
- Recording of the finding (50) to the report as being corrected during the audit (3004),
- Recording of the report to the virtual archive module (40) with the electronic signature integration (3005),
- Not operating of the finding tracking module (20) for this user (K) as there is no finding (50) input for the user (K) (3006),
- Determining a target correction period for the correction of the finding (50) by negotiation between the auditor (D) and the auditee (Y) (3007),
- Controlling whether the correction record is made within the target correction period by the branch for the finding (50) (3008),
- Controlling whether the auditor (D) confirms the correction transaction with the information and the documents (3009),
- Requesting time extension by the auditee (Y) (3010),
- Controlling whether the auditor (D) confirms the time extension request (3011),
- Controlling whether the correction record for the finding (50) is made within the time extension (3012),
- Sending of the warning messages periodically to the auditor (D) and the auditee (Y) and affiliated manager of the auditee (Y) until the finding (50) is corrected (3013) (Figure-4).

In the reporting method (4000), initially it is controlled whether the audit report is completed. If the audit report is not completed; stages of the uncompleted reports can be monitored with the audit report monitoring module (31). If the audit report is completed; the report and the finding (50) within the report are monitored by both the audited department and all managers of the audited department with the audit report monitoring module (31), and the audit results obtained from the reporting module (30) are used in the following decisions.

If the audit report is completed; assessments written by all departments on the basis of the finding (50) are monitored with the audit detection and reporting module (32) and the finding (50) are classified on the basis of bank-wise/coordinatorship/regional directorate/branch and portfolio.

After the classification of the finding (50) on the basis of bank-wise/coordinatorship/regional directorate/branch and portfolio, the number of finding (50) detected on the basis of the audited user (K) and risk of the finding (50) detected on the basis of audited user (K) risk are monitored within the frame of classifications and the audit results obtained from the reporting module (30) are used in the following administrative decisions by the managers.
The reporting method (4000) rendering the work processes and their concentrations on the basis of the sub-processes and the audit points of the audit finding (50) reportable without any manual transaction, and enabling the evaluation and ranking of risky transaction tendencies of work departments and department workers on the basis of the related risk criteria, comprising the steps of:

- Controlling whether the audit report is completed (4001),
- Monitoring of the report and the finding (50) within the report by both the audited department and all managers of the audited department with the audit report monitoring module (31) (4002),
- Monitoring of all assessments written by all departments on the basis of the finding (50) with the audit detection and reporting module (32) (4003),
- Classifying the finding (50) on the basis of bank-wise/coordinatorship/regional directorate/branch and portfolio with the audit detection and reporting module (32) (4004),
- Monitoring of the number of the finding (50) detected on the basis of the audited user (K) within the frame of the classifications (4005),
- Monitoring of the risk of the finding (50) detected on the basis of the audited user (K) within the frame of the classifications (4006),
- Using the audit results obtained from the reporting module (30) in the following administrative decisions by the managers (4007),
- Monitoring of the stage of the uncompleted reports with the audit report monitoring module (31) (4008) (Figure-5).

In the virtual archive and electronic signature integration method (5000), the finding (50) can be monitored by the auditee (Y) from the moment it was started to be written can be corrected during the audit interactively. It is controlled whether the auditee (Y) thinks that the finding (50) is a correct/truth-reflecting finding (50) while the audit report is being written.

In inquiry of whether the auditee (Y) thinks that the finding (50) is a correct/truth-reflecting finding (50) while the audit report is being written, if the auditee (Y) thinks that the finding (50) is a correct/truth-reflecting finding (50) while the audit report is being written; the finding (50) is included into the audit report. If the auditee (Y) does not the finding (50) is a correct/truth-reflecting finding (50) while the audit report is being written; the auditor (D) and the auditee (Y) negotiate.

At the end of the negotiation, it is controlled whether the auditor (D) thinks that the finding (50) is a correct/truth-reflecting finding (50). If the auditor (D) does not think that the finding (50) is a
correct/truth-reflecting finding (50); the finding (50) is excluded from the audit report. If the auditor (D) thinks that the finding (50) is a correct/truth-reflecting finding (50); the finding (50) are finalized as a result of the negotiations.

After the finalization as a result of the negotiations, the finding (50) are included into the audit report. The audit report is transmitted to the auditee (Y) for replying of the finding (50). The finding (50) are replied by the auditee (Y) and re-transmitted to the auditor (D). The auditor (D) states his/her comments about whether he agrees with the finding (50) replies or not and the report is completed. It is recorded to the virtual archive module (40) with the completion record automatically. The auditor (D) signs the reports recorded in the virtual archive module (40) using the subjective electronic signatures with the electronic signature.

The virtual archive and electronic signature integration method (5000) enabling the recording of the audit report to the virtual archive module (40) with electronic signature after the completion of the audit, comprising the steps of:

- Monitoring of the audit report by the auditee (Y) from the moment it was started to be written, correction the data (50) during the audit interactively (5001),
- Controlling whether the auditee (Y) thinks that the finding (50) is a correct/truth-reflecting finding (50) while the audit report is being written (5002),
- Finalization of the finding (50) as a result of the negotiations (5003),
- Inclusion of the finding (50) within the audit report (5004),
- Transmittance of the audit report to the auditee (Y) for replying of the finding (50) (5005),
- Re-transmittance of the finding (50) to the auditor (D) as being replied by the auditee (Y) (5006),
- Making comments for the finding (50) replies by the auditor (D) (5007),
- Completion of the report (5008),
- Recording to the virtual archive module (40) with the completion record automatically (5009),
- Signing of the reports recorded in the virtual archive module (40) with the electronic signature and the subjective electronic signature by the auditor (D) (501 0),
- Negotiation between the auditor (D) and the auditee (Y) (501 1),
- Controlling whether the auditor (D) thinks that the finding (50) is a correct/truth-reflecting finding (50) (5012),
- If the auditor (D) reach the conclusion that the finding is not a correct/truth-reflecting finding, removal of the finding (50) from the audit report (501 3) (Figure-6).
Around these conceptions, the banking audit system (1) enabling the audit of the bank employees working in the banking sector in terms of competence/qualification, the audit of the banking transaction's conformity to the in-bank and legal regulations and the supervision of the efficiency of the systems; and after the audit, the monitoring of the related regulations of the data within the audit reports within the targeted period in accordance with the audit report of the invention and many applications of the method may be improved, however, the invention is not limited to what is disclosed here, basically as stated in the claims.
CLAIMS

1. Method (1000) for a banking audit system (1) enabling the supervision of the bank employees working in the banking sector in terms of competence/qualification, the supervision of the banking transaction's conformity to the in-bank and legal regulations and the supervision of the efficiency of the systems; and after the audit, the tracking of the related correction actions of the finding (50) within the audit reports within the targeted period in accordance with the audit report, characterized in that said method comprises the following steps:

   - Controlling whether the user (K) is caught by the risky user detection module (10) (1001),

   - If the user (K) is caught by the risky user detection module (10), adding the user (K) to the user list to be audited (60) by the risky user detection module (10) (1002),

   - Auditing of the user (K) as a whole over the live screens integrated into the main banking platform of the bank (1003),

   - Controlling whether the auditor (D) has any finding (50) for the user (K) by the finding tracking module (20) (1004),

   - If the auditor (D) has any finding (50) for the user (K), controlling whether the finding is corrected during the audit (1005),

   - If the finding (50) is corrected during the audit, recording of the finding (50) as being corrected during the audit (1006),

   - Recording of the report to the virtual archive module (40) with the electronic signature integration (1007),

   - Including the completed reports within the scope of the reporting module (30) (1008),

   - Presenting the report results on the basis of the department and the finding (50) to the use of the administrative departments (1009),

   - Controlling whether the auditor (D) thinks that the user (K) is risky (1010),

   - If the auditor (D) thinks that the user (K) is risky, adding the user (K) to the user list to be audited (60) by the auditor (D) (1011),

   - If the auditor (D) does not think that the user (K) is risky, excluding the user (K) from the audit (1012),

   - Determining of the target correction period for the finding by the parties (1013),

   - Controlling whether the finding is corrected within the target correction period (1014),

   - Confirming and recording of the correction by the auditor (D) (1015),
- Granting a time extension if the finding is not corrected within the target correction period (1016),
- Controlling whether the finding is corrected within the time extension (1017),
- If the finding is not corrected within the time extension, sending warning messages periodically to the parties and managers until the finding is corrected (1018),
- Presence of the user (K) with no detected finding by the auditor (D) as a user (K) having been audited and having no finding in the audit report (1019).

2. The method according to claim 1 and characterized in that said method comprises the step of adding the user (K) to the user list to be audited (60) by the risky user detection module (10) if the user (K) is caught by the risky user detection module (10) (1002).

3. The method according to claim 1 and characterized in that said method comprises the step of controlling whether the auditor (D) thinks that the user (K) is risky if the user (K) is not caught by the risky user detection module (10) (1010).

4. The method according to claim 1 and characterized in that said method comprises the step of adding the user (K) to the user list to be audited (60) by the auditor (D) if the auditor (D) thinks that the user (K) is risky (1011).

5. The method according to claim 1 and characterized in that said method comprises the step of excluding the user (K) from the audit if the auditor (D) does not think that the user (K) is risky (1012).

6. The method according to claim 1 and characterized in that said method comprises the step of controlling whether the finding (50) is corrected during the audit if the auditor (D) has any finding (50) for the user (K) (1005).

7. The method according to claim 1 and characterized in that said method comprises the step of the presence of the user (K) with no detected finding (50) by the auditor (D) as a user (K) having been audited and having no finding (50) in the audit report if the auditor (D) has any finding (50) for the user (K) (1009).

8. The method according to claim 1 and characterized in that said method comprises the step of recording of the finding (50) as being corrected during the audit if the finding (50) is corrected during the audit (1006).

9. The method according to claim 1 and characterized in that said method comprises the step of determining the target correction period for the finding (50) by the parties if the finding (50) is not corrected during the audit (1013).

10. The method according to claim 1 and characterized in that said method comprises the step of controlling whether the finding (50) is corrected within the target correction period after the determination of the target correction date for the finding (50) by the parties (1014).
11. The method according to claim 1 and characterized in that said method comprises the step of confirming and recording of the correction by the auditor (D) if the finding (50) is corrected within the target correction period (1015).

12. The method according to claim 1 and characterized in that said method comprises the step of granting a time extension if the finding (50) is not corrected within the target correction period (1016).

13. The method according to claim 1 and characterized in that said method comprises the step of controlling whether the finding (50) is corrected within the time extension after the granting of the time extension for the correction of the finding (50) (1017).

14. The method according to claim 1 and characterized in that said method comprises the step of confirming and recording of the correction by the auditor (D) if the finding (50) is corrected within the time extension (1015).

15. The method according to claim 1 and characterized in that said method comprises the step of sending warning messages periodically to the parties and managers, if the finding (50) is not corrected within the time extension, until the finding (50) is corrected (1018).

16. The risky user detection method (2000) according to claim 1 and characterized in that said method comprises the steps of:

- Handling all users (K) of the department subject to the audit (2001),
- Controlling whether the users (K) have any credits being tracked in non-performing loan accounts (2002),
- Ranking of all users (K) automatically in accordance with risk criteria determined by the internal audit department (2003),
- Selecting at least 20 and at most 80 users (K) from the ordered list automatically such that it will form at least 20% of the credit risk of the audited department (2004),
- Controlling whether the user (K) is among the selected users (K) (2005),
- Formation of the list of user to be audited (60) (2006),
- Controlling whether there are at least 5 users (K) in portfolio of each portfolio manager in the department subjected to the audit in the user list to be audited (60) (2007),
- Directly accepting the user list to be audited (60) without further addition (2008),
- Existence of the user list to be audited (60) as a tab in the audit transaction module (12) (2009),
- One by one auditing of the users (K) in the user list to be audited (60) by the auditor (D) (2010),
- Controlling whether the auditor (D) has any finding (50) for the user (K) in the user
list to be audited (60) (2011),
- Marking of the user (K) as automatically audited (2012),
- Controlling of whether the auditor (D) thinks that the user (K) is risky during the audit (2013),
- Excluding the user (K) from the audit (2014),
- Adding automatic user from the ranking formed according to determined criteria such that there will be at least 5 users of each portfolio manager in the user list to be audited (60) (2015),
- Marking of the user (K) as audited in the user list to be audited (60) by the auditor (D) (2016),
- Controlling whether the credits of the users (K) are transferred to the non-performing loan accounts before the previous audit date (2017),
- Controlling whether the credit balance is among the highest 10 users (K) (2018).

17. The finding tracking method (3000) according to claim 1 and characterized in that said method comprises the steps of:
- Controlling whether the auditor (D) has any finding (50) for the user (K) (3001),
- Controlling whether the correction record is made before the completion of the audit for the finding (50) (3002),
- Controlling whether the auditor (D) confirms the correction transaction with the information and the documents (3003),
- Recording of the finding (50) to the report as being corrected during the audit (3004),
- Recording of the report to the virtual archive module (40) with the electronic signature integration (3005),
- Not operating of the finding tracking module (20) for this user (K) as there is no finding (50) input for the user (K) (3006),
- Determining a target correction period for the correction of the data (50) by negotiation between the auditor (D) and the auditee (Y) (3007),
- Controlling whether the correction action is taken within the target correction period by the branch for the finding (50) (3008),
- Controlling whether the auditor (D) confirms the correction action with the information and the documents (3009),
- Requesting time extension by the auditee (Y) (3010),
- Controlling whether the auditor (D) confirms the time extension request (3011),
- Controlling whether the correction action for the finding (50) is taken within the time
extension (3012),
- Sending of the warning messages periodically to the auditor (D) and the auditee (Y) and affiliated manager of the auditee (Y) until the finding (50) is corrected (3013).

18. The reporting method (4000) according to claim 1 and characterized in that said method comprises the steps of:
- Controlling whether the audit report is completed (4001),
- Monitoring of the report and the data (50) within the report by both the audited department and all managers of the audited department with the audit report monitoring module (31) (4002),
- Tracking of all assessments written by all departments on the basis of the finding (50) the audit detection and reporting module (32) (4003),
- Classifying the finding (50) on the basis of bank-wise/coordinatorship /regional directorate/branch and portfolio with the audit detection and reporting module (32) (4004),
- Monitoring of the number of the finding (50) detected on the basis of the audited user (K) within the frame of the classifications (4005),
- Monitoring of the risk of the finding (50) detected on the basis of the audited user (K) within the frame of the classifications (4006),
- Using the audit results obtained from the reporting module (30) in the following administrative decisions by the managers (4007),
- Monitoring of the stage of the uncompleted reports with the audit report monitoring module (31) (4008).

19. The virtual archive and electronic signature integration method (5000) according to claim 1 and characterized in that said method comprises the steps of:
- Monitoring of the audit report by the auditee (Y) from the moment it was started to be written, correction the finding (50) during the audit interactively (5001),
- Controlling whether the auditee (Y) thinks that the finding (50) is a correct/truth-reflecting finding (50) while the audit report is being written (5002),
- Finalization of the finding (50) as a result of the negotiations (5003),
- Inclusion of the finding (50) within the audit report (5004),
- Transmittance of the audit report to the auditee (Y) for replying of the finding (50) (5005),
- Re-transmittance of the finding (50) to the auditor (D) as being replied by the auditee (Y) (5006),
- Making comments for the finding (50) replies by the auditor (D) (5007),
Completion of the report (5008),
Recording to the virtual archive module (40) with the completion record automatically (5009),
Signing of the reports recorded in the virtual archive module (40) with the electronic signature and the subjective electronic signature by the auditor (D) (5010),
Negotiation between the auditor (D) and the auditee (Y) (5011),
Controlling whether the auditor (D) thinks that the finding (50) is a correct/truth-reflecting finding (50) (5012),
if the auditor (D) reach the conclusion that the finding (50) is not a correct/truth-reflecting finding (50), removal of the finding (50) from the audit report (5013).

20. The method according to claim 16 and characterized in that said method comprises the step of controlling whether the credits of the users (K) are transferred to the non-performing loan accounts before the previous audit date if the users (K) have any credits being tracked in the non-performing loan accounts (2017).

21. The method according to claim 16 and characterized in that said method comprises the step of ranking of all users (K) automatically in accordance with risk criteria determined by the internal audit department if the users (K) have no non-performing loan (2003).

22. The method according to claim 16 and characterized in that said method comprises the step of forming the list of user to be audited (60) if the user (K) is among the selected users (K) (2006).

23. The method according to claim 16 and characterized in that said method comprises the step of controlling of whether the auditor (D) thinks that the user (K) is risky during the audit if the user (K) is not among the selected users (K) (2013).

24. The method according to claim 16 and characterized in that said method comprises the step of directly accepting the user list to be audited (60) without further addition if there are at least 5 users (K) in portfolio of each portfolio manager in the department subjected to the audit in the user list to be audited (60) (2008).

25. The method according to claim 16 and characterized in that said method comprises the step of adding automatic user (K) from the ranking formed according to determined criteria such that there will be at least 5 users of each portfolio manager in the user list to be audited (60) if there are not at least 5 users (K) in portfolio of each portfolio manager in the department subjected to the audit in the user list to be audited (60) (2015).

26. The method according to claim 16 and characterized in that said method comprises the step of marking of the user (K) as automatically audited if the auditor (D) has any finding (50) for the user (K) in the user list to be audited (60) (2012).
27. The method according to claim 16 and characterized in that said method comprises the step of marking of the user (K) as audited in the user list to be audited (60) by the auditor audited if the auditor (D) has any finding (50) for the user (K) in the user list to be audited (60) (2016).

28. The method according to claim 16 and characterized in that said method comprises the step of controlling whether the credit balance is among the highest 10 users (K) if the credits of the user (K) are transferred to non-performing loan accounts before a previous audit date (2018).

29. The method according to claim 16 and characterized in that said method comprises the step of forming the list of user to be audited (60) if the credits of the user (K) are not transferred to non-performing loan accounts before a previous audit date (2006).

30. The method according to claim 16 and characterized in that said method comprises the step of forming the user list to be audited (60) if the credit balance is among the balance is among the highest 10 users (K) (2006).

31. The method according to claim 16 and characterized in that said method comprises the step of controlling of whether the auditor (D) thinks that the user (K) is risky during the audit if the credit balance not among the highest 10 users (K) (2013).

32. The method according to claim 16 and characterized in that said method comprises the step of forming the user list to be audited (60) if the auditor (D) thinks that the user (K) is risky during the audit (2006).

33. The method according to claim 16 and characterized in that said method comprises the step of excluding the user (K) from the audit if the auditor (D) does not think that the user (K) is risky (2014).

34. The method according to claim 17 and characterized in that said method comprises the step of controlling whether the correction record is made before the completion of the audit for the finding (50) if the auditor (D) has any finding (50) for the user (K) (3002).

35. The method according to claim 17 and characterized in that said method comprises the step of not operating of the finding tracking module (20) for this user (K) as there is not finding (50) input for the user (K) if the auditor (D) has no finding (50) for the user (K) (3006).

36. The method according to claim 17 and characterized in that said method comprises the step of controlling whether the auditor (D) confirms the correction transaction with the information and the documents if the correction record is made before the completion of the audit for the finding (50) (3003).

37. The method according to claim 17 and characterized in that said method comprises the
step of determining a target correction period for the correction of the finding (50) by negotiation between the auditor (D) and the auditee (Y) if the correction action is not taken before the completion of the audit for the finding (50) (3007).

38. The method according to claim 17 and characterized in that said method comprises the step of the recording of the finding (50) to the report as being corrected during the audit if the auditor (D) confirms the correction transaction with the information and the documents (3004).

39. The method according to claim 17 and characterized in that said method comprises the step of determining a target correction period for the correction of the finding (50) by negotiation between the auditor (D) and the auditee (Y) if the auditor (D) does not confirm the correction transaction with the information and the documents (3007).

40. The method according to claim 17 and characterized in that said method comprises the step of controlling whether the auditor (D) confirms the correction transaction with the information and the documents if the correction record is made by the branch within the target correction period for the finding (50) (3009).

41. The method according to claim 17 and characterized in that said method comprises the step of requesting time extension by the auditee (Y) if the correction record is not made by the branch within the target correction period for the finding (50) (3010).

42. The method according to claim 17 and characterized in that said method comprises the step of the recording of the report to the virtual archive module (40) with the electronic signature integration if the auditor (D) confirms the correction transaction with the information and the documents (3005).

43. The method according to claim 17 and characterized in that said method comprises the step of requesting time extension by the auditee (Y) if the auditor (D) does not confirm the correction transaction with the information and the documents (3010).

44. The method according to claim 17 and characterized in that said method comprises the step of controlling whether the correction record for the finding (50) is made within the time extension if the auditor (D) confirms the time extension request (3012).

45. The method according to claim 17 and characterized in that said method comprises the step of sending of the warning messages periodically to the auditor (D) and the auditee (Y) and affiliated manager of the auditee (Y) until the finding (50) is corrected if the auditor (D) does not confirm the time extension request (3013).

46. The method according to claim 17 and characterized in that said method comprises the step of controlling whether the auditor (D) confirms the correction transaction with the information and the documents if the correction action is taken for the finding (50) within the
47. The method according to claim 17 and characterized in that said method comprises the step of sending of the warning messages periodically to the auditor (D) and the auditee (Y) and affiliated manager of the auditee (Y) until the finding (50) is corrected if the correction action is taken for the finding (50) within the time extension (3013).

48. The method according to claim 18 and characterized in that said method comprises the step of tracking of the report and the finding (50) within the report by both the audited department and all managers of the audited department with the audit report monitoring module (31) if the audit report is completed (4002).

49. The method according to claim 18 and characterized in that said method comprises the step of tracking of all assessments written by all departments on the basis of the finding (50) with the audit detection and reporting module (32) if the audit report is completed (4003).

50. The method according to claim 18 and characterized in that said method comprises the step of classifying the finding (50) on the basis of bank-wise/coordination/regional directorate/branch and portfolio with the audit detection and reporting module (32) if the audit report is completed (4004).

51. The method according to claim 18 and characterized in that said method comprises the step of tracking of the stage of the uncompleted reports with the audit report monitoring module (31) if the audit report is not completed (4008).

52. The method according to claim 19 and characterized in that said method comprises the step of the finalization of the finding (50) as a result of the negotiations if the auditee (Y) thinks that the finding (50) is a correct/truth-reflecting finding (50) while the audit report is being written (5003).

53. The method according to claim 19 and characterized in that said method comprises the step of the negotiation between the auditor (D) and the auditee (Y) if the auditee (Y) does not think that the finding (50) is a correct/truth-reflecting finding (50) while the audit report is being written (5011).

54. The method according to claim 19 and characterized in that said method comprises the step of the finalization of the finding (50) as a result of the negotiations if the auditor (D) thinks that the finding (50) is a correct/truth-reflecting finding (50) (5003).

55. The method according to claim 19 and characterized in that said method comprises the step of the removal of the finding (50) from the audit report if the auditor (D) does not think that the finding (50) is a correct/truth-reflecting finding (50) (5013).
56. A step according to the previous claims and characterized in that said user (K) is a bank customer.

57. A system (1) used in the supervision of the bank employees working in the banking sector in terms of competence/qualification, the audit of the banking transaction's conformity to the in-bank and legal regulations and the supervision of the efficiency of the systems; and after the supervision, the tracking of the related correction action of the finding (50) within the audit reports within the targeted period in accordance with the audit report and said system (1) is characterized in that

- At least one risky user detection module (10) enabling the preparation of the user lists (60) to be audited, forming a basis for the audit and to be audited, using certain risk parameters and enabling the realization of the audit over the live screens,

- At least one working index module (11) comprising the user lists to be audited (60) to which the users (K) are added by the risky user detection module (10) by means of precision sampling and/or added manually in a situation arising during the audit,

- At least one audit process module (12) containing all information of the audit and the auditor (D),

- At least one in-report detection tracking module (13) enabling the display of the related audit point explanation of each user (K) whose input is made to the audit points during the audit along with the branch reply,

- At least one finding tracking module (20) systematically tracking the correction processes relating to the risky transactions subject to the audit report,

- At least one reporting module (30) rendering the work processes and their concentrations on the basis of the sub-processes and audit points of the audit finding (50) reportable without any manual transaction,

- At least one audit report tracking module (31) enabling the tracking of the all conducted audits by filtering,

- At least one audit and detection reporting module (32) enabling the tracking of the problems encountered in the banking processes and the tracking of the areas of concentration of the audit points,

- At least one virtual archive module (40) enabling the tracking of the audit reports recorded as electronically signed,

- At least one data (50) expressing incompleteness/error/violation to bank regulation or law detected on works and transactions of the users (K) audited by the auditor (D),
- At least one the user list to be audited (60) comprising the list of user (K) to be audited during the audit.
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

<table>
<thead>
<tr>
<th>INV.</th>
<th>Classification of subject matter</th>
</tr>
</thead>
<tbody>
<tr>
<td>G06Q 10/00</td>
<td>G06Q 4/00</td>
</tr>
</tbody>
</table>

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

**Minimum documentation searched (classification system followed by classification symbols)**

GG6F G06Q

**Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched**

**Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)**

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP 1 926 246 A1 (LI DONGSHENG [CN]) 28 May 2008 (2008-05-28) abstract; claims 1, 16, 18, 19, 24, 27; figures 1-4</td>
<td>1-57</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

See patent family annex.

Date of the actual completion of the international search: 21 April 2016

Date of mailing of the international search report: 07/07/2016

Name and mailing address of the ISA/European Patent Office, P.B. 5018 Patentlaan 2, NL-2280 HV Rijswijk, Tel.: (31-70) 340-2040, Fax: (31-70) 340-3016

Authorized officer: Viets, Ana
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
</table>