INTERNAL AUDIT AND ITS APPROACH TO THE RISK MITIGATION

[a]VADIM BENEŠ
Vysoká škola finanční a správní, o.p.s., Estonská 500, 101 00 Praha 10
email: [a]vadim.benes@gmail.com

Abstract: This thesis is analyzing the modern role of the internal audit in corporate (mainly banking) structures. It describes the changes made in the social role of auditing during the years and emphasizes the internal audit´s risk management function, rather than just control function. Attention is given to the methodology used, especially to the currently most widespread risk-based auditing approach. Also one of the most recent approaches to auditing – so called continuous auditing - is briefly described and the possibilities of its implementation into the risk-based framework are outlined.

Keywords: Internal audit, continuous audit, risk-based audit, compliance audit, control audit, risk management, risk mitigation, audit methodology, audit planning.

1 Introduction

The Institute of Internal Auditors defines the internal audit officially as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Internal audit in the modern sense is a relatively new but yet an indispensable part of the corporate structure of the most of large corporations. In some areas, such as banking, its existence is based on the legislative requirements. It's a logical step as the internal audit is, due to its independence, not only an internal control tool, but also a significant assistant, a partner and a point of contact for an external regulator of the banking industry. The basic principles of the cooperation between an internal audit and a regulator are described, among others, in material prepared by Basel Committee on Banking Supervision entitled Internal Audit in Banks and the Supervisor's Relationship with Auditors. According to this document, the supervisory authority should assess the quality of the bank´s internal audit and, if the evaluation goes well, it can rely on it in identification of the high-risky areas (it can use the reports of internal audit as a source of an information about the problems of internal controls in the audited areas, or on the other hand, it can focus on the risk identification in those parts (processes) of the bank, where the audit was not conducted for a long time)). Supervisor and internal auditors should also arrange regular meetings and discussions related either directly to individual banks or only common, sector-wide issues.

This thesis is trying to analyze the modern role of internal audit in corporate (mainly banking) structures and gives a special attention to the methodology used. It also tries to bring the new insight into risk-based auditing by implementing principles of continuous auditing into risk based framework.

2. The social role of the internal audit and methodological approaches to its process

The various trends and opinions on the appropriate work content of internal audit and its social roles over time are not strictly separable. These trends are influenced by economic and social characteristics of the time and largely overlap each other. A characteristic feature is also a fact that these trends do not necessarily exclude each other. In general, without the strict categorization, it can be seen that in the last 70 years there was a shift in the understanding of the role of the internal audit from a kind of “external audit addition”, dealing only with the financial indicators, over the assessment of the effectiveness of controls, to the audit of complex processes and finally to the role of consultative business partner and a provider of continuous and comprehensive assurance on the internal risk environment. Perhaps with the exception of the first-mentioned approach, it can´t be said, that the internal audit as we know nowadays, does not fulfill the task.

The aforementioned trends in the economic and social role of internal audit are followed by the development in the methodological bases for which more strict classification is possible. The main methodological approaches specific for the internal audit are the compliance based auditing (sometimes also referred as a control based or transaction based) and risk based auditing (RBA).

2.1 Compliance / control based audit

Compliance / control based audit is the basis of methodology of internal audit. In essence it is the one of the first methodological approaches that can be considered as specific solely for internal audit (considering the modern understanding of the concept of internal audit). As its name suggests, it deals primarily with an assessment of compliancy of internal activities with the internal methodology or regulatory measures and also with the control functionality and the control implementation in accordance with the methodology or regulations. This assessment is done through the testing of individual transactions within the institution.

The drawback factor of this approach is that while assessing the existence and effectiveness of the controls, it does not examine its global impact or significance and motivations leading to its implementation. Compliance audit is therefore unable to determine whether the area is overly controlled. Compliance audit also does not concern about the rules itself; therefore it does not assess its ability to reduce risks. It is thus theoretically possible that in the audited area there are a number of risks not covered by valid methodology and required controls, and audit still does not consider this area as problematic.

The last, but not insignificant problem of this approach is that it is largely based on the transactional principle (as already mentioned, sometimes the whole methodology is called "transaction based"). This is reflected in the absence of a global perspective. Output of compliance audit can sometimes provide only sketchy information about the company's internal processes (e.g. considering an area of consumer credits, the process is not viewed as a whole - from the initial contact with the client, to the repayment, or collection process, but only as the single transaction or control – e.g. the presence of the client signature on the contract is checked etc.).

2.2 Risk based audit

At present, it is clearly the most frequently applied approach to the implementation and run of internal audit. This popularity is based on both a natural progression - a shift in the role of internal audit from a purely supervisory role to the role of risk-preventive tool - as well as on number of regulatory requirements – e.g. in the Czech banking sector the regulator´s decree on prudential rules for banks requires (although indirectly) to use risk-based principles in auditing when declares, that that the planning and scheduling of capacities of internal auditors is based on the risk analysis. The risk analysis performed before starting the audit work is the cornerstone of the risk-based methodology. Based on this analysis the capacities of audit teams are then redistributed with primary intention to cover the most risky areas. Individual audits are no longer run based on regular time schedule, but based on risk weights assigned to the individual areas.

Another important element of RBA is the preference of a process approach. In the literature (e.g., Griffiths (2005)) the process based audit (sometimes also known as systemic or process-systemic) is sometimes considered as a separate audit methodology. But such approach is not entirely correct. Process audit cannot be seen as a separate methodology, but as a necessary part of the risk-based auditing. As mentioned by

Stanciu (2008), risk doesn't recognize organizational charts. It doesn't confine itself to functions and units, processes and roles; it travels through the bank in an interdependent and connected way. It is therefore not safe to practice risk management on an exposure-to-exposure: risks must be recognize and managed holistically across the entire bank. Therefore, if the RBA should run effectively, it has to be applied in the process way.

What precisely does the term process approach mean? As the name suggests, the fundamental principle of process based auditing is the analysis of complex processes and systems rather than individual transactions or process parts – considering the case of consumer credits area, all the steps involved in the process of granting, approval, drawing and repayments or collections and recovery are analyzed throughout the entire bank, not only in relation to one branch (if the sample of cases from one branch is used during the testing, the conclusions are then generalized and applied on the entire bank).

But even though the process approach is strongly advised, some examples of the non-process approach to the RBA can also be found. Sharma (2004) defines it as a risk-focused internal audit and describes it on an example of the bank which divides its branches into three categories according to the amount of income produced. The riskiness (and related remedial measures like the frequency of audit inspections) is then assigned to particular branches based on this income amount.

However, as mentioned before, if the risks should be comprehensively analyzed, it is highly advisable to perform audits in the process way as it is more transparent, comprehensible and it gives an better assurance, that none of the risks was omitted due to the fact that it fell "somewhere between the focus" of the parts of the non-process audits.

The most ideal case, however, is not the use of the RBA only. It is the combination of both the RBA and compliance/transaction-oriented audit. In such a case the audit of the transactions works as the internal part of the RBA allowing a more accurate estimate of the riskiness of individual processes. This combination, however, is very costly, as the number of auditors needed logically rises (part of audit staff has to be assigned to conduct RBA, part to conduct compliance audit) and the implementation of the transaction principles into the audit process is very time consuming. The possible solution of this problem is the introduction of so called automatic or continuous auditing. This solution will be further discussed later in the text.

Besides the approaches mentioned above, there are several others, less important or strongly sector-specific. Wynne (2004) mentions the example of a pre-payment audit consisting of control of payment documents just before the related transaction is carried-out (in essence, this is a form of ex-ante compliance auditing). Another approach, mentioned e.g. by Lonsdale (2000) is a value-for-money auditing, dealing mainly with assessment of the effectiveness and costs at which the institution (usually a government - but not exclusively) manages the resources entrusted. Rattliff et al. (1996) mentions a performance audit, focused on the efficiency and effectiveness of the company (although this area falls within the scope of controlling, rather than audit), quality audit and audit of financial controls (including control of accounting and financial indicators).

3. Basic principles of risk management via risk based auditing

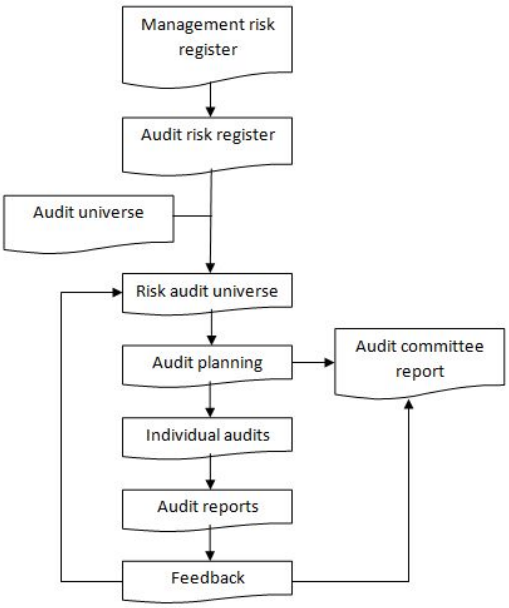
Application of the principles of the RBA is reflected both in the planning and running phase of audits.

3.1 Planning in the process of RBA

The basic requirement for the RBA is the existence of the Audit Universe (AU). This consists of a list of all auditable actions and activities assigned to the audited entity. This list is then the primer basis for the subsequent risk assessment and preparation of the risk-based audit plan.

In literature (e.g. Griffiths 2006), the requirement for additional register can be found - the register of risks identified by the management of business departments. This risks identified by business should be afterwards assigned to particular actions and activities registered in the AU. In practice, however, the requirement for a risk register is stated differently - the risk management system is divided into three parts (or sometimes called three lines of defense) - the first part is the management of individual business units which is required to identify the risks associated with the processes in its responsibility and also manage some basic risk-related tasks (e.g. establishing the job position of a local risk managers). The second part, consisting of specialized risk management departments and other individual risk-management functions is working with risks identified by management (of course not only by them). The third part is mainly control focused and it is provided by the internal audit dept. One of the most important conditions of the successful operating of the audit work is the auditors´ independence. In order not to jeopardize it, it is necessary for the audit to run its own risk map. There are many reasons for such an individual approach - the management of business units may not be able to identify all the risks associated to the activities within its competence (one can consider some "professional blindness" or the management may not always be motivated to reveal all the risks, as such a reveal can bring more attention of auditors). The risks of activities recorded in the AU should thus be determined directly by auditors and risk management registers should be considered only as the one of the sources used while determining the risks.

Scheme 1: RBA process



Source: own arrangements

After assigning the particular risks, the individual activities are grouped into so-called auditable units (e.g. retail loans, asset-liability management, subsidiaries, etc.). These units are then evaluated in terms of risks and materiality.

At first, the inherent risks are analyzed (IR - the risk based on the very nature of the activity, measured before application of controls). Also the controls risk is analyzed (the risk rising from inefficiency of controls applied). The inherent risk analysis involves classical groups of risks e.g. market risk, credit risk, operational risk, reputational risks, legal risk etc. The length of the period since the last audit performed can be also involved as one of the parameters. These risks are evaluated based on auditor´s professional judgment for each activity involved in the given auditable unit. Usually the scale of 0-5 is used, but direct verbal classification is also possible.

Table 1: Assessment of inherent risk of auditable unit

Auditable unit Retail Credits	Credit risk	Market risk	Operational risk	Reputational risk	Total
Client´s identification	5	1	3	1	10
Client´s registration	3	1	5	1	10
Evaluation of the request by the system	2	1	1	1	5
Evaluation by the underwriter	4	1	3	3	11
Overall IR score for the whole unit	9				

Source: own arrangements

The total score for the inherent risk of auditable unit is then calculated as the average of risk values of all the activities included in the unit. This numerical value is then (based on the risk scale) transferred into verbal classification (low, medium, high).

Besides this approach, requiring a relatively detailed breakdown of auditable units, it is also possible to use the less detailed approach consisting of a direct evaluation of individual risk categories of the auditable unit (i.e. without the necessary breakdown). The total value of IR for auditable unit is then simply given as a sum of individual risks values.

The control risk is analyzed in the similar way. The analysis consists of the evaluation of the quality of the internal control, management approach to risks etc. The scores of the control and inherent risk are then recorded into frequency matrix, which determines the required frequency of audits in aforementioned auditable unit. (1 – yearly; 4 – each four years).

Table 2: Frequency Matrix

		Control risk		
		Low	medium	high
Inherent risk	low	4	4	3
	medium	3	3	2
	high	2	1	1

Source: own arrangements

The IRB methodology in general requires the main focus of auditors to be set on the most risky areas of the company. This, however, does not mean that the riskless, less-risky or less significant parts of the company should be completely omitted. The minimum frequency at which control of the less significant departments should be evaluated depends entirely on the decision of the company. The optimal frequency is considered to be about 4-5 years.

Besides the above mentioned approach using the frequency matrix, there are many other ways how to approach the risk-based planning. One of them is a simple comparison of overall risk scores of particular units. In this case, the numerical values of the inherent and control risk are not transferred to the verbal evaluation, but are added together. Total risk score is then recorded to Risk Audit Universe and the resources are allocated according to the risk score order. The advantage of this approach is, in addition to its simplicity, the fact that it allows direct comparison of the annual values of the total risk. The growth of this value should then have consequences in the shortening of the audit period.

During the analysis of inherent risk also one of its most important parameters is assessed - the materiality (significance) of impact of its realization. In case of verbal evaluation, the effect of materiality may be added by simply decreasing or increasing of the evaluation level (e.g. by lowering the riskiness from medium to low).or the IR score (before the transformation to verbal evaluation) can be multiplied by the materiality weights. In case of pure numerical evaluation, the materiality coefficient is simply added to the overall risk score

3.2 Principles of the RBA during the audits´ run

The principles applied during the audit planning phase are applied also in the actual course of individual audits. The difference here lies in the fact that while in the planning process the risks are assessed in relation to the auditable units and processes, during the run of particular audits, the evaluation is done on activities level.

Again, there is the inherent and the control risk assessment involved. Risks taken from the Risk Audit Universe (or added to the process directly by the auditor) are recorded in the Risk Matrix and evaluated in terms of likelihood and size of potential impact.

Table 3: Evaluation of inherent risk

Source: Griffiths (2006); customized

The table of the inherent risk assessment assumes the numerical assessment on scale of 1-5 and risk appetite set on level 4 (i.e., if the overall inherent risk score will be less or equal to 4, the risk will be, in order of efficiency, considered as irrelevant for the additional audit testing). The rest of the risks will be involved in standard audit testing procedures. In ideal case, the implemented control will be sufficiently effective to lower the residual risk score below the 4. If it isn´t, the written recommendation to the management of related business unit is formulated in the final audit report. Based on the residual risk score, the priorities are assigned to the particular recommendations. After the final report publication, the follow-up phase of the audit is started (the evaluation of recommendations fulfillment).

4. Continuous auditing as the direction of future development of internal audit

The RBA is now clearly most widely used methodology of internal audit. But the development in IT area has its effects also in the audit domain. This trend is mostly evident in the development of so called automatic or more often continuous auditing (CA). The theoretical origins of this tool can be dated back to the mid-nineties. In practice, the first attempts to implement CA appeared at the turn of the century.

Continuous auditing is defined by Kogan et al. (1999) as the type of auditing that produces results at the same time or within a short interval after the event occurs. The Institute of Internal Auditors defines continuous auditing as an automatic method

used for valuation of risks and controls at regular (frequent) basis.

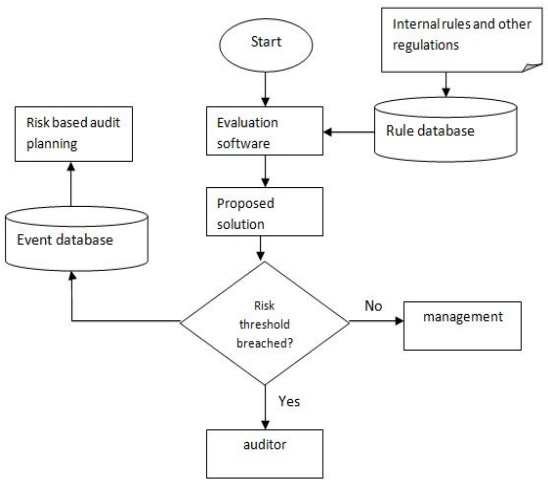
In essence, it is not a separate audit methodology, but one of the practical applications of the transactional audit methodology. As mentioned above, the transactional or compliance based audit is a bit outdated methodology. The main goal of current auditing is not a detailed analysis of individual transactions, but rather risk-based view on the audited area. Despite all this, there are still areas, primarily related e.g. to the regulator reporting, where the use of a transactional approach remains important (risk here derives mainly from penalties for fail for inaccurate reporting to regulatory authorities). It is also possible to implement some risk-based principles into the process and also to use its outcomes as a basis for further RBA planning.

The process of the continuous auditing is largely a technical matter. Significantly lower interest of both academics and practitioners is focused on its implementation into the audit, or risk-management frameworks in general. Even though it is mainly a transactional audit, it is possible to incorporate in it some of the RBA components (mainly in relation to dealing with its outcomes). The most of continuous audit procedures are based on a rule-based method. Less frequent (mentioned for example by Lee (2007)) is a case-based method, introducing the elements of the precedent into the process of the continuous auditing by comparing individual transactions with pre-set precedent cases and subsequent application of precedent remedial actions (in case of LEE mainly repressive).

The rule based method is based on the setting of the clear rules derived from the internal methodology or regulatory rules, and its registration in special database (rule database). The ongoing transactions are then assessed by the specially designed software in sense of compliancy with rules registered in the rule database. In case that the transaction violates some of the rules, the report is generated and the auditor is immediately informed about the transaction.

As already mentioned, it is theoretically possible to include some limited elements of the RBA into this process – this could be done by setting a limit (in sense of amount or materiality of rule breached) for erroneous transactions, corresponding to the risk appetite of the company or the audit department. In case that the erroneous transaction amount is below this threshold, only the business management is informed. Otherwise (serious violations or the transaction above the limit) the auditor is informed. In both cases these incidents should be recorded in detail - both for possible use for case-based identification, or as one of the important risk estimation inputs for the subsequent risk-based audit planning

Scheme 2: The process of rule-based continuous audit with the risk-based elements involved



Source: Own arrangements

The procedure above is one of the possible forms of the assurance based audit, mentioned e.g. by Griffiths (2005) as one of the most innovative approaches to provide a comprehensive audit control. Along with continuous monitoring from the business side, this combination represents a very effective internal control framework. Despite above mentioned the continuous auditing is still very rarely used approach in practice. Barrier of larger expansion of CA can be found in insufficient information availability – there are a number of theoretical papers on the continuous auditing and there are also a number of practical manuals, but most of these are strongly IT orientated. But the main users of such system do not recruit from academics or IT professionals – they are just standard auditors and from their point of view there is still a large information gap.

There are also some limitations in practical point of view – especially in data availability area. The continuous auditing requires access to transactional systems´ data flow and such a connection is very difficult to establish. The costs of such implementation are also one of the important factors preventing the CA growth.

5. Conclusion

Internal audit in the modern sense is a relatively new but rapidly developing profession. This is caused by the large expectations from both regulators and management of audited companies.

The methodological approaches to audit work are changing during the time, but the main trend is set in direction of the risk related and process based matters rather than on rules compliancy. This is also reflected in the currently most applied methodology – risk based auditing. In this essay the RBA methodology was analyzed and some future perspectives were outlined – mainly in relation to the implementation of continuous auditing into Risk Based structures. The continuous auditing, even though representative of a bit outdated compliance/transaction based auditing, could bring significant improvements into the RBA approach. Nevertheless, there are still barriers in the way to its wider implementation – mainly related to data availability. This, however could change while e.g. old, incompatible transactional systems in banks are gradually replaced by the new, more suitable ones. The monitoring-net consisting of the management reporting, continuous auditing and RBA as presented here, represents one of the most suitable the future of auditing and risk management.

Literature:

1. Griffiths, D.: *Risk Based Internal Auditing. Three Views on Implementation*. 2006. Available at: < http://www.internalaudit.biz/files/implementation/Implementing%20RBIA%20v1.1.pdf>
2. Griffiths, P.: *Risk-Based Auditing*. Gower Publishing Limited, 2005. ISBN 0-566-08652-2
3. Kogan, A; Sudit, E; Vasarhelyi, M.: *Continuous Online Auditing. A Program of Research*. 1999. Available at: <http://accounting.rutgers.edu/MiklosVasarhelyi/Resume%20Articles/MAJOR%20REFEREED%20ARTICLES/M21.%20cont%20online%20auditing%20program%20of%20research.pdf>
4. Lee, G. *Rule-Based and Case-Based Reasoning Approach for Internal Audit of Bank*. 2007. Available at: < http://www.deepdyve.com/lp/elsevier/rule-based-and-case-based-reasoning-approach-for-internal-audit-of-UmNQpwyfc4>
5. Lonsdale, J.: *Developments in Value-For-Money Audit Methods: Impacts and Implications*. 2000. Available at: <http://ras.sagepub.com/content/66/1/73.full.pdf+html>
6. Rattlif, R; Wallance, W; Summers, G; McFrland, W; Loebbecke, J.: *Internal Auditing Principle and Techniques.* The Institute of Internal Auditors, 1996. ISBN 978-0894133268
7. Sharma, G.*: Risk Based Internal Audit in Banks*. 2004. Available at: <http://220.227.161.86/10931p1057-66.pdf>.

8. Stanciu, V.: *Internal Audit Approach in Banks*. 2008. Available at: <http://anale.feaa.uaic.ro/anale/resurse/016_F13_Stanciu.pdf >
9. Wynne, A.*: Pre-payment checks, compliance audit or risk-based audit what is the most effective role for internal audit?* 2004. Available at: <http://www2.accaglobal.com /doc/publicsector/ps_doc_014.pd>

Primary Paper Section: A

Secondary Paper Section: AH