J Manag Gov (2009) 13:101–130
DOI 10.1007/s10997-008-9072-7

Risk based internal auditing within Greek banks: a case study approach

Andreas G. Koutoupis · Anastasios Tsamis

Published online: 1 October 2008

Abstract Internal Audit functions within Greek banks are imposed both by the Greek law for publicly listed enterprises (Law 3016/17.5.2002), as well as by the Bank of Greece (Bank of Greece Governor's Act. Number 2577/9-3-2006). Based on the traditional approach of internal audit within Greek Banks, an inspection of branches and credit on a tick and check (compliance) basis was conducted. Recent research (Koutoupis and Tsamis, Fourth European Academic Conference on Internal Audit and Corporate Governance. Cass Business School, London, United Kingdom, 2006) comes to a conclusion that this approach does not result in adequate coverage of risks. In addition, new international regulations and best practices such as basel committee on banking supervision requirements, COSO enterprise risk management (ERM) suggested framework, as well as The Institute of internal auditors standards for professional practice of internal auditing (standards) were in most cases partially or fully ignored by the vast majority of Greek banks. However, minimum requirements regarding the operation of internal audit functions have been set up by the Bank of Greece, which in most cases are followed by the Greek banks, as well as periodically assessed by the above banking regulator. Risk based internal audit (RBIA) was an unknown concept for the vast majority of publicly listed and non-listed Greek enterprises until very recently. Only Greek subsidiaries of US and UK enterprises were aware of the RBIA audit concept (including big foreign banks which operate in Greece as subsidiaries), as they were periodically audited by group audit functions as an immediate result of relevant risk assessments. Also, the majority of Greek publicly listed enterprises use the audit cycle approach in developing their long term (3 year) and annual audit plans, which means that they

A. G. Koutoupis (✉) · A. Tsamis
Department of Public Administration, Auditing & Taxation Sector, Panteion University of Social and Political Sciences, 268 Kifisias st., Chalandri, Athens, Greece
e-mail: andreas.koutoupis@gr.pwc.com

A. Tsamis
e-mail: tsamis.a@emporiki.gr

audit specific business cycles and activities within a predefined time interval (1–3 years). Audit planning is based on the head's of internal audit and internal auditors experience without formal application of risk assessment and audit planning techniques. All Greek banks that participated in the corporate governance and internal auditing survey (Koutoupis, Third European Academic Conference on Internal Audit and Corporate Governance, 2005) stated that they follow a risk-based audit approach and develop risk based audit plans; however the vast majority of them could not prove it through a clearly documented risk assessment and risk-based audit plan. Sarbanes–Oxley Act (2002) directed National Bank of Greece to adjust its audit planning process to a risk based one. Also, other big Greek banks (case study 1–3) are now either considering or adopting a RBIA approach, mostly because of Bank of Greece pressures. internal audit functions within small banks still follow the audit cycle approach. In this paper, current status of Greek banks RBIA approach will be discussed based on relevant references, as well as on three case study examples. This research will be based on relevant literature review, as well as authors' professional experience in past and current projects related to risk assessment, audit planning and RBIA. Specifically, RBIA approach will be critically evaluated based on three big Greek banks analysis on a case study format and benchmark against basel requirements, ERM and standards for professional practice of internal auditing. Based on the relevant assessment, best practices and recommendations for improvement will be identified.

Keywords Audit cycle approach · Audit planning · Bank of Greece · Basel requirements · Compliance · COSO · Enterprise risk management (ERM) · Greek banks · Internal auditing · Internal controls · Risk assessment · Risk based internal audit (RBIA) · Standards for the professional practice of internal auditing (standards)

Abbreviations

ERM	Enterprise risk management
CAEs	Chief audit executives
RBIA	Risk based internal audit

1 Introduction and research objectives

Internal Audit functions within Greek banks have started shifting roles and responsibilities during the last three years due to increased requirements by Bank of Greece (the Greek financial services regulator) and other best practice bodies such as COSO committee, basel committee, as well as local corporate governance laws and regulations. The traditional approach of internal audit included mainly the inspection of branches and loans based on a tick and check (compliance) approach.

All Greek banks which participated in a recent internal auditing survey (Koutoupis 2005) stated that they follow a risk-based approach and develop risk based audit plans; however the vast majority of them could not prove it through a clearly documented

risk-based audit plan. In fact, all banks consider risks informally when developing the long term (if applicable), and annual audit plans. However, this is based in most of the cases on relevant experience (Auditors view of risk, past audits, time elapsed since last audit, fraud events, etc.) and not based on the modern risk based audit theory and practice.[1] Moreover, the development of a long-term audit plan covering all components of the audit universe was not evidenced and documented.

The above research results leaded us to the development of this case study approach on RBIA. The goal was to assess the current risk assessment and audit planning approach followed by three major Greek Banks as a mean to evaluate the advantages and disadvantages, and highlight relevant best practises. Sarbanes Oxley Act (2002), Combined Code—UK (1998) and basel requirements are stressing the need for establishing adequate and effective risk management systems. Moreover, relevant control frameworks have been developed as a response to relevant risk assessment and risk-based audit requirements (the most famous is COSO due to Sarbanes–Oxley provisions).

Currently, the above best practice requirements are not applicable for the Greek banks, except from those requirements set by Bank of Greece, which are not always in accordance with standards for international practice of internal auditing (Standards 2004). Greek banks with the exception of foreign big banks subsidiaries have not realised the benefits of adopting risk assessment and risk based audit frameworks.

The main objective of this study is to stress the importance of the adoption of RBIA methodology towards an improved audit planning process for internal audit functions in Greek banks. This study will provide Greek banks internal audit functions with recommendations for improvement in order to apply RBIA concept and methodology towards adequate and effective audit planning.

Accordingly, the main research objectives of this paper have as follows:

- To assess the impact of Bank of Greece and other regulators in relation to the application of RBIA methodology within Greek banks internal audit functions, as well as to assess the impact of best practice bodies such as Basel, COSO and the standards for the professional practice of internal auditing to the adoption of RBIA methodology by internal audit functions.
- To examine the relationship of enterprise risk management (ERM) methodology with RBIA methodology as implemented within Greek banks.
- To evaluate the audit planning process in Greek banks internal audit functions. To evaluate how bank members of the board of directors, audit committee members and senior management influence the audit planning process and how chief audit executives (CAEs) perform audit scoping based on empirical or methodological risk assessment.

In order to identify best practices and areas of improvement, three major Greek banks internal audit functions will be assessed as a mean to refer to the advantages and disadvantages of each approach. Specifically, case study 1 sample performs audit planning based on audit cycle approach; case study 2 sample develops audit

[1] For more about Risk based internal auditing (RBIA), see *Risk Based Internal Auditing (Position Paper)*. The Institute of Internal Auditors, UK and Ireland, August 2003.

plan based on a high level risk assessment linked to audit universe, and case study 3 sample adopts risk based audit planning.

2 Research methodology

2.1 Introduction

Risk based internal audit (RBIA) is a relatively new best practices methodology for Greek banks internal audit divisions. Current trends of corporate governance and risk management have affected significantly the role of modern internal audit. Traditionally, banks internal audit divisions practices included a tick and check approach; they used to perform compliance audits focusing mainly on branches and not focusing on other high risk areas such as treasury, or risk management.

The adoption of RBIA according to best practices should provide assurance that:

- Business risks are identified, evaluated and treated in a consistent and continuous way.
- The system of internal controls and the ongoing management monitoring activities over internal controls are well designed and operate effectively, efficiently and economically in managing those risks according to directions provided (or approved) by the board of directors.

In other words, internal audit needs to focus on risks, rather than compliance activities using a cyclical approach (i.e. audit all activities in a predefined period without focusing on risks).

This chapter includes relevant literature review, as well as the case study method that researchers followed. Firstly, it describes the main sources of data used for this study, and then explains and describes the types of data used and how these have been gathered. Therefore, this section describes how the research field study was carried out, the type of data used, and the research approach that followed.

Three case studies were developed in order to identify advantages and disadvantages for each one of the methods adopted by the relevant banks. The first case refers to a new internal audit division which does not use risk based audit concept at all. The second case refers to an internal audit division that develops the audit plan based on a basic risk assessment and other risk related factors. The third case refers to an internal audit division that makes use of a comprehensive RBIA approach.

2.2 Literature review

Very few academic papers (at the best of knowledge) have been developed addressing RBIA. Literature review includes risk assessment and audit planning chapters in several relevant books (for specific information see section 'References'). Literature review was based on the Institute of Internal Auditors (The IIA-Inc.) material (mainly the latest edition of Standards for professional practice of internal auditing, 2004), basel committee recommended practices on internal auditing, and COSO enterprise risk management (ERM) methodology. Finally, an

extensive research was made on PricewaterhouseCoopers relevant publications and resources on risk assessment and audit planning methodologies, as well as relevant internal audit and risk assessment manuals and reports.

2.3 Research setting

This study focuses on the evaluation of RBIA approach within three big Greek banks. Each selected bank internal audit division represents different risk assessment and audit planning practices. Case study 1 represents the vast majority of Greek banks internal audit divisions and includes those that do not adopt RBIA practice at all. Case study 2 represents those internal audit divisions that either state (however not documenting) that they adopt the RBIA approach, or internal audit divisions that adopt a high level approach on developing audit plans based on a relevant risk assessment. Finally, case study 3 represents internal audit divisions that have fully adopted the RBIA approach. Furthermore, the researchers will assess the impact of basel requirements, COSO ERM framework and the standards for the professional practice of internal auditing to them.

2.4 Sources of information

Qualitative research has been carried out to address the research topic, using primary and secondary data. The focus is both on the primary and secondary sources of information. The primary sources of this study are the professional experience of the authors in the field of internal auditing and compliance within banks, especially the participation as consultants in risk assessment and audit planning activities, as well as compliance monitoring, whereas secondary sources are the books, the relevant working papers, and suggested sources of internal auditing banking proposed practices.

The sources of information that have been used as a basis for the theoretical and analytical part of the study are described below.

2.4.1 Primary sources of information

Professional experience of the authors in all banks that constitute the case study sample, as well as the advanced knowledge with respect to risk assessment and audit planning practices of the industry. Professional experience is demonstrated through participation in a number of relevant projects. Also, relevant risk assessment, audit planning and internal audit questionnaires, checklists, manuals and reports for a number of clients have been used.

2.4.2 Secondary sources of information

1. Academic, professional journals and publications: *International Journal of Auditing, Internal Auditor, Internal Auditing, Managerial Auditing Journal, Accounting & Business Research, Harvard Business review, McKinsey Quarterly, Journal of Finance, Management Accounting*;

2. Participant banks' annual reports and other related published data;
3. Web site information;
4. Codes of best practices (mainly COSO ERM suggested framework and basel committee suggested best practices);
5. PricewaterhouseCoopers clients databases (my client and TeamMate audit management system databases, knowledge exchange, banking network of excellence and global best practices).

All the selected banks are publicly listed in the Athens stock exchange (ASE), are very large in terms of capitalization and revenue, and attract attention from domestic and foreign investors, both institutional and individual. The researchers used self-selection as the process to gather credible and adequate sample.

The aforementioned sources have produced a number of references that are included in the bibliography. As far as possible the included references have been read, the abstracts inspected and any relevant book reviews noted.

2.5 Case studies development

As stated before, case studies were selected as they constitute a representative sample. Specifically, in all cases an examination was made to the following factors:

1. *Defining the audit universe*—For all case studies the paper refers to practices that internal audit divisions follow in order to define the bank's audit universe (i.e. all potential audit or consulting nature type projects including the assessment of central divisions, branches, subsidiaries locally or internationally including other activities that are considered risky).
2. *Risk assessment*—Risk assessment includes the procedures that internal audit divisions use in order to identify and evaluate main and secondary risks related to audit universe on an inherent and residual level and based on their impact and likelihood to the achievement of relevant objectives.
3. *Scoping*—This section refers to practices related to prioritization of risks that are linked to specific areas included in the audit universe.
4. *Audit planning*—In this section attention is paid to audit planning considerations such as selection of areas to be audited, available audit hours, resource requirements and limitations and resource allocations per selected audit area.

3 Audit planning issues within Greek banks—regulatory issues and best practice requirements

Modern internal audit requires effective, efficient and economic audit planning as a mean to achieve set audit objectives both in terms of appropriate risk and control coverage. Adequate audit planning requires effective risk assessment which will allow auditors to focus on truly high risk areas. According to enterprise risk management framework (COSO 2004), risk is any event that could prevent an organization from achieving its objectives.

Risk assessment consists of risk identification and risk analysis. Risk identification includes examining external factors such as technological developments, competition, economic changes, etc. and internal factors such as personnel quality, entity's nature of activities, the characteristics of information system processing, etc. Risk analysis involves estimating the significance of risk, assessing the likelihood and impact of the risk occurring, and considering how to manage risk.[2]

Risk assessment allows internal audit functions to consider how potential events might affect the achievement of bank objectives. The risk assessment process begins by defining the audit universe. The audit universe includes all central divisions, branches, business units, subsidiaries, special projects, special investigations and other compliance related projects (i.e. corporate governance related projects).

Evidence from a recent research (Koutoupis 2005), demonstrated that the vast majority of Greek banks do not follow a documented risk-based approach, and development of risk based audit plans; however all of them state that they are taking into consideration the assessment of risks. In fact, all listed Greek banks internal audit divisions state that they consider risks when developing their long term plan (if applicable) and annual audit plan; however, this is based on relevant experience (auditors view of risk, past audits, time elapsed since last audit, fraud events, etc.) instead on the modern risk based audit theory and practice.[3]

This paper with the use of three case studies will examine all current practices with respect to risk assessment and audit planning in Greek banks internal audit divisions. *Performance standard 2010* (Standards 2004) requires the chief audit executive to establish risk based audit plans to determine the priorities of the internal audit activity, consistent with the organizational goals. However, principle 11 of basel internal audit in banks and the supervisors' relationship with auditors require banks not to exclude any activity from the scope of audit,[4] which effectively means that all activities should be audited in a predefined minimum time interval. With respect to risk assessment and audit planning paper, basel requires an audit plan to be developed based on a relevant risk assessment which will include the timing and frequency of planned internal audit work. An important step is that risk assessment methodology should be written and appropriately followed by internal audit division. It should also include all bank's activities and entities, as well as other assignments within a reasonable time period (e.g. within three years).

Finally, Greek regulatory framework (i.e. Bank of Greece Act 2577/9.3.2006 and Corporate Governance Law 3016/17.5.2002) requires specific audits to be included within banks annual audit plan; however it does not require specifically risk based audit planning, although it is informally recommended (i.e. through the audits performed by the regulator to banks).

In the following chapters risk assessment and audit planning methodologies will be analyzed in three representative cases which will assist in identifying advantages

[2] *Enterprise Risk Management Framework.* USA: Committee of Sponsoring Organizations (COSO), 2004.

[3] For more about Risk Based Internal Auditing (RBIA) see *Risk Based Internal Auditing (Position Paper).* The Institute of Internal Auditors, UK and Ireland, August 2003.

[4] *Basel Committee on Banking Supervision: Internal Audit in Banks and the Supervisors Relationship with Auditors.* Basel: August, 2001, pp. 9–10.

and disadvantages for each approach, as well as recommending specific risk assessment and audit planning approaches.

4 Case study 1

Although the bank assigned as case study 1, was founded early in the 20th century, only after obtaining universal banking license by the regulator (i.e. Bank of Greece), it established a comprehensive internal audit function. Until then it had established a branches inspection division with limited internal auditing responsibilities.

Currently, internal audit division consists of 25 internal audit managers, staff and consultants covering the whole audit universe of the bank. The internal audit division has not adopted a systematic risk assessment approach, as well as not developed risk based audit planning. Therefore in the following lines, the methodology adopted to develop an audit plan will be presented.

The purpose of internal audit division is to assess the audit needs of the bank in order to prioritize them so that the annual audit plan is prepared. Internal audit division's goal is to cover audit universe within three years.

4.1 Defining the audit universe

In order to assess the audit needs of the bank and prepare the audit plan, internal audit division initially identifies bank's business activities taking into consideration all the main risks that might affect the entity's smooth operation.

4.2 Risk assessment

Regarding the assessment of the audit needs, some very important parameters were assessed in order to determine the scope and type of audits more effectively.

The last year audit planning analysis of the data gathered has shown that:

1. About 45% of the total number of branches were auditing before 2005.
2. A significant number of central divisions (90%) have never been audited by the internal audit division.

Based on the above findings, "*time interval elapsed since last audit*" was considered the most important factor regarding the assessment of the audit needs of 2006.

Therefore in the preparation of the annual audit plan greater importance was given to the audit of branches network and in particular of the branches that had not been audited for a long period.

4.3 Audit scoping

The main objectives of the relevant audit scoping included the following quantitative goals:

- Fifty branches of case study 1 sample, which were not auditing during the previous year (2005), will be audited. The scope and type of the audit is analytically explained at the qualitative goals;
- Audits performed by experienced personnel, will be conducted in the following high risk divisions (high risk description is based on internal audit division experience):

  1. Treasury division
  2. Information systems division
  3. Financial operations division
  4. Consumer loans division
  5. General services division (procurement sub-division)

4.4 Audit planning

Important prerequisite in order to adequately perform the audits in the first three divisions is the employment of at least three experienced internal auditors during the first quarter of 2006, which have adequate and relevant audit experience in the fields of treasury (dealing room), information systems and financial operations (accounting department).

The audit of the last two divisions will be conducted by personnel of the bank, which will become members of the internal audit division after receive relevant training.

In addition, audits will be conducted in credit cards sub-division and non-performing loans subdivision.

5 Case study 2

The purpose of case study 2 was to assess the audit needs of the bank, with primary goal to update, and prioritize them so that an audit plan is developed for internal audit division (annual and three year audit plan). The bank's primary goal was to cover all audit areas within three years with the assistance of an external audit firm—advisor.

The bank internal audit division for this project used a risk assessment software tool, which has the capability to produce multiple risk graphs for every activity, and to connect them with the relevant hours needed to audit each one of them.

5.1 Defining the audit universe

In order to assess the audit needs of the bank in case study 2 and develop the audit plan, business activities were initially identified taking into consideration all the main risks that might affect the entity's activities and objectives.

Analysis of the organizational structure has shown that the business activities of the bank include 27 central divisions, 458 branches, and 13 subsidiaries with more

than 50% shareholding. In addition of the activities directly associated with the organizational structure, activities associated with special projects taken up by internal audit division were identified, as well as compliance projects with respect to compliance with regulatory authorities (i.e. Bank of Greece and capital markets commission).

Main activities of central divisions and subsidiaries were also identified so that there is a clearer depiction of the organizations activities and the risks associated to them.

5.2 Risk assessment

In this stage, the primary risks related to the bank and its activities, and those directly related to the strategic goals of the bank, were identified. With enterprise risk we refer to the possibility that an event or action may adversely influence the banks' ability to succeed in its business objectives, and achieve its strategic goals.

For this purpose a specific approach was followed where risks related to the bank in entity level, Division level, business unit level, and subsidiaries level were considered. It should be noted that during this project, business risks were identified and assessed, however not in detail as this would demand extensive resources for a long period of time, something which constitutes this assignment as a project itself.

For the identification of risks, data were collected by the bank, as well as from best practices available through PricewaterhouseCoopers networks of excellence and global best practices databases. During the identification of risks, compliance risk was also considered (i.e. due to the obligations of the bank to national regulatory authorities).

The main business risks identified include credit risk, operational risk, reputation risk, market risk, cash flow risk, legal and compliance risk, financial risk and strategic risk.

At this stage the enterprise risks were sorted according to their possible impact to the operations of the bank. The assessment of risks forms a vital part of the procedure related to the formation of the audit plan. For the evaluation of risks, data collected from similar efforts, as well as experience gained from external advisors in similar organizations and activities was used.

Risk assessment software was used as a mean to link the various business activities of the bank with the risks associated to them and rate them according to the extent of their impact to the bank.

On the next stage of the process, enterprise risks were rated according to the possible impact on the Banks' operations and sorted in the following categories:

- High risk
- Medium risk
- Low risk

The rating relates to the impact that risks have on the efficiency and effectiveness of the banks' operations as a whole, and not the effect on each activity separately. For example a risk may have significant impact on a specific division that is related to, but its impact on the whole organization may be low.

In relation to the branches network, an interpretation was made as far as what is high, medium, low branch network risk; mainly in relevance with credit and operational risk which are the main risks associated with branches network.

It has to be noted that operational risk was difficult to be identified and ensure that it has been properly measured given that there is no common interpretation of what operational risk is; also several subcategories may come in existence due to inefficiencies in procedures in place and generally weaknesses of the Internal Audit framework.

To link central divisions with their relevant risks the following data were used:

- Work performed during prior projects, etc;
- Existing central divisions audit programs;
- Central divisions operations based on the bank's charter;
- external advisors experience from work performed in similar enterprises;
- relevant bibliography.

Given that full recognition and assessment of risks was not exclusively related to the operation cycle of this project, the usage of the above data was considered necessary. In order to have a complete assessment of the risks involved with Central Divisions, and the impact on the operations, Bank questionnaires were sent to the Central Divisions management with the activities that were related to them. Management was asked to categorize the operations based on the risk they entailed.

Given that the existing data is limited and does not allow a detailed assessment of risks a similar approach was used to approach the rating of risks related to subsidiaries of the group.

5.3 Audit scoping

While assessing the audit needs with the assistance of external advisors, interviews were held with senior members, and where necessary with other members of internal audit division; in addition consideration was given to past audit work performed by internal audit division, work performed by external advisors in conjunction with internal audit division, and the objectives of the management.

The assessment of the audit needs was determined by previous experience of identifying risks, as well as with other quantitative and qualitative criteria that significantly influenced audit need prioritization.

Quantitative and qualitative criteria were gathered for all business activities of the bank and were then inputted into risk assessment software, which can be used to produce various assessments and extractions of statistical data.

The variables taken in consideration were category of branch (according to bank policies), amount and balance of loans granted, personnel number, time elapsed since last audit, prospective organisational changes, special issues existence, detailed documented procedures etc.

While assessing audit needs in order to effectively define the audit scope, higher rating was given to certain variables to achieve a more efficient establishment of audit scoping, type of audits, as well as hours of audit work needed.

Performing analysis of data gathered, it was concluded that out of 458 branches, 155 branches have either not been audited since 2000, or have never been audited at all. Likewise, a significant number of central divisions have fully or partially remain un-audited by internal audit division for many years. Same findings occurred in relation to subsidiaries of the group. The above findings were justified by the fact that internal audit division previous years audit scoping rated as more important the operational part of the audit, which resulted to focus less on branches network audits.

Based on the above, time elapsed since last audit considered as the main variable in assessing audit needs for 2006 and the forthcoming 2 years.

Therefore, considering the bank's objectives, in the annual audit plan the audit of branches network was given a higher score; and in particular branches that have either been audited long time ago, or never been audited.

Based on the above, the audits of central divisions were significantly reduced. In particular it was proposed to perform audits only in Financial operations and credit (corporate and consumer) divisions of the bank. In addition, specific activities of information systems and electronic banking divisions of the bank were decided to be audited by relevant IT auditors of information systems audit sub-division.

With respect to subsidiaries audit, planned audits were significantly reduced due to internal audit division objectives.

5.4 Audit planning

Decisive factor of the number of audits to be conducted by the internal audit division during 2006 was the recent implementation of TeamMate audit management system application within the bank. The need of division's members to get familiar with the application through training and on-the-job training is generally accepted.

Furthermore for completing the audit assignments of the internal audit division within a time horizon of 3 years, additional staff decided to be employed. All these have as a result to minimize the total number of audits to be performed for 2006, and extend the number of audits to be performed in the next 2 years.

The total number of audit assignments has as follows:

Branches audits	100
Central divisions–credit	8
Central divisions—treasury and risk management	8
Information systems audits	8
Subsidiaries audits	7
Special issues audits (beside small issues)	186
Compliance audits	3
Total audits	320

Internal audit division also determined the frequency and detail that every activity or operation must be audited, as well as the full cycle of audit assignments. The divisions objective is to address all audit needs in 3 years time.

In relation to branches, given the large number of branches, regular audits of each branch of the network will be performed at least once every 3 years.

As far as the central divisions concerned, the frequency that these will be audited was determined by the number of activities each performs, and the risk that its operations bear; as a result credit and financial operations divisions are audited on a yearly basis for some of their operations. The same applies for information systems and electronic banking services.

Related to the subsidiaries of the group the frequency that audits were conducted was based on the specific industry these are into and the risk that the bank bears because of them; as a result certain financial institutions operations are audited every year.

The available audit hours of internal audit division was calculated in man-weeks. In order to calculate the available audit time public holidays, annual leave and other days off mainly due to illnesses, study leave and maternity days off were deducted.

The available weeks per auditor are as follows:

Total working weeks	52
Bank holidays	3
Annual leave	5
Other absences	1
Total available working weeks per person	43

During audit needs assessment and for the determination of audit hours to be allocated by the internal audit division, particular attention was paid to the calculation of non-audit work of internal audit division.

For the allocation of the audit hours needed for each audit project, several interviews were conducted with Senior and other members of senior management taking into consideration the following:

- Type of the audit;
- Audited business unit, operation, activity;
- The work load of the branch, central division, subsidiary;
- The time needed to complete pilot projects undertaken by external advisors and internal audit division in branches, central divisions and subsidiaries;
- The number of personnel to be engaged for the audit of each branch, central division, subsidiary and ad-hoc projects (i.e. special issues) and Compliance issues;
- The time needed by internal audit division to perform audits during previous years;
- Audit experience of team members.

Allocated hours do not include those allocated for preparation and closing of the audit activities. Time needed for these activities was separately calculated and included in non-audit tasks of the division.

Based on this and after interviews with senior members of the audit division the following projects have been decided to be included in the relevant audit plan:

5.4.1 Branches

- Audit of 100 branches that have either been audited before 2000 or have never been audited;
- Branches audited by another review body since 2000 and after are not included in the 2006 audit plan, as well as all new Branches that will be included in 2008 audit plan;
- For the determination of audit sample the share that each branch classification (i.e. A+, A, B, C, D) in the branches network was used, as well as the time needed to perform the audit in conjunction with the number of available auditors needed;
- The large number of audits in branches of categories C, D, and E is normal given the fact that audits in these categories are shorter in time needed and fewer human resources required to conduct them;
- The number of auditors needed and the time available for the audit will be determined according to the category of the branch.

5.4.2 Central divisions

5.4.2.1 General operational audits

- Audits in all credit related divisions and financial operations divisions will be conducted given the fact that these are the main divisions of the bank, and possess a significant number of organisational operations;
- In these central divisions, 2 audits will be performed each year for some of their activities, with primary goal to audit the majority of their operations within 3 years;
- For these audits, 2 auditors are required and the audit time available will be 4 weeks.

5.4.2.2 Special audits

- Audits in treasury and risk management divisions given their high risk will be performed yearly. In these divisions, audits for some of their activities will be performed with primary goal to audit the majority of their operations within 3 years;
- For special audits, personnel of special audits sub-division will be used. In each audit, 3 specialised auditors will be used for 3 weeks;
- The audits of the above services were rated according to their bearing risk. For this purpose questionnaires were sent to central divisions in order to assess their operational risk based on the likelihood of the risk and its impact to the

operations of the bank. Operations were categorised as: high risk, medium risk, low risk;
– Questionnaires were then assessed in co-operation with members of the management of internal audit division.

5.4.2.3 Information systems audits

– After interviewing a senior member of the IT audit sub-division, performance of eight audits in applications and systems of specific central divisions was agreed;
– Co-operation of information systems audit sub-division and internal auditors is proposed so that operational and functional audits of the above divisions are achieved;
– Effort should be made so that audits for information systems and the relevant function (i.e. treasury, financial operations, etc.) by the general auditors are performed simultaneously;
– For each audit assignment three auditors are required.

5.4.2.4 Subsidiaries

– It is proposed that all Financial Institutions subsidiaries are audited yearly for some of their functions with primary goal to audit the majority of their operations within 3 years;
– Full scope reviews of specific manufacturing subsidiaries of the bank, are proposed to be audited once per 3 years. As far as its two subsidiaries which are going to be audited within the next years, audits will be detailed for all their operations because of their high work volume and the risk rating of the companies;
– Other non financial services companies will be audited once every 3 years by performing general audits;
– For these audits 3 persons are required;
– The variable factor considered for rating these companies is the time elapsed since last audit.

5.4.2.5 Special audits Special audits assessment of audit needs was determined after examination made by interviews conducted with members of special issues audit sub-division of the internal auditing division, and considering data from previous years. special issues are categorised in big, normal and small issues and in most cases causing special audits to be performed.

– Big issues are related to cases that are big frauds. Eight weeks are needed for their audit with the participation of two auditors. These issues usually come up on average twice a year;
– Normal Issues relate to cases that 2–3 days for their examination are needed and the participation of 1 auditor from Special Issues Division (for example burglaries and disputes between employees);

- Small issues relate to cases that are directly examined and usually half day on average for their examination is needed;
- Preparation of audit and examination of data is considered as non-working event of special issues division and usually takes a working day. In relation to Big issues, the preparation of audit is included in audit plan given that the data is examined before the actual audit of the branch by the auditors;
- Sum up of the project and report is also considered non-working event and usually takes one working week per auditor that participated in the audit. Small issues are an exception as examination of the issue is completed after examining the issue.

5.4.2.6 Compliance audits

- Compliance audits were also included into the audit plan. In these audits, corporate governance related audits are included, which is proposed to last for six working weeks with two auditors participating;
- Two additional audits are included that will be conducted by special audits sub-division and relate to compliance with IFRS and quality safeguarding audits based on ISO standards.

5.4.2.7 Non-audit work Before developing the audit plan, great attention was paid to the calculation of non-working events performed by internal audit division. Non-audit work includes the following:

- Managerial work
- Preparation and closure of audit assignments
- Training and information
- Follow up
- Administrative tasks
- Reports
- Support.

For each of the above work relevant performance time has been calculated. careful establishment of non working events is necessary for the calculation of available hours of the division to perform the annual audit work.

Audit plan includes branches network, central divisions, subsidiaries, special issues and compliance audits so that all kinds of possible audits to be performed and effectively exploit human resources of the various sub-divisions of the internal audit division.

5.4.2.8 Time schedule explanation In the relevant time schedule the following are noted:

- Audit work to be performed per type of audit (branch, central division, subsidiary, special issues and compliance audits);
- Audit duration in man-weeks;

- Required resources for each audit;
- Frequency of audits;
- Total man weeks per audit activity;
- Non-audit work of division and required man-weeks for their performance.

Considering all the above mentioned, the number of human resources needed from internal audit division so that audit work planned for the year 2006 is defined, as this arose from audit needs assessment and is mentioned in the completed audit plan.

Risk rating per auditable unit can be found in Appendix "Case study 2 risk rating per auditable unit". It is graphically shown the risk rating for each business unit, as this arose from audit needs assessment as we have already mentioned earlier. Summing up, risk has been calculated based on the impact to the organisation and date of last audit performed by internal audit division. The colour changes according to the risk rating; red colour shows high risk units, yellow moderate risk units, while green shows low risk business units.

6 Case study 3

Case study 3 has established 2 internal audit divisions which report to the audit committee of the bank and senior management. Domestic internal audit division focuses on domestic audits (over branches network, central divisions, domestic subsidiaries and other relevant projects), while group audit for international business focuses on international branches and subsidiaries (currently in seven countries). The first division adopts the cyclical approach, while group audit for international business recently adopted the risk based approach which will be presented in the following lines. Group audit for international business decided to be truly risk focused, rather than adopting a cyclical approach in its work. The assurance given now needs to focus on those controls and risk management activities that address the key risks within the auditable entity. To achieve this, internal audit will be working closely with the board and senior management, since they bear the ultimate responsibility for risk management. Both board and senior management fully support the RBIA approach.

6.1 Risk based internal audit methodology[5]

Initially, group audit for international business audit teams should acquire a deep knowledge of business at the local level (either at branches, or subsidiaries), especially strategic and business objectives. This will help internal auditors to understand the significant risks related to the achievement of objectives and motivate management to identify them. The main output of this step is the risk compiled by senior management (with the assistance of internal audit).

[5] The relevant information obtained by Risk Assessment and Internal Audit Manual of Case Study 3 Internal Audit division.

This step is considered the cornerstone of RBIA. It is a prerequisite that enables internal audit to target its efforts more effectively towards the areas, and risks that matter the most. It also requires a high level of input from both management and staff. It is therefore essential that staff from different levels involved, as far as this is practicable.

The second stage involves collecting information on management's assessment of the previously identified risks and determining how these are currently being managed by the entity. This, in effect, entails a preliminary assessment of the control environment (as mentioned before, internal control is only one mean of managing identified risks).

The point of this stage is to gain management input on the assessed level of the previously identified risks, and on their management approach. This enables internal audit to filter and prioritize risks, in order to develop its periodic audit plan. In other words, at the end of this stage, the internal audit teams should be able to decide which risks should be reviewed to ensure that are properly managed, when and how they should be reviewed. As a result, the risk register at this point does not only contain a complete list of previously identified risks, but it can also be filtered to produce a list of risks that will be subject for review by internal audit.

The group audit committee will be presented with a consolidated report regarding the international internal audit plans, in order to approve or amend it, accordingly.

Once again, management input is essential. The audit plan should be based on management's assessment of risks. Internal audit is called to provide assurance on the effectiveness of risk management for those risks that are considered to be high. To carry out this, risks will be prioritized and grouped into a series of audit assignments, according to the internal audit resources availability.

The final stage of group audit work consists of carrying out individual internal audit assignments, based on the periodic audit plan. The objective of each assignment will be to assess the effectiveness of internal controls and management monitoring activities of selected risks within the audit universe.

The results of each audit assignment are to be fed back into the risk register. Such results may include the identification of new risks, an updated assessment of risk levels based on audit findings etc. By utilizing these results, group audit for international business will be able to periodically inform the group audit committee of any changes in the risk profile of all international operations, risks that remain above specified tolerance levels, as well as pending corrective actions management has agreed to. A flexible risk register, continuously updated, permits the international internal audit team to remain focused on the high level risks.

A periodically updated audit plan contributes to the effectiveness of the internal audit function, since it takes internal audit away from the traditional, cyclical, compliance-based testing and closer to working based on the risks inherent in each entity. If compliance-based work is required, it is classified as "management request" work.

Group audit division has developed a generic risk framework, which is basically a high-level categorization of all risks a financial institution can face. All internal audit teams/internal auditors are invited to use this in the risk identification process. Risk framework is combined with a categorization of the High-level processes/

functions within a financial institution. Taken together, these two lists form a double-entry table where risks are linked to bank activities (i.e. in compliance with COSO enterprise risk management principles).

Having established a risk framework, group audit division has developed a common language for risk analysis. Consequently every risk is analyzed in two dimensions, namely likelihood of occurrence (LoO) and financial impact (FI) as the best practice dictates. Each dimension scored using a five-rate scaling scheme. By multiplying the scores of the two dimensions, a total risk score (TRS) is attributed to each risk.

LoO and FI are easily understood concepts. For this reason they are the most commonly used dimensions for risk measurement. It is considered as very important that senior management defines not only the rating scales for each dimension (since different risk weights may be attributed to international subsidiaries), but also the acceptable levels of risk, based on a pre-determined risk scoring system.

LoO represents an assessment of how often a specific risk may materialize, within a specified time period, which it gives the estimated frequency of a risk occurring. Financial impact represents an assessment of the effect on profits for a single materialization of a risk. If a risk materializes, the effect can be a direct loss (e.g. money embezzlement–fraud related) or an indirect one (e.g. fines, lawsuits against the bank). Financial impact also represents the potential cost of remedial measures (e.g. replacement of IT infrastructure) and other opportunity costs. Total Risk score represents the total risk exposure attributed to a specific risk within a specified period, i.e. the potential financial impact of a risk during that period. This exposure is expressed by calculating the potential minimum and maximum amounts at risk for each combination of LoO and FI scores. In other words, a TRS score will indicate the minimum and maximum loss (not an average or an exact estimate of the loss) that we can suffer from a specific risk within a specified period. Based on TRS, each risk is characterized as minimal, low, medium, high and catastrophic.

Risk assessment takes place at two levels, namely the inherent level (Inherent Risk—IR) and the residual level (Residual Risk—RR). At the inherent level, the significance of each risk is assessed without considering any mitigation measures. In other words, inherent risk is measured as if there were no controls in place to reduce it. At the residual level, the significance of each threat is assessed having in mind the control framework in place, i.e. after established controls. The relationship between IR and RR produces another useful measure for group internal auditors, namely the control effectiveness score (CES). CES represents the difference between IR and RR as controls are expected to reduce risk levels. On the other hand, while assessing inherent and residual risk levels, it is assumed that controls in place are adequate and effective in mitigating risks.

6.2 Defining the audit universe

The previous steps assist case study 3 to define the audit universe of the bank as a mean to develop a periodic audit plan for all international units of the group (i.e. Bulgaria, Serbia, Romania, Cyprus, FYROM, Albania and United Kingdom). The

audit plan lists the assignments that should be carried out by internal audit team over a specified period. It is a result of:

- Analyzing the information contained within the Risk Registers.
- Feedback provided by local internal audit managers.
- Incorporating management requests and specific directions related to Internal Audit.

Group audit considers neither efficient nor (cost) effective to review the complete set of risks (included in the risk register) within a single time period (i.e. a year). Therefore, the periodic audit plan represents an attempt to prioritize audit assignments so that they can address the most significant risks within a Unit, making the best use of internal audit resources and avoiding duplication of efforts with external parties providing assurance services.

Audit universe according to case study 3 procedures may exclude certain activities from it such as the following:

– Any inherent risks that fell below the risk appetite are considered to be within tolerable levels, even without any mitigation measures. Therefore, they should be factored out of the audit universe.
– The group audit committee may have requested assurance for some risks by other parties besides internal audit. (i.e. external auditors or compliance office). If such assurance services are provided and the results are reported directly to the group audit committee, then devoting internal audit resources to reviewing the same risks would result in duplication of efforts.
– The senior management team of the group may arrive to a decision that due to the nature of certain risks, there are no cost-effective ways to reduce them below the risk appetite levels; however these risks will be tolerated. Therefore there is no reason to include them in the audit plan, unless there are contingency plans linked to these risks. In the latter case, these risks should remain within the risk register, so that these plans are audited.

6.3 Risk assessment

Group audit for international business groups risks in a way that enables them to audit several risks in one audit assignment. Even though it is not necessary to assign all risks into audit groups, it can be proved very helpful for planning purposes, as this practice can easily lead to the determination of the scope of each audit.

Alternative categorizations include:

- Grouping by business units
- Grouping by processes
- Grouping by objectives

The choice for the categorization rests with the head of group audit. However, usually risks are grouped by auditable units (i.e. divisions, departments, branches, etc). The advantage of this approach is that it enables an internal audit team to cover one physical location in one visit. However, care should be taken so that some risks

(i.e. related to IT) are duplicated across all units. In that way, it will be ensured that internal audit will cover these risks in all units where they may have an effect.

Time elapsed since last audit a specific risk is also a very important factor should taken into account as time passes, as series of events may cause the risk to be inflated (i.e. organizational changes, new systems, turnover of competent personnel). In effect, the auditor's assessment of risk becomes less reliable. Therefore, group audit inflates the risk score for every year that risk has not been audited.

6.4 Scoping

The periodic audit plan may include audit assignments (having either an assurance or a consultancy nature) that are based on criteria other than risk. Such assignments may be requested by management, or may be mandatory in nature (dictated by regulatory authorities), or may focus on areas subject to significant changes.

Ideally, every mandatory audit should be a unique audit group, comprised of a series of risks, analyzed according with the risk register requirements. The same approach should be pursued for management requests. Such requests may originate from local senior management, the senior management team of the group or the group audit committee.

6.5 Audit planning

Group audit for international business comes up with estimates regarding the implementation of each individual audit assignment, from initiation to the submission of the final audit report as a mean to effectively allocate resources. Estimates are based on the number and experience of local internal audit staff. In the absence of budgetary historic data on audit assignment implementation schedules, local internal audit managers provide their own estimates for each assignment within their periodic audit plan, beginning from the assignments with the highest scores. It is up to head of the group audit to decide on the time unit that will be used for these estimates (hours/days).

Total available internal audit time is calculated considering the following factors:

- Number of internal auditors who can carry out assignments on their own (experienced auditors);
- Number of internal auditors who cannot carry out assignments on their own, but as part of a team (less experienced auditors);
- Working hours per day;
- Participation in training programs (estimate);
- Other events (i.e. administrative work, etc.).

7 Conclusions & best practices recommendations

Although standards for professional practice of internal auditing and basel committee requirements require risk-based audit plans to be established and

followed up by internal audit divisions, current practice has not incorporated standardized risk assessment and audit planning procedures by Greek Banks. Despite the fact that Bank of Greece does not require the usage of RBIA planning approach, when audits are performed to banks by the Bank of Greece issues are raised for not adopting such a methodology.

According to case studies developed in the previous chapters, there are several approaches on risk assessment and audit planning such as the cyclical approach, focus on high level risks approach and fully adopted RBIA planning, which is the recommended one. Cyclical approach ensures audit of all activities of the bank within a predefined time interval which may be time consuming and does not ensure focus on high risk activities. RBIA focuses on working towards high risk areas rather than performing compliance type audits without focusing on risks. Greek banks seem to adopt an intermediary approach taking into account risks, however neither documenting them, nor linking them to a relevant risk assessment, which is also far away from best practice. A comparative table on three identified approaches can be found at Appendix "Case studies1, 2 & 3 comparative table". Specifically, taking into account the three selected case studies, we observed the following:

- *Defining the audit universe*: In the first two case studies audit universe is defined after detailed analysis of relevant organizational charts which include all central divisions, branches, subsidiaries and business units, as well as mapping all critical projects and activities that carry some risk and should be included in the audit plan, as well as regulatory–compliance related requirements. In the third case, audit universe is defined after comprehensive risk assessment and prioritization of risks and relevant linkage to bank activities. This option represents best practice.
- *Risk assessment*: In the first case study, risk assessment is not performed at all, while in the second case study, risk assessment is based on a high level review of the main risks of the bank, which is also linked to the factor of time elapsed since last audit. Finally, risk assessment in the last case study includes detailed mapping of risks per audit area on a relevant risk register, as well as a risk analysis based on likelihood of occurrence and impact and linkage to audit universe components.
- *Scoping and audit planning*: Scoping and audit planning is the most essential part of the process as it is usually the result of risk assessment. In the first case, scoping is based on audit cycle approach therefore all audit areas are reviewed in a predefined time interval (2 years) without taking into account relevant risks. In the second case, time since elapsed since last audit and high level risk assessment impact is linked to specific audit areas and sub-areas. Finally, in the third case, scoping and audit planning consist of risks identified as high importance and may include audits across many audit areas that risks apply.

Audit planning should be driven by relevant risk assessments in order to provide assurance more effectively to management and stakeholders that the bank objectives will be achieved in the most effective and cost efficient manner. Risk assessment is

a major COSO component of internal controls framework and suggests that the bank must be aware of, and deal with the risks it faces. The main objective of the risk assessment and planning process should be the development of an annual audit plan in order to deploy resources. Long term audit plan should cover all potential audit areas (including divisions, branches, subsidiaries and other activities of the group) at least once in a predefined time interval (for example 3 years), considering risk factors, such as the size of business units, the complicacy of the audit, the individuality of auditable areas and subsidiaries environment, etc. As a general principle, new activities should be considered as a higher risk, than the existing activities, as well as a substantial transaction is considered as higher risk, than a minor transaction.

A long-term audit plan should be established for reasons of better organization and integrated planning of the audits. This plan should include audits to be executed, their timeframe and the required resources. The establishment of the long-term plan comes as a consequence of the need for controlling and monitoring the general progress of the bank and the assurance that the audit function keeps up with the overall group strategy.

Audit plan should be based on a fiscal year, so next year planning should occur early in the first quarter of the year with the audit committee approval of the plan at a predefined meeting. Control, risk self, assessment meetings help to learn about any changes to the business strategy and objectives or control environment.

The proposed annual planning phase can be summarized into the following steps:

1. Divide banking operations into auditable entities/activities. These might be divisions, branches and subsidiaries, as well as any other risk related projects and other activities.
2. Identify risk factors, such as:

   - Size of the area to be audited including the number of employees.
   - Years of operation of the entity/activity under review.
   - Years of operation under the current management.
   - Changes in the organizational chart of the unit.
   - Number and amount of transactions (reflected in local currency/EUROs).
   - Major changes in operations, programs, systems and controls.
   - The date and results of the last audit/follow-up (including results of external audit reviews).
   - Adequacy of central information systems.
   - Adequacy of security measures (wherever applicable).
   - Product development, new operations.
   - Deviations from approved budget.
   - Fraud cases detected.

Risk factors in each auditable entity/activity might be expressed quantitatively, qualitatively or in a combination of both (depending on the factor).

3. Assign a risk rating to each auditable entity/activity. This might be as simple as high/medium/low.
4. Decide which audit to perform based on risk considering any management requests. The internal audit function may audit high-risk entities/activities every year, medium risk entities/activities every 2–3 years and low risk entities/activities every 3–4 years.
   The periodic risk assessment considers the reliability and effectiveness of these controls in mitigating the significance and/or likelihood of risk occurrence. Based on this knowledge, various risks may be reclassified due to improved knowledge of the system of internal controls. However, even in areas where controls are thought to be effective, Internal audit function must incorporate the periodic testing of key controls to ensure they continue to assist to mitigating critical risks.
   Audit plan monitoring is preferably realized through the use of project management software tools. The division may use a specialized tool for resource and project management in order to ensure the effectiveness and efficiency of planning and its monitoring.

Appendices

Case study 2 custom measures

Branches

As far as for the branches network the qualitative and quantitative criteria used:

- Code and serial number of branch;
- The code refers to the number that is assigned to the branch on the "ON-LINE" system of the bank;
- State and category of the branch;
- *Additional products offered by the branch* This relates to all products offered by the branch that are in addition to the basic products offered. These may be offered by each branch within the approved limits based on its category;
- *Number of personnel in each branch* The data were collected from the relevant central division, which provided internal audit division with the relevant chart showing the actual number of personnel in each branch;
- *Branch financial results* The branch financial results were provided by the financial division for the year ended 31/12/2004;
- *Number and balance of depository accounts, and repos* The data were collected from "electronic system of the bank" with accounting balance on 31/12/2004;
- *Number and balance of loan accounts* The data were collected from "electronic system of the bank" with accounting balance on 31/12/2004;
- *Existence of organizational changes within the year* The data was collected from the relevant central division of the bank, which provided internal audit

with the relevant chart showing all the organizational changes during last year (2004 and after) for managerial and sub-managerial positions within the branch;
- *Years elapsed since last audit conducted by the internal audit division* These data refer to audits performed from 2000 and onwards. Prior audits are not considered given that a period of more than 6 years elapsed. Audits performed in collaboration with external advisors are included in the audit work performed by the management. Likewise branches that have never been audited are marked with a high risk score;
- Data since last audit from Central Bank of Greece or any other regulatory authorities;
- *Areas covered during last audit and type of audit* The data were extracted using the audit reports issued, found in the database of the division;
- *Special issues* The data were collected from the Department of Examination of Special Issues. Only the most important special issues were included. Basic categories of special issues are: financing issues, cash deficiencies, depository accounts related issues, ATMs, robberies, card skimming, employee disputes, commitment to the branch budgeted finance and deposits (credit divisions).

The following data were taken in consideration for the calculation: industry data, market data, geographic data, competition data, amount of transactions in the past years.

Central divisions

In relation to central divisions, the qualitative and quantitative data used:

- *Operations of central divisions* The operations referred are directly related to the organization of the bank;
- *Existence of documented procedures* Acceptable answers in this field: exist and are fully documented, exist with some omissions, no documented procedures;
- *Organizational changes within the year* The data were collected from the relevant central division of the bank, which provided internal audit division with the relevant chart showing all the organizational changes during 2004 and after, for managerial, and sub-managerial positions within the central division, and the sub-division the change relates to;
- *Information systems changes within the year* The data were collected from the information systems control sub-division and relates to changes that will be made to information systems and electronic banking divisions;
- *Years elapsed since last audit performed by the internal audit division* These data refers to audits performed from 2000 and onwards. Prior audits are not considered given that a period of more than 6 years elapsed. Audits performed in collaboration with external advisors are included in the audit work performed by

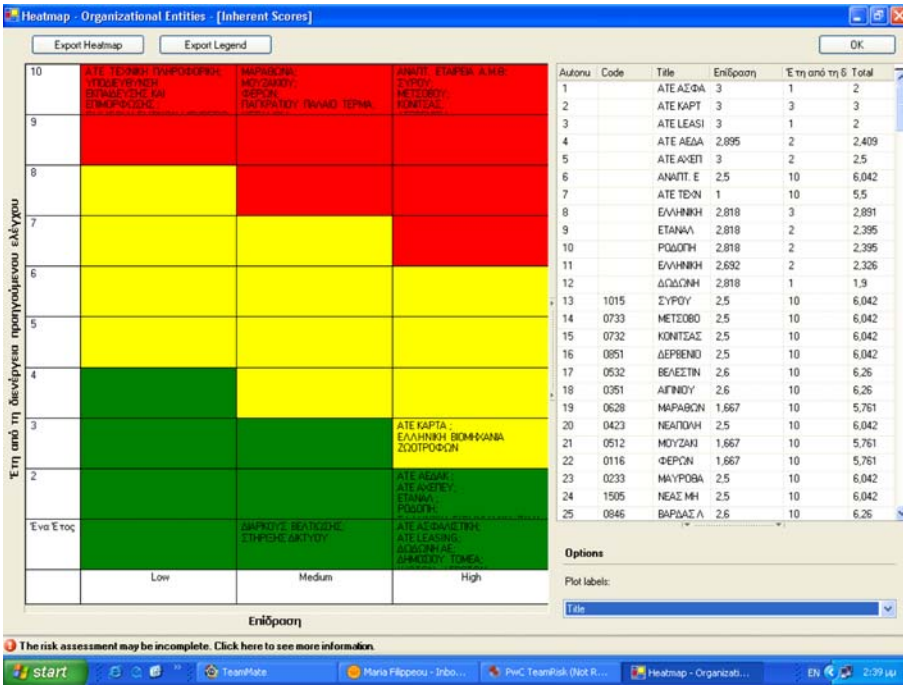
the management. Likewise central divisions that have never been audited are marked with a high risk score;
- Areas covered during last audit and type of audit;
- Audit performed by external auditors;
- Special issues;
- *Commitment to the central division budget* The data were collected from central finance division with accounting balance on 31/12/2004.

Subsidiaries

In relation to subsidiaries the qualitative, and quantitative data used:

- *Industry and location* The industry the subsidiary operates in and its location;
- *Shareholding of the bank* The data were collected by the Department of Subsidiaries of Internal Audit Division of the bank with data dated January 2005. The shareholding is a result derived both from direct and indirect shareholdings of the bank;
- *Basic products* The basic products the subsidiary deals with according to data provided by subsidiaries department;
- *Activities/transaction cycles* The activities and main transaction cycles of subsidiaries were identified. As far as industrial companies for which no audit schedules were devised the activities used were derived from the general audit schedule of industrial companies;
- *Personnel number* The data were collected by the strategic division of the bank, which provided us with the relevant chart showing the number of personnel in each subsidiary;
- *Existence of internal audit division/number of auditors*, The existence of internal audit division and the number of personnel employed;
- *Financial results* The financial results were provided by the division of group strategy for the year ended 31/12/2004;
- *Organizational changes within the year* The data were collected from the division of group strategy, and relates to all organizational changes of subsidiaries during last year (2004 and after) for managing director or director positions in the company;
- *Years elapsed since last audit performed by internal audit division* These data refer to audits performed from 2000 and onwards. Prior audits are not considered given that a period of more than 6 years elapsed. Likewise subsidiaries that have never been audited are marked with a high risk score;
- Audit performed from external auditors;
- Areas covered during last audit and type of audit;
- Special issues.

Case study 2 risk rating per auditable unit



Red = High risk units, branches, subsidaries, and central divisions
Yellow = Medium risk units, branches, subsidaries, and central divisions
Green = Low risk units, branches, subsidaries, and central divisions

Case studies 1, 2 & 3 comparative table

Case study 1	Case study 2	Case study 3
Audit universe		
In order to assess the audit needs of the bank and prepare the audit plan, internal audit division initially identified bank's business activities including: • 25 Central divisions, • 137 Branches, • 849 Post offices, • 1 Subsidiary.	Business activities were initially identified taking into consideration all the business activities of the bank including: • 27 Central divisions, • 458 Branches, • 13 Subsidiaries with more than 50% shareholding, • Special projects, • Compliance with regulatory authorities.	Operations in seven (7) countries including all core and support banking functions, as well as relevant subsidiaries.

Appendix continued

Case study 1	Case study 2	Case study 3
Risk assessment		

• Not documented risk assessment.
• Main risks consideration based on auditors' experience (high level approach).
	• Primary risks related to the bank and its activities, and those directly related to the strategic goals of the bank were identified.
	• Risks related to bank on entity level, business unit and subsidiary level considered.
	• Business risks included: credit risk, operational risk, reputation risk, market risk, cash flow risk, legal and compliance risk, financial risk and strategic risk.
	• The above risks were linked to all banking operations and activities.
		• Main risks, as well as detailed risks were identified and compile the risk register.
		• Management's assessment of the previously identified risks.
		• Prioritisation of risks.
		• Two fold analysis for each risk:
		  • Financial impact.
		  • Likelihood of cccurrence.
		  • Total risk score (TRS).
		• Two level risk assessment:
		  • Inherent risk.
		  • Residual risk.

Scoping		
• 40% of branches. • Time elapsed since last audit.	• Branches audits based on time elapsed since last audit. • Central divisions—credit: 8 audit assignments. • Central divisions—treasury and risk management: 8 audit assignments. • Information systems audits: 8 audit assignments. • Subsidiaries audits: 7 audit assignments. • Special issues audits (beside small issues): 186 audit assignments (average) • Compliance audits: 3 audit assignments. • Time elapsed since last audit.	• Risk grouping into auditable units (e.g. human resources risks, information systems risks). • Audit assignments based on criteria other than risk (e.g. regulatory and management requests). • Time elapsed since last audit. • Inherent risks below risk appetite outside scope. • Risks that management is willing to tolerate. • Assurance services provided by third parties outside scope.
Audit planning		
Year 1 • 50 Branches. • Treasury division. • Information systems division. • Financial operations division. • Consumer loans division. • General services division (general procurement sub-division). • Credit card sub-division.	Year 1 • Branches audits: 100 (22%) that have never been audited or audited before the year 2000. • Branches will be audited once every 3 years. • Frequency determined by the number of activities each central division performs and the relevant risks.	Group audit for international business groups risks in a way that enables them to audit several risks in one audit assignment. Even though it is not necessary to assign all risks into audit groups, it can be proved very helpful for planning purposes, as this practice can easily lead to the determination of the scope of each audit.

Appendix continued

Case study 1	Case study 2	Case study 3
• Non-performing loans subdivision.	• All credit related and financial operations divisions will be audited every year in certain activities. The same applies to Information systems related divisions. • Primary goal to audit the majority of operations of credit and F.O. divisions within 3 years. • Subsidiaries audited based on the risk of their Industry (i.e. financial Services considered as higher risk than manufacturing however time elapsed since last audit will be also considered). • Financial services divisions will be audited on a yearly basis. • Total available working weeks per person: 43.	Alternative categorizations include: • Grouping by business units. • Grouping by processes. • Grouping by objectives.

References

A New Agenda for Corporate Governance Reform. The Institute of Internal Auditors, UK and Ireland, July 2002.

ATE Bank Risk Assessment and Audit Planning. (2005). Report prepared by PricewaterhouseCoopers. Athens.

Bank of Greece Governor's Act. Number 2438/6.8.1998.

Bank of Greece Governor's Act. Number 2560/1.4.2005.

Bank of Greece Governor's Act. Number 2577/9.3.2006.

Basel Committee on Banking Supervision: Framework for the Evaluation of Internal Control Systems. Basel: January 1998.

Basel Committee on Banking Supervision: Enhancing Corporate Governance for Banking Organisations. Basel: September, 1999.

Basel Committee on Banking Supervision.: Internal Audit in Banks and the Supervisors Relationship with Auditors. Basel: August, 2001.

Basle Committee on Banking Supervision: Compliance and the Compliance function in Banks. (2005). Basel: April 2005.

Commission Decision of 28 April 2005 establishing a group of non governmental experts on corporate governance and company law (2005/380/EC). Official Journal of the European Union, L126/40, 19-5-2005.

Committee of Sponsoring Organization of the Tradeway Commission (COSO). (1992). *Internal control—integrated framework*. Jersey City (USA): AICPA/COSO.

Corporate Governance Law 3016/ 17-5-2002. Hellenic Republic, 2002.

Enterprise Risk Management Framework. Committee of Sponsoring Organizations of the Treadway Commission (COSO Report). (2005). USA: 2005.

Greek Postal Savings Bank Audit Planning Report prepared by PricewaterhouseCoopers. Athens, 2006.

Group Audit for International Business Internal Audit & Risk Assessment Manual: Alpha Bank, Athens 2006.

Koutoupis, A. (2004). Corporate governance and internal control systems. *Athens: Economic Chronicles Journal*, Issue Number 126 (March–April 2004).
Koutoupis, A. G. (2005). Corporate governance and internal audit in Greece, Panteion University of Social and Political Sciences. In *Third European Academic Conference on Internal Audit and Corporate Governance*.
Koutoupis, A. G. (2006). Corporate governance & business risk management regulations and best practices impact on internal controls & internal audit activities within Greek publicly listed enterprises. In *Fourth European Academic Conference on Internal Audit and Corporate Governance*.
Koutoupis, A., & Marios, M. (2004). Internal auditing and risk assessment. *Naftemporiki Newspaper*, Athens, 27/4/2004.
Koutoupis, A., & Tsamis, A. (2006). Reengineering internal audit and compliance functions within Greek banks. In *Fourth European Academic Conference on Internal Audit and Corporate Governance* (Main Conference—6 April 2006), Cass Business School, London, United Kingdom (5–7 April 2006).
McNamee, D., & Selim, M. G. (1998). *Risk management: Changing the internal auditor's paradigm.* Altamonte Springs, FL: The Institute of Internal Auditors.
Melville, R. (1997). *Re-engineering audit: Quality, control self assessment and the balanced scorecard.* Management Working Paper, City University Business School.
Risk Based Internal Auditing (RBIA)—Position Paper. The Institute of Internal Auditors UK and Ireland, August 2003.
Risk Management and Internal Control in the EU—Discussion Paper. FEE, March 2005.
Selim, G., & McNamee, D. (1999a). The risk management and internal auditing relationship: Developing and validating a model. *International Journal of Auditing, 3*, 159–174.
Selim, G., & McNamee, D. (1999b). Risk management and internal auditing: What are the essential building blocks for a successful paradigm change? *International Journal of Auditing, 3*, 147–155.
Standards and Guidelines for the Professional Practice of Internal Auditing. London: The Institute of Internal Auditors-U.K., 2004.
The Combined Code: Principles of Good Governance and Code of Best Practice. UK: June 1998.
The Sarbanes–Oxley Act—An Overview (Unpublished Presentation). PricewaterhouseCoopers, 2002.

Author Biographies

Andreas G. Koutoupis BSc (Honors), MSc (Internal Audit), PhD, MIIA, PIIA, CIA, CCSA is a senior manager of PricewaterhouseCoopers internal audit services, Athens, Greece. He is carrying out research in corporate governance, business risk management and internal auditing practices in Greece, as well as benchmarking with global best practices. Andreas Koutoupis has an extensive professional experience on financial services organizations (mainly banks) as a project manager in complex assurance and consulting engagements. Also, he is teaching internal auditing on the MSc of taxation and auditing, Panteion University.

Anastasios Tsamis BA, MA (accounting and finance), PhD is the compliance officer of Emporiki Bank, Athens, Greece. He is also an associate professor of accounting and finance at the department of public administration, Panteion University of social and political sciences, Athens–Greece. He has served as a director of the organization division of Emporiki Bank, as well as a member of the board of directors of "Hermis" mutual funds management corporation (MFMC). He has carried out research in a wide range of areas, such as finance, international financial reporting standards (IFRS) and tax legislation. Anastasios Tsamis has published many articles related to accounting, finance, industrial growth, management etc.