Internal Auditing and Risk Assessment in Large Italian Companies: an Empirical Survey

Marco Allegrini and Giuseppe D’Onza
University of Pisa

This paper aims at achieving an overall view regarding the state of the art of internal auditing in large Italian companies. Mainly, it is focused on risk assessment practices and on the execution of a risk-based approach in the audit process.

The research is based on a survey carried out on the ‘Top100’ companies listed at the Italian Stock Exchange.

Survey results reveal that practices vary significantly among three different models:

1. A few companies (25%) carry out mainly traditional compliance activities and they generally follow an audit-cycle approach for the annual audit planning;
2. In most companies (67%), internal auditors adopt the COSO model and perform mainly operational auditing. Risk-based approach is applied predominantly at macro level.
3. Finally, it is possible to identify a very few large companies (8%), in which auditors are applying a risk-based approach both at macro and micro level.

Key words: internal auditing, control governance, control model, risk assessment, risk-based auditing, audit planning, Control Risk Self Assessment, Italian companies, survey.

SUMMARY

The research aimed at verifying the main features of internal auditing activities in large Italian listed companies. Survey results show that all the financial institutions and Mib30 companies have an internal audit unit. In banks and insurance firms, the internal audit department has been established mainly to comply with regulatory requirements; in some cases, it represents an evolution of the previous ‘compliance office’.

In many companies, the internal audit unit is small in size (fewer than 10 employees). Bank and insurance companies usually have by far a higher ratio of auditors to employees than other firms. The analysis reveals that the organisational independence of the internal audit department is often ensured, in so far as it is not placed under line management.

Then, it is possible to identify a new trend in the largest business groups: the setting up of a specific audit company, carrying out internal auditing activities exclusively for the whole business group. In regard to the types of auditing, operational audit generally prevails, especially in Top30 companies. In financial institutions and in smaller companies

Correspondence to: Marco Allegrini, University of Pisa, Italy.
Email: allegrini@ec.unipi.it
compliance auditing is also rather important. Generally, companies do not assign many resources to the financial audit.

Survey results highlight that companies have usually developed a structured methodology for risk assessment, primarily to enhance corporate governance and internal control systems. Respondents underlined the contribution provided by internal auditors in the risk assessment process. In some cases, they co-operate with external consultants by monitoring activities and customising the methodology to the organisation. In many companies, they directly provide the methodology. In a few cases, they act as facilitators in the self-assessment. In financial institutions, internal auditors usually assert to participate in the risk management team and to provide some contribution in the qualitative assessment of operational risks.

It is worth mentioning that soft variables, such as senior management support, culture, integrity, communication are generally perceived as critical success factors of risk assessment projects. This is consistent with the general recognition of the role played by the control environment for the effectiveness of the internal control system.

Survey results reveal that risk assessment findings are also considered as a powerful input for planning the annual schedule of audits (macro level). Instead, in planning each audit engagement (micro level), risk assessment is used in order to limit or expand the controls. As a consequence, in most companies, individual audits still seem to be control-based, and not risk-oriented (Selim & McNamee, 1998). Regarding CRSA projects, survey results show that in the Italian context this methodology is still in a 'start-up phase', being applied throughout the entire organisation only by a few ‘pioneers’.

1. RESEARCH METHODOLOGY

Aim of the paper

Regarding the ‘Top100’ companies listed on the Italian Stock Exchange, the objectives of the survey are:
1. to achieve an overall view regarding internal auditing practices;
2. to analyse risk assessment activities;
3. to examine the application of risk-based auditing;
4. to define the acceptance of CRSA (Control Risk Self Assessment).

Project objectives and background

The main research tool is the questionnaire, which was sent to the audit departments of all the companies included in the sample.

At the beginning of the project, the questionnaire was focused on the practice of CRSA (Control Risk Self Assessment). The idea to carry out the survey arose in the summer of 2001 at the Centre for Internal Auditing at the CUBS (City University Business School) in London. The goal was to extend to the Italian context a prior research carried out on CSA practices in the United Kingdom (Melville, 1999). But, first contacts with companies revealed that this methodology is not so accepted as it is in Anglo-Saxon countries. Therefore, we decided to broaden the subject of the research, and to work out the questionnaire into four parts:

1. structure and activities of the internal audit department;
2. application of control models;
3. risk assessment practices and risk-based auditing;

To investigate the practice of CRSA, we decided to carry out also some direct interviews with chief internal auditors of three companies that had implemented successfully the project.

Finally, we examined the public corporate governance report issued by the companies included in the sample. This kind of analysis allowed us to get other information on the control governance system of respondents.

Sample

The research is based on a survey of the ‘Top100’ companies listed on the Italian Stock Exchange. The sample includes three categories:¹
1. companies listed at the Mib30 section;
2. companies listed at the Midex section (25);
3. other Top100 companies, classified from the 56th position to the 100th, according to their market capitalisation.

Answers

In all, 52 companies have filled in the questionnaire. Moreover, 13 companies stated
that they have not set up an internal audit department. By including the latter, the answer rate is 65% (70% in Mib30, 76% in Midex and 56% in ‘other’ Top100 companies).

2. THE ITALIAN CONTROL GOVERNANCE FRAMEWORK

The control governance model in Italian companies seems to be quite complex, given the existence of several bodies and actors involved in the monitoring of the Internal Control System (hereafter, called ICS).

At present, the civil law requires listed and non-listed companies (with the exception of small organisations) to have a board of auditors (collegio sindacale) as a control body. Its members are appointed by shareholders, and shall attend the board of directors’ meetings.

The Preda Code (a self regulation act for listed companies) recommends that the board of directors, in performing its supervisory duties, should establish an audit committee made up of non-executive directors and that the majority of members should be independent (Italian Committee for the Corporate Governance of Listed Companies, 1999). However, the analysis of the public corporate governance report has shown that 23% of the companies do not have an audit committee.

It is worth pointing out that in listed companies there is an overlap between the board of auditors and the audit committee.

The board of auditors shall supervise:
- the organisation’s compliance with the law and the regulations;
- that directors perform their work with professional due care;
- the adequacy of the organisational structure, of the accounting system, and of the internal control system.

In non-listed companies, the board of auditors shall also verify the true and fair view of financial accounts.

The audit committee has the task of:
- monitoring the internal control system;
- assessing the internal audit plan;
- reporting to the board of directors on its activity and on the adequacy of the ICS, at least once every six months.

Moreover, the Preda Code requires listed companies to appoint one or more persons to monitor the internal control system (‘preposto al controllo interno’), who should be independent from actors subject to their control. They should report on their activities and findings to the board of directors, to the audit committee and to the board of auditors. The latest version of the Code suggests that the chief internal auditor should carry out this function. In the public corporate governance report, this actor is mentioned in 44% of companies. Regarding the aforementioned percentage, we found that in 47% of cases, this actor corresponds to the chief internal auditor; in 33% he is a director, in other cases, he is a member of the audit committee.

Regarding the Internal Audit department, survey answers revealed that 13 companies do not have such a unit. Particularly, all Mib30 organisations have an internal audit department, whereas it is absent in 16% of Midex companies and in 24% of companies ranked from the 56th to the 100th position.

In January 2003, the Italian company law has been modified, so that the control governance framework is going to change significantly. The new law will be enforced starting from 2004, and it suggests the possibility for companies to choose among three alternative models:
- Horizontal-Dualistic model (traditional), characterised by a board of directors and a board of auditors, both appointed by shareholders;
- Vertical-Dualistic model, characterised by the existence of an executive board and of a surveillance board, that is appointed by shareholders. The surveillance board has the tasks to appoint executives, approve company and group financial statements, and supervise the ICS;
- Monistic model, characterised by the existence of a board of directors that is nominated by shareholders, and an audit committee appointed by the board of directors.

3. INTERNAL AUDITING: STRUCTURE AND ACTIVITIES

The questionnaire aimed firstly at highlighting the organisational status of the audit department and the main activities it usually performs.

Particularly, the analysis regards:
- the audit department size;
- the position in the organisation structure and the reporting lines;
c) the internal auditing in business groups;
d) the types of auditing;
e) the application of control models.

(a) Audit department size

The sample includes a few companies with large internal audit departments, whereas most companies have a very small audit unit. Actually, in most cases, the internal audit department has fewer than 10 employees.

The ratio of auditors to employees is, on average, about one to six-hundred, with relevant differences among the industries analysed.

Banks and insurance companies usually have by far a higher ratio (one every one hundred and twenty) than other firms. This result seems consistent with international practices, as revealed by a survey of the ‘Basel Committee on Banking Supervision’ carried out in 2002.

In fact, in financial institutions, the internal audit unit often includes the prior ‘compliance office’. Moreover, regulations issued by external supervising institutes (the Bank of Italy, Consob, etc.), are a driving force to broaden internal auditing activities.

(b) Position in the organisation structure and the reporting lines

In this regard, we analysed two different subject matters:
- the position in the organisational structure: who does the chief internal auditor hierarchically depend from?
- The reporting lines: who shall the chief internal auditor periodically report to?

Regarding the position in the organisation, the chief internal auditor is generally placed hierarchically under the Chief Executive Officer (44%) or the Chairman (23%). Therefore, we can assert that the organisational independence of the internal audit department is often ensured.

In relation to the reporting lines, the chief internal auditor periodically reports to the audit committee (92%) and to the board of auditors (92%), who are the bodies responsible for monitoring and supervising the ICS. The chief executive officer receives audit reports in 44% of cases.

The frequency varies in relation with the receiver of the periodic reporting, the company practice and the materiality of audit findings. A report on activities performed is generally provided every quarter to the audit committee and to the board of auditors, twice a year to the board of directors.

(c) Internal auditing in business groups

Most of the companies included in the sample belong to a business group. Therefore, we aimed at understanding:
- the position of internal audit departments in the business group;
- the functional relationship between the internal audit unit of the head office and the audit resources located in the subsidiaries.

Regarding the former, we identified three main alternatives:
- the internal audit department is set up only in the parent company, and it carries out auditing activities for all the subsidiaries (centralised model); it is applied in 46% of cases;
- a new company is purposely established just to perform auditing activities for the whole business group (delegation model); this kind of model has been adopted recently by a few conglomerate groups (12%);
- auditing departments are established both in the parent company and in two or more subsidiaries (widespread model); this option has been followed by 42% of companies.

The analysis, industry by industry, shows that the centralised model prevails in the service and in the manufacturing/retail industries, whereas the widespread model characterises the banking and insurance groups.

The analysis of data, taking into account segments of the stock exchange, reveals that the larger companies usually adopt the widespread model, whereas the centralised model prevails in smaller ones.

It is worth pointing out that the delegation model has generally been adopted in order:
- to produce synergies, and to increase the effectiveness and efficiency of auditing activities;
- to enhance co-ordination of auditing engagements;
- to strengthen independence from line management.

In business groups that adopt the widespread model, there can be different kinds of relationships amongst audit departments.

Generally, the audit department of the parent company co-ordinates the activities carried out in the subsidiaries (87%), through the definition...
of some general criteria for the annual audit planning.

In many cases, specific audit engagements, such as IT, fraud, ethical, and environmental auditing, are carried out directly by the parent company audit department.

(d) Types of auditing

The survey also aimed at analysing the percentage of audit resources devoted to:

- financial audit;
- operational audit;
- compliance audit;
- other activities (IT audit; fraud investigation; risk assessment; special projects).

Results show that operational audit generally prevails (34% of audit resources), especially in Mib30 companies. The scope of internal audit generally regards the suitability of procedures from the perspective of economy, effectiveness, and efficiency (Chambers, 1987).

Compliance audit is the second relevant scope of auditing activities (20%); particularly, in financial institutions and in smaller companies, auditors review the systems, which have been established to ensure compliance with legal and regulatory requirements, policies and procedures.

Financial audit seems to be considered the sole responsibility for external auditors; in fact, internal audit departments allocate small resources for the review of the reliability of public financial statements (5%). Instead, the review of management information systems receives a higher percentage of resources (10%).

The size of audit resources devoted to risk assessment (16%) reveals the relevance of this kind of activity, especially in large companies.

(e) Application of control models

The research team sought to assess the awareness and application of control models (Coso, Coco, etc.) in the organisations.

Control models have broadened the view of internal control and have strengthened the concept of control environment, risk assessment, monitoring and continuous improvement as key control principles (Roth, 1995).

However, a number of respondents (26%) do not believe that control models provide an effective basis for designing the internal control system, and therefore they have not integrated COSO into their audit process. Their control system seems to follow the traditional foundation of specified control process, procedure and structure, and the focus is entirely addressed to monitoring and assessing control activities.

Most companies (74%) are trying to incorporate COSO principles in the internal control policies and procedures. They have integrated COSO into their audit process; in particular, the framework is used to catalogue the audit results in the reports to senior management and to the board of directors (Wallance & White, 1994).

It is worth mentioning the relevance of the control environment, and the strong interest that senior management seems to address to this component of the internal control system.

However, results reveal that auditors do not usually address qualitative issues in their work, perhaps for the subjectivity involved in this kind of audit. Some interviewed stated that informal controls are not tangible and, therefore, are not subject to the verification demanded by traditional auditing methodology (Makosza & McCuaig, 1990).

4. RISK ASSESSMENT

Risk assessment is a method of identifying, measuring and prioritising risk. It is a prerequisite of risk management, which is the process of determining whether or how much of the risk is acceptable and what actions should be taken in order to avoid, to share or to control the risk (McNamee, 1998).

To protect and add value to the organisation, different steps of risk assessment should be approached in a methodical way. The survey particularly aims at identifying the application of risk assessment models, the main actors involved, the objectives pursued and the impact generated by the law on corporate frauds.

Application

Risk assessment models seem to be widespread in large companies. Most companies (62%) have adopted a structured methodology for risk assessment, and a few organisations (19%) reveal their willingness to introduce it.

Many companies implemented a risk assessment project more than one year ago and are going to repeat it once a year or every two years. However, there are a few companies that will not replicate
risk assessment activities in the next few years, since the project was not completely successful or they think there will not be significant changes in the business risks.

As easily foreseen, all financial institutions have developed a structured model to monitor business risks, primarily to comply with regulatory requirements. Banks and insurance companies have introduced quantitative models to monitor and control credit, market and operational risks.

Moreover, survey results show that risk assessment methodology is generally more applied in Mib30 companies than in Midex and ‘other’ ones. Actually, in large groups, the high organisational complexity seems to imply the need for assurance tools, in order to monitor systematically the organisation’s risk exposures in all business areas.

Regarding the area of implementation, a formalised risk assessment methodology is generally applied in all the business processes and departments (74%). In other cases, it is applied partially, since it is not implemented in those departments that manage intangible variables, such as R&D and human resources units.

We can assume, on the basis of interviews and comments provided by respondents, that the extension of the area covered by the project also depends on the time that has elapsed since the first introduction, and on the number of times it has been repeated.

It is worth pointing out that the project’s critical success factors are generally linked with soft variables, such as support at the top level, culture and communication. On the contrary, technical elements (clear identification of processes and their owners, development of a formal risk assessment model) are considered less important. This is consistent with the general recognition of the role played by the control environment in the internal control system.

Main actors
Risk management involves the contribution of many actors at different levels of the organisation.

The board of directors and the chief executive officer have the responsibility for setting the strategic direction of the business and creating the environment for an effective risk management system. As mentioned above, the survey highlights that the sponsorship of senior management is perceived as the most important success factor for the introduction and the continuous improvement of risk management projects.

The business unit managers have primary responsibility for managing risks on a regular basis. They should promote the culture of risk within their operations and set risk management objectives into their business (AIRMIC, ALARM, IRM, 2002). Nevertheless, a few companies (5% of respondents) have run a risk assessment project without the involvement of the line management. In these cases, internal auditors co-operate with external consultants to identify and to measure business risks.

The risk management unit should set and update policies and methodologies to monitor business risks and to support the decision making process. The survey shows that a formal risk management department has usually been established in bank and insurance companies (70%), while in other industries it is rarely set up as an independent unit.

In financial institutions, the analysis of business risks is carried out by the risk management unit in co-operation with line managers. Internal auditors assert to participate in the risk management team, and to provide some contribution in the qualitative assessment of operational risks.

According to the new definition of internal auditing, auditors should play a relevant role in evaluating and improving the effectiveness of the risk management processes. In fact, ‘the internal auditing process provides assurance to management and the audit committee that risks to the organisation are understood and managed appropriately’ (IIA, 2002). Their task may well spread over a large range of possibilities (IIA-UK and Ireland, 2002):

• auditing the risk management process throughout the organisation and providing assurance on the management of risk;
• supporting the risk management process, as members of risk committees, as providers of tools and techniques or as analysts in the identification of business risks;
• training the line staff and facilitating self-assessment workshop;
• co-ordinating risk reporting to the board of auditors, to the audit committee and to the senior management.

Respondents underlined the contribution provided by internal auditors in the risk assessment process. The survey reveals that internal auditors in Italian companies may:
• co-operate with external consultants in the risk management project, by monitoring activities and customising the methodology to the organisation (30%). In very few cases, line management is not involved in the project (5%). This hypothesis regards smaller companies, where the risk identification process is generally not comprehensive;

• support the risk management process directly in co-operation with line management (37%), by providing methodologies, and carrying out some consultancy services in risk management activities;

• facilitate the control risk self assessment (18%). When a risk assessment project has been introduced in co-operation with an external consultant, internal auditors underline that a critical element concerns the customising of the external model to the organisation.

Main objectives

We suggested a list of possible objectives of the risk assessment project, and asked internal auditors to assess them, using a 4 point scale. The objective that received the highest score was ‘Developing a systematic approach that management could use whilst dealing with the risk’ (3.3). A formal methodology allows line management to be aware of risks which fall within their responsibility, in order to set up a risk treatment process. Moreover, it contributes to a more efficient use/ allocation of capital and resources within the organisation.

In many companies, especially financial institutions, the introduction of a risk assessment system has been spurred on also by regulatory requirements. External reporting is not considered an objective of risk assessment. In Italy, external risk reporting is not widespread; no standard or professional report specifically requires this kind of disclosure, and also companies do not seem to be very keen on it.

Impact of corporate fraud law on risk assessment

Law No. 231/2001 established corporate responsibilities for fraud against government organisations, following the model defined in the USA by the Federal Sentencing Guidelines. It recognises the possibility to avoid/mitigate corporate responsibility whenever the company has a structured internal control system to prevent fraud against government organisations. In order to set up an effective internal control system, the law requires to start with a risk assessment activity to identify the organisational areas in which corruption or illegal acts could be carried out.

This law constitutes a pressure factor to introduce a formalised risk assessment methodology (16%), or to broaden the existing risk assessment activities by developing a specific fraud risk assessment project (43%).

5. RISK-BASED AUDITING

The standards issued by the Institute of Internal Auditors (IIA, 2002) incorporates risk assessment into internal audit planning at two levels:

• in planning the annual schedule of audits (macro risk assessment);

• in planning each audit engagement (micro risk assessment).

The research aimed at achieving an overview regarding the execution of a risk-based approach into internal auditing activities.

Macro risk assessment

Most respondents (72%) declare to apply a risk-based approach in the annual audit planning. Chief internal auditors seldom use a formalised model in which risk factors are weighed numerically according to their importance, and a quantitative rating is assigned to each auditable unit. In fact, auditing resources are often allocated on the basis of the auditors’ perception about the area with material risks.

Other companies state to adopt the traditional ‘cycle approach’, since they simply divide the audit universe in some parts and a portion is completed each year. However, a part of audit resources are also reserved for management requests, special projects and other engagements. Interviewees were also asked to pinpoint some possible risk factors, taken from the literature (Patton et al., 1983). The adequacy of internal controls and the changes in the organisational structure are perceived as the most important risk factors.

Previous audit results reveal the adequacy of internal controls; moreover, when a full risk assessment project has been carried out by line management, it provides further evidence for the evaluation of controls.

The changes in the organisational structure (generated by merger & acquisitions, downsizing,
and outsourcing) may imply some relevant modifications in the control environment. They could require a review of the control activities, and of the information and communication system, in order to maintain their adequacy.

**Micro risk assessment**

The objective to embrace risks in planning each audit engagement is perceived as less important than in planning the annual schedule of audits. In a few cases (25%), internal auditors just test if the control activities are working as intended. In those cases, the audit work is performed according to a traditional approach, and the scope of the engagement is to verify the compliance of the activities with policies, procedures and rules.

Most companies (67%) state that in the individual audit they apply the COSO model, for the engagement planning and the reporting of internal audit findings. In the planning of individual audits, they generally start from the recognition of significant risks inherent to the activity, in order to limit or expand the testing of controls.

In a small number of companies (8%), the audit objective is based on how management deals with risks and the audit is designed to test risk management techniques (Selim & McNamee, 1998). In these cases the yearly application of CRSA enable auditors to have an understanding of the most important business risks and to focus on the effectiveness of risk management.

In conclusion, it seems that most companies are still following the control paradigm and this reduces the actual contribution of internal auditors to risk management activities.

6. **CONTROL RISK SELF ASSESSMENT**

The last section of the questionnaire aimed at determining the state of the art of Control Risk Self Assessment (CRSA) in large Italian companies. CRSA is a systematic and participative technique used to identify, classify, assess, measure and evaluate risks and controls (IIA, UK and Ireland, 1999).

Actually, different techniques are used in the organisations to identify and assess both risks and controls, called Control Self Assessment (CSA), Control Risk Self Assessment (CRSA), Risk and Control Self Assessment (RCSA), Business Self Assessment (BSA), Management Self Assessment (MSA). Each of these techniques is based on a different methodology and has a different focus, but for our purposes, we do not attempt to identify which method is adopted by Italian companies and we use the term CRSA (to include both CSA/CRSA and the other techniques).

Melville (1999) distinguishes four stages in the history and developments of CSA:
- the introduction in Gulf Canada (1985);
- the ‘early pioneers’ that adopted CSA (1990);
- the ‘wide acceptance’ by internal auditors (1995);
- the CSA as the ‘default internal audit methodology’ (2000).

The research aimed at identifying in which phase of the developments of CRSA mentioned above, Italian companies could be placed, the driving force behind the CRSA and the critical success factors.

Survey results show that, in Italy, CRSA may be considered in a ‘start-up phase’, since it is possible to identify:
- a few ‘early pioneers’ (6) stating to have implemented self assessment throughout their entire organisation;
- some (5) declaring to have started applying CRSA only in a few business areas;
- a number of companies (10) revealing their willingness to introduce it within the next year.

Other companies state that they have no plan to apply CRSA, either they believe that this methodology is not suitable for their organisation or that senior management would not strongly support the project. In small companies, there is insufficient knowledge and experience of this technique.

Only three companies introduced CRSA more than two years ago. The others implemented CRSA in the last two years, but their willingness to repeat it in the near future is not clear.

Generally, at the beginning self assessment was tested in one or two areas (process or subsidiary), in order to verify the opportunity to broaden it to the whole organisation. The pilot project was carried out in those areas having a suitable culture for the successful outcome of CRSA; in most cases, it regards the accounting, the disbursement and the production departments.

All the companies that have implemented a CRSA project declare that it helps management, at all levels, to assume responsibility and accountability for effective control and risk management (Jordan, 1995; McCuaig, 1998). Some
practitioners emphasise that CRSA is a powerful way to improve the organisation’s control environment. Then, it is generally recognised that CRSA offers lots of benefits for audit departments, because it extends the audit coverage, it helps internal audit to focus on risks and to understand the business (Wade & Wynne, 1999; Arthur Andersen, 1994).

Consistent with answers obtained in the ‘risk assessment section’, in the financial institutions regulatory requirements are usually considered as strong incentive factors for the introduction of a self assessment project. Regarding the critical success factors of the project, respondents highlight that the support of senior management is crucial to the success of CRSA. Then, they assert that the corporate culture is vital to the successful launch of the project, in so far as it encourages the active participation of all users.

As far as the CRSA tool is concerned, all survey respondents state that the questionnaire is the main instrument. Only two companies adopt the workshop, in addition to and not in place of the questionnaire.

7. CONCLUSIONS

The analysis of the survey answers indicates the existence of different approaches of internal auditing activities in the Italian context. In fact, on the basis of some relevant variables (size of the audit department; types of auditing; application of control models; introduction of a risk assessment methodology; risk-based auditing; CRSA), we can deduce that practices vary significantly among three different models:

(a) a few companies (25%) have a small audit department carrying out traditional assurance activities. The internal auditor is still perceived as an inspector, and he mainly performs compliance audits. These companies do not integrate the COSO into their audit process, and have a control system entirely based on hard variables. The annual audit planning generally follows an audit-cycle approach. This model often pertains to smaller companies.

(b) In most companies (67%), internal auditors are providing some contributions to the risk management process, and they are trying to incorporate the COSO model in the internal control policies and procedures and in the audit process. In this context, internal auditors perform mainly operational audits and make use of risk assessment findings in planning the annual schedule of audits (macro level). Instead, in planning the individual audits, they generally start from the recognition of significant risks inherent to the activity, in order to limit or expand the test of controls. The audit department of financial institutions generally follows this model.

(c) Finally, it is possible to identify a very few large companies (8%), in which the audit unit is focused also on consulting activities. Internal auditors attempt to add value through a more active support to risk management at different levels, and to align internal audit objectives with the strategic goals of the organisation. This group includes the ‘early pioneers’ of CRSA projects, in so far as they aim at strengthening the accountability at all levels of management for risk and control. They focus their work on significant risks, and they are trying to adopt a collaborative approach with line management. Actually, a risk-based approach is applied both at macro and micro level, so that we can assume that they are embracing the risk paradigm (Selim & McNamee, 1998). Furthermore, internal auditors focus the monitoring activities on soft controls.

Finally, it is worthy of mention that the scenarios of internal auditing in the Italian context could change in the near future, mainly for two factors:

- the pressures on organisations to ensure the reliability of financial statements (following Enron and WorldCom scandals) could imply an increase in the financial auditing activities;
- the enforcement of the new company law from 2004 could imply a new corporate governance framework in the Italian system.

NOTE

1. We refer to the official composition of the Italian Stock Exchange in the third quarter of 2002.

REFERENCES


Chambers, A. (1999), ‘Quo vadis internal auditing?’, Management Accounting, October.
Committee of Sponsoring Organization of the Tradeway Commission (COSO), (1992), Internal Control – Integrated Framework, Jersey City, AICPA/COSO.
German Accounting Standards Committee, (2001), E-GAS 5, Risk Reporting.
Italian Committee for the Corporate Governance of Listed Companies, (1999), Report, Code of Conduct.
Sawyer, L. B. (1996), Sawyer’s Internal Auditing, 4th edition, Altomonte, IIA.
The Institute of Internal Auditors (UK and Ireland), (1999), Control and Risk Self Assessment, Professional Briefing Note n. 14, London, UK: Institute of Internal Auditors United Kingdom and Ireland.
The Institute of Internal Auditors (UK and Ireland), (2002), The Role of Internal Audit in Risk Management, Position Statement.
The Institute of Internal Auditors, (2002), Professional Practice Framework (The Standards for the Professional Practice of Internal Auditing), The Institute of Internal Auditors.

**AUTHOR PROFILES**

**Marco Allegrini** is Associate Professor at the University of Pisa, where he is investigating corporate governance and business communication issues.

**Giuseppe D’Onza** is a PhD student in ‘Business Economics’ at the University of Pisa, and he is carrying out research in internal auditing and business strategy.

This paper is the result of joint research. However, Marco Allegrini is the author of sections 1, 2, 3 and 7; Giuseppe D’Onza is the author of sections 4, 5 and 6.
QUESTIONNAIRE

Section A: Background information

1. General information regarding the organisation

<table>
<thead>
<tr>
<th>Name of the organisation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Headquarters of organisation (city and country)</td>
<td></td>
</tr>
<tr>
<td>Name of the Business Group</td>
<td></td>
</tr>
</tbody>
</table>

2. Main business of the organisation:

<table>
<thead>
<tr>
<th>Finance/banking</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing/retail</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td></td>
</tr>
</tbody>
</table>

3. Number of employees in your organisation

<table>
<thead>
<tr>
<th>&lt;1,000 (please specify)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000–2,000 (please specify)</td>
<td></td>
</tr>
<tr>
<td>&gt;2,000 (please specify)</td>
<td></td>
</tr>
</tbody>
</table>

4. Number of auditors in your organisation (please specify)

<table>
<thead>
<tr>
<th>1–10</th>
<th>11–20</th>
<th>21–30</th>
<th>31–40</th>
<th>&gt;40</th>
</tr>
</thead>
</table>

5. Who does the chief internal auditor hierarchically depend from?

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Board of Directors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Chairman</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Chief Executive Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Board of Auditors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E. Audit committee</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F. Line management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G. Others (please specify)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. Who shall the director of the internal auditing department periodically report to? Please also indicate the frequency.

A. Board of Directors
B. Chief Executive Officer
C. Chairman
D. Board of Auditors
E. Audit committee
F. Line management
G. Other (please specify)

7. In case your organisation belongs to a business group:

Only the parent company has a structured internal audit department, and it carries out auditing activities for all the subsidiaries (centralised model)

A new company is purposely established to perform auditing activities for the whole business group (delegation model)

Audit departments are established in two or more companies of the group (widespread model)

8. Relationship between audit departments of the same business group:

Parent’s audit department co-ordinates all the subsidiaries’ audit departments’ activities

Subsidiaries’ audit departments plan and perform activities autonomously

Other (please specify)

Do subsidiaries use parent company audit resources for specific engagements (IT auditing, fraud auditing, ethical auditing, environmental auditing, etc.)?  

Yes  No
9. How much of your planned annual auditing activity is devoted to: (in percentage)

<table>
<thead>
<tr>
<th>Type of Audit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial audit for public financial statements</td>
<td></td>
</tr>
<tr>
<td>Audit of the management information system</td>
<td></td>
</tr>
<tr>
<td>Operational audit</td>
<td></td>
</tr>
<tr>
<td>Compliance audit</td>
<td></td>
</tr>
<tr>
<td>Special projects</td>
<td></td>
</tr>
<tr>
<td>IT Audit</td>
<td></td>
</tr>
<tr>
<td>Fraud investigation</td>
<td></td>
</tr>
<tr>
<td>Risk assessment</td>
<td></td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**Section B: Control models**

1. Please indicate the extent to which you agree or disagree with the following statements about Control Models:

   *(Key: SD = Strongly Disagree; D = Disagree; A = Agree; SA = Strongly Agree; DK = Don’t Know/Neutral)*

<table>
<thead>
<tr>
<th>Statement</th>
<th>SD</th>
<th>D</th>
<th>A</th>
<th>SA</th>
<th>DK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control models provide an effective basis for designing the internal control system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control models provide an effective basis for control system reviews</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control models provide an effective support for the reporting of internal auditing findings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control models are used widely in my organisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senior management in my organisation is strongly interested in the control environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal auditors in my organisation address qualitative issues in their work (for example, communication, management information, ethical issues, equal opportunities)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Section C: Risk assessment practices and risk-based auditing

1. Has your organisation introduced a formalised risk assessment process?
   - Yes
   - No
   - We are introducing it

2. When did the business process risk assessment begin?
   - In the last year
   - More than 1 year ago (please specify)
   - We are introducing it

3. Does your organisation have a formal risk management department? Please describe the relationship between the risk management unit and the internal audit one.

4. In your organisation, the risk assessment is carried out by:
   1. Internal auditors in co-operation with the line management
   2. External consultants in co-operation with the line management and with the support of Internal auditors
   3. Management during the Control Risk Self Assessment facilitated by Internal auditors
   4. Internal auditors in co-operation with external consultants but without the involvement of the line management
   5. No role of internal auditors (please specify)

5. In which areas have you implemented the risk assessment activity?
   1. In all the functions and processes of the organisation
   2. Production
   3. Research and Development
   4. Finance
   5. Organisational and human resources
   6. Accounting
   7. Marketing and sales
   8. Purchasing
   9. Information systems
   10. Other (please specify)
6. In your organisation, which are the main objectives of the risk assessment activity?
(Key: Lowest = 1; Highest = 4)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Developing a systematic approach that management could use in dealing with the risk</td>
</tr>
<tr>
<td>2</td>
<td>Identifying most critical areas to define the audit plan (macro risk assessment)</td>
</tr>
<tr>
<td>3</td>
<td>Embracing risks in individual audit (micro risk assessment)</td>
</tr>
<tr>
<td>4</td>
<td>Complying with the regulatory requirement</td>
</tr>
<tr>
<td>5</td>
<td>External risk reporting</td>
</tr>
<tr>
<td>6</td>
<td>Value creation</td>
</tr>
<tr>
<td>7</td>
<td>Other (please specify)</td>
</tr>
</tbody>
</table>

7. Effects of D.Lgs. 231/2001 (corporate fraud law) on risk assessment:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The organisation had not yet introduced a formalised risk assessment process. However, it is going to work out and implement some specific fraud assessment project consistent with the Law 231</td>
<td></td>
</tr>
<tr>
<td>The organisation had already introduced a formalised risk assessment process. However, it could work out and implement a specific project consistent with the model established by the Law 231</td>
<td></td>
</tr>
<tr>
<td>No fraud risk assessment activity will be carried out</td>
<td></td>
</tr>
</tbody>
</table>

8. If risk assessment implementation was successful, please assess the following factors:
(Key: Lowest = 1; Highest = 4)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear definition and communication of objectives</td>
<td></td>
</tr>
<tr>
<td>Culture and attitudes towards controls and risks</td>
<td></td>
</tr>
<tr>
<td>Clear identification of processes and their owners</td>
<td></td>
</tr>
<tr>
<td>Management support at top level</td>
<td></td>
</tr>
<tr>
<td>Development of a formal risk assessment model</td>
<td></td>
</tr>
</tbody>
</table>

9. The audit plan is prepared according to:
(Key: Lowest = 1; Highest = 4)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests of senior management</td>
<td></td>
</tr>
<tr>
<td>Risk-based approach</td>
<td></td>
</tr>
<tr>
<td>Cycle-based approach</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>
10. In case of risk-based audit planning, which are the risk factors taken into account? (Key: Lowest = 1; Highest = 4)

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional competence of the human resources</td>
<td></td>
</tr>
<tr>
<td>Changes in the organisational structure (merger and acquisitions, downsizing, outsourcing)</td>
<td></td>
</tr>
<tr>
<td>Impact of activities on the corporate image</td>
<td></td>
</tr>
<tr>
<td>Complexity of operations</td>
<td></td>
</tr>
<tr>
<td>Adequacy of internal controls</td>
<td></td>
</tr>
<tr>
<td>Degree of automation</td>
<td></td>
</tr>
<tr>
<td>Relationship with State and governmental organisations</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
</tbody>
</table>

**Section D: General CRSA questions**

1. Have you used CRSA in the last three years?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>We are going to introduce it in the next year</td>
</tr>
</tbody>
</table>

2. How long have you used CRSA in your organisation?

<table>
<thead>
<tr>
<th>Duration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;12 months</td>
<td></td>
</tr>
<tr>
<td>13–&lt;24 months</td>
<td></td>
</tr>
<tr>
<td>24–&lt;36 months</td>
<td></td>
</tr>
<tr>
<td>&gt;36 months</td>
<td></td>
</tr>
</tbody>
</table>
3. In which areas have you implemented CRSA?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In all the functions and processes of the organisation</td>
</tr>
<tr>
<td>2.</td>
<td>Production</td>
</tr>
<tr>
<td>3.</td>
<td>Research and Development</td>
</tr>
<tr>
<td>4.</td>
<td>Finance</td>
</tr>
<tr>
<td>5.</td>
<td>Organisational and human resources</td>
</tr>
<tr>
<td>6.</td>
<td>Accounting</td>
</tr>
<tr>
<td>7.</td>
<td>Marketing and sales</td>
</tr>
<tr>
<td>8.</td>
<td>Purchasing</td>
</tr>
<tr>
<td>9.</td>
<td>Information systems</td>
</tr>
<tr>
<td>10.</td>
<td>Other (please specify)</td>
</tr>
</tbody>
</table>

4. For what reasons have you introduced the CRSA in your organisation (Key: Lowest = 1; Highest = 4)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>To increase the audit coverage with the same audit resources</td>
</tr>
<tr>
<td>2.</td>
<td>To comply with the law (L. 231/2001)</td>
</tr>
<tr>
<td>3.</td>
<td>To carry out a business process reengineering project</td>
</tr>
<tr>
<td>4.</td>
<td>To improve internal communication of objectives (management by objectives)</td>
</tr>
<tr>
<td>5.</td>
<td>To achieve a learning process for participants</td>
</tr>
<tr>
<td>6.</td>
<td>To help management at all levels to assume responsibility and accountability for effective control and risk management</td>
</tr>
<tr>
<td>7.</td>
<td>To support the business planning strategy</td>
</tr>
<tr>
<td>8.</td>
<td>Others (please specify)</td>
</tr>
</tbody>
</table>

5. If CRSA implementation was successful, please rank the following factors: (Key: Lowest = 1; Highest = 4)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>Management support at top level</td>
</tr>
<tr>
<td>B.</td>
<td>Users were included in the preparation</td>
</tr>
<tr>
<td>C.</td>
<td>An effective planning of the workshop</td>
</tr>
<tr>
<td>D.</td>
<td>Skills of the facilitator</td>
</tr>
</tbody>
</table>
6. Which tools have you used for CRSA?

| Questionnaire | Workshop | Seminars | More instruments | Others (please specify) |

Section E: Further information

Please add any specific or general comments on the issues raised in this questionnaire that you feel have not been sufficiently addressed.