IT Auditing in Italian Banks: An Explanatory Study

Rita Lamboglia and Giuseppe D'Onza

Abstract This study analyses the characteristics of IT auditing in banks. Based upon two Italian case studies, the article provides a qualitative assessment of the objectives of the IT audit, the activities performed, the stakeholders served and the critical success factors that influence the capability of IT auditing to add value. The results show that the scope of the IT auditing function has extended; nowadays senior managers expect IT auditors to support them in the evaluation of the IT system and in the assessment of IT security controls. Regarding IT auditing activities, the most commonly performed are risk assessment and information security risk assessment. Considering stakeholders, the interviewees revealed that the main stakeholders are executive managers, while the critical success factors are the characteristics of the control environment, the capacity of the IT auditor to stay in touch with the business, and behavioural skills.

Keywords IT auditing · Banks · Case study

1 Introduction

In recent years, the importance of Information Technology (IT) auditing has grown with the increase of the demand for control mechanisms that can protect the value IT systems could deliver to enhance corporate business processes. A global study on internal auditing activities (entitled "Common Body of Knowledge in Internal Auditing"), carried out in 2010 [1], highlighted that the audit engagement on IT/ICT systems ranks sixth among the 25 activities considered in the study [2].

R. Lamboglia (✉) · G. D'Onza
Department of Business Administration, University of Pisa, Pisa, Italy
e-mail: rlamboglia@ec.unipi.it

G. D'Onza
e-mail: gdonza@ec.unipi.it

D. Baglieri et al. (eds.), *Information Systems, Management, Organization and Control*, Lecture Notes in Information Systems and Organisation 6,
DOI: 10.1007/978-3-319-07905-9_7,

The analysis of these results per industry shows that banks and insurance companies are the organizations where IT auditing engagements show the highest percentage and are performed by more than 80 % of 13,500 internal auditors who took part in that survey [3].

The most likely reason of these results is that financial companies show extensive adoption of IT to process their operations, and this has created a strong demand of assurance and consulting activities regarding the IT systems.

Another possible reason is that, since 2004, bank supervisory authorities have issued some regulations and exerted a certain pressure on financial companies to establish and periodically test the adequacy of internal controls over IT processes and resources.

Despite the importance recognized to IT auditing as an essential service to improve the effectiveness of the IS in the financial industry, there is still a very limited number of studies that investigated this topic in this industry.

Some studies analysed the problem of control over IT systems in relation to the decision of banks to outsource their IS function [4, 5], which highlighted that the need to maintain control over outsourced IS applications may increase their transaction costs. The presence of these costs could lead to the decision to manage IT services in house or through the parent company.

Other researchers [6] investigated the benefits internal auditors may obtain through a more intensive use of audit technology tools, due to the opportunity to process a large amount of data for auditing purposes in banks, as well as in other entities.

Therefore, the topic of IT auditing in banks remains quite unexplored in academics and professional studies.

This paper aims at contributing to the literature by analysing the characteristics of IT auditing in two large Italian banks. More specifically, the paper focuses on the following topics: the objectives of the IT audit department, the activities performed, the stakeholders served, and the critical success factors that influence the capability of IT auditing activities to add value.

The remainder of the paper is organized as follows: the second section reviews the relevant literature and formulates the research questions; the third section outlines the methodology used to carry out this study; the fourth section presents the results of the interviews; and the last section summaries and discusses the conclusions of this study.

2 Literature Review and Research Questions

IT auditing is part of the managerial control exercised over a company's IT system, which is designed and implemented in order to help a growing number of organizations monitor the effectiveness of their IT risk management system.

Despite its relatively short history, IT auditing has rapidly evolved over time as a result of the swift development featuring the use of information technology in business processes.

These changes concern many characteristics of IT auditing like the roles and objectives associated to that activity, the stakeholders it serves, the type of engagements performed, the skills and competencies IT auditors should possess to carry out their tasks effectively [7].

When considering the objectives of IT auditing, the definitions provided by academic and professional studies highlight different goals organizations could achieve by setting up this activity.

One of the most commonly adopted definitions identifies an IT audit as [8, 9] "a process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, achieves organizational goals effectively, consumes resources efficiently".

Other definitions highlighted the organizational perspective of IT auditing and defined this activity as a process for "discovering, monitoring and evaluating an organisation's information resources in order to implement, maintain, or improve the organisation's management of information" [10].

Another definition considers IT auditing as an independent and objective assurance and consulting activity performed with the aim of analysing whether the risks and controls related to the information systems are properly managed.

As an example, the assessment of IT risks and controls may be performed with the purpose of analysing if:

- the company's IT resources are effectively safeguarded;
- the integrity, confidentiality, and reliability of information are maintained;
- IT processes and resources assist the organization in achieving its business objectives (effectiveness);
- the IT strategy is aligned with the business strategy and allows the company to get a high return from the IT investment.

Taking all these definitions together, it clearly appears that the objectives of the IT audit department may vary between companies and encompass different features. Based on these considerations, we considered it interesting to analyse the objective of IT auditing in the banks under examination. So, our first research question is:

RQ1: Which are the main objectives of IT auditing in Italian banks?

The IT audit department performs a great number of activities because nowadays auditors serve a greater number of customers than in the past.

When considering the taxonomy of IT auditing, it is worth noting the variety of classifications existing in the literature.

A traditional and widespread classification distinguishes between auditing general IT controls and auditing IT application controls [11].

A growing number of authors have adopted the classification proposed by the CobiTframework to categorize IT auditing. These activities are often classified considering two dimensions of the "CobiT cube": the type of IT processes analysed and the business requirements to be met by the audit [12]. Regarding IT processes, auditing activities are classified based on each phase of the IT system's life cycle by distinguishing, for example, the audit of the hardware procurement process from IT implementation and support.

When analysing business requirements, IT audits are classified into security, compliance, reliability, effectiveness, etc.

Other authors [13] combined these two dimensions and proposed the following classes: organizational IT audits; technical IT audits; application IT audit; development/implementation IT audits; compliance IT audits.

When we looked at the IT auditing activities proposed by the academic and professional literature, interestingly we noticed that there are many other activities, like the assessment of the disaster recovery plan, the review of software development documentation, and so on.

These considerations point out the difficulties one encounters when trying to develop a comprehensive list of IT auditing activities, as well as when seeking to define boundaries between those activities.

For the purpose of this study, researchers used the classification proposed by Moeller [14] on the hierarchy of control measures, integrated with the CobiT model [15]. Figure 1 shows the IT control hierarchy with, at the top of the model, IT governance controls; the second level refers toIT management controls, and IT technical controls are shown in the lower part of the figure.

A brief explanation of IT auditing, regarding each of the three control levels, is given below.

The importance of IT governance has grown over time, with increasing investments made by the organizations in their IT systems and with the greater significance these systems have acquired for the company's competitiveness and profitability.

There is a variety of definitions of IT governance. According to Moeller [14], "IT internal controls at governance level involve ensuring that effective IT management and security principles, policies, and processes with appropriate compliance measurement tools are in place".

The IT Governance Institute (ITGI) provides a broader definition of IT governance: "the leadership and organizational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives" [16]. The ITGI recognized the importance of IT Governance with the issuance, in 2005, of the COBIT 4.0 framework regarding IT governance.

The CobiT model [15] identifies five areas of control, namely (Fig. 2):

1. Strategic Alignment
2. Value Delivery
3. Risk Management
4. Resource Management
5. Performance Measurement

Fig. 1 IT general and application control hierarchy. *Source* Moeller 2010, p. 156

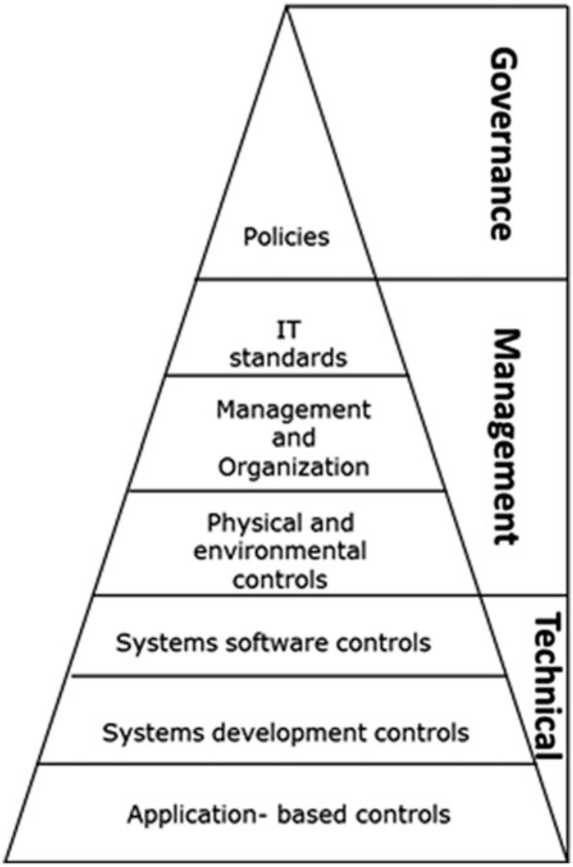
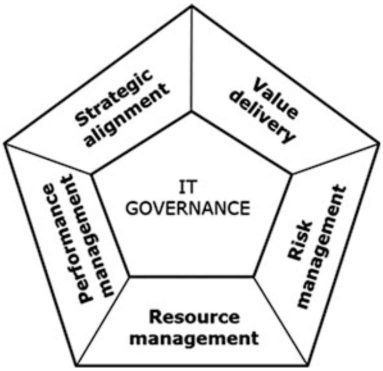

Governance
Policies
Management
IT standards
Management and Organization
Physical and environmental controls
Technical
Systems software controls
Systems development controls
Application- based controls

Fig. 2 COBIT IT governance focus. *Source* CobiT 4.0



Strategic Alignment regards the connection between the company's strategic plan and IT plans and its purpose is to ensure that strategic goals are supported by IT investments. Auditing strategic alignment means to analyse: (1) the strategic fit of IT systems in terms of how IT supports the implementation of the business strategies of the company or creates new business opportunities; and (2) functional integration, which concerns how the choices made in the IT domains (architecture, process, people) impact the business domain and vice versa [17].

The assessment of Value Delivery aims at examining if IT systems deliver the promised benefits and if their output is in line with the defined business requirements. The achievement of this goal requires an adequate use of applications, information and technology solutions.

The analysis of Resource Management regards the optimization of the IT investment and a proper management of critical IT resources: processes, people, applications, infrastructure and information.

Risk Management is audited by referring to the policies the organization adopts to manage its IT risks effectively, in order to ensure that these risks are properly understood and effectively managed at all organizational levels.

Performance Measurement examines strategy implementation, project completion, the use of resources, process performance and service delivery. It includes setting and monitoring measurable objectives for IT process deliverables (process outcomes) and how they are delivered (process capability and performance).

As shown in Fig. 1, general IT management controls include: IT standards, management and organization, physical and environmental controls.

Regarding IT standards, IT auditors should identify and assess whether the processes, policies and procedures that allow IT systems to work effectively and deliver their services have been established, communicated to and followed by all the members of the IT organizations. These standards generally cover the phases of the IT system's life cycle and could regard many processes like IT service design, change and configuration management, operation and incident management, control procedure documentation.

The second level of general IT management controls regards the IT organization and management processes. IT auditors should review the organizational and managerial controls existing in the IT function. These auditing activities address different issues like there view the presence of an adequate, updated and documented disaster recovery plan, the existence of an IT business continuity management process, the asset management process of IT resources, etc.

The third component of IT management control concerns physical and environmental controls. In order to provide a broader view of these controls, researchers have renamed this level "IT security controls" to encompass all the actions taken to mitigate security risks and build up an effective IT security environment. Regarding this area, IT auditors could help the company improve its IT security strategy and security standards, mechanisms and procedures in place.

The last level of the IT control hierarchy describes IT technical controls, which include: system software controls, system development controls and application-based general controls.

The audit work on system software controls and system development controls consists in reviewing controls regarding the operating system (OS), the database management system and other operating programs. The objective of this audit could involve different issues like the authorization rules for software installation, the maintenance and upgrading of programs.

Application-based controls refer to the review of IT applications, which are used by companies to support a variety of processes such as accounting, procurement, production, marketing. IT auditors are required to evaluate the adequacy and operation of the application systems and their capability to contribute to the effectiveness of the business processes.

Figure 3 shows the model researchers used to analyse the IT auditing activities performed by banks, with the integration of the control hierarchy proposed by Moeller with the COBIT 4.0 framework [15].

In order to analyse the activities carried out by the banks at issue, researchers formulated the following research question:

RQ2: Which the activities shown in Fig. 3 is/are performed in the companies analysed?

The studies conducted on IT auditing highlighted that the number of stakeholders served by this activity has increased during the years. While, at an early stage, EDP auditors worked mainly to support external auditors, their activity has expanded over time to meet the demand of assurance and consulting activities coming from other parties like the IT function, senior managers, the board of directors, the audit committee, etc. [18].

Regarding banks, the regulatory framework defined by the Supervisory Authorities considers IT auditors as part of the “third line of defence”, which provide an independent assurance to the Board of Directors, business unit executives and the Audit Committee on the management of IT risks and on the status of the IT controls incorporated in the business processes (“first line of defence”). As a “third line of defence”, IT auditors are also required to provide an independent assurance on those functions (like the risk management unit) that oversee IT risks and controls as a “second line of defence”.

Significant differences are generally recognized in describing the relative power of these stakeholders [19]. In this context, it is worthwhile analysing the perception of the interviewees regarding the following research question:

RQ3: Who are the main stakeholders of IT auditors?

The literature on the value drivers of the auditing activity shows many factors that may affect the capacity of this activity to add value for the organization it serves [20–22].

These factors are: the characteristics of auditors (e.g. objectivity, credibility, leadership, skills, etc.); the way activities are performed and the tools used (e.g. risk-based audit plans, risk assessment methodology, etc.); the environment where auditors perform their engagements (e.g. characteristics of the control environment, support by the top management, etc.).

When considering the studies on the critical success factors of IT auditing, other variables could be identified, such as ethical standards for IT auditors, adequate

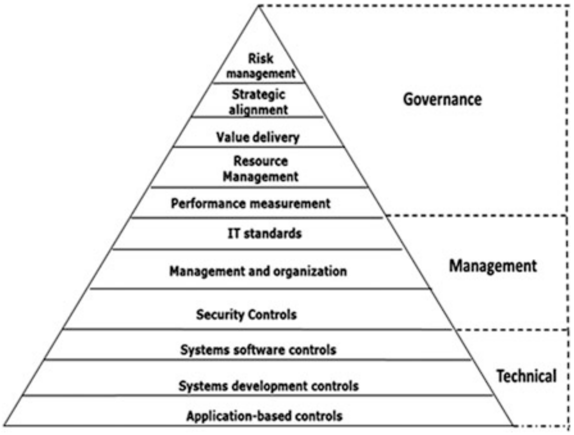


Fig. 3 IT auditing activities

planning of the IT engagement, and so on [23]. These mixed evidences highlight that a dominant model does not exist and that additional analysis is needed on this subject. All these considerations lead us to the following research question:

RQ4: What are the main critical success factors for IT auditing activities?

3 Research Methodology

Researchers decided to focus their investigation on the banking industry. The reasons behind this decision have been extensively described in the introduction.

This study concerned the two largest Italian banking groups. We selected the largest organizations based on the evidence of a previous research, which described a positive relationship between firm size and the creation of an IT audit function [24].

Furthermore, these groups operate on an international scale and their parent companies are both listed in the Milan Stock Exchange.

We used a holistic case study method to describe the IT auditing phenomenon in its real-life context.

To select the two case studies inspired by previous research on internal audit, we also took into account the age of the internal audit function [25], as well as the number of internal auditors. Concerning these parameters, we included a company with a mature internal audit function and with a large internal audit department.

Table 1 shows some characteristics of the case studies that have similarities. This will increase the comparability of results [26].

Researchers conducted semi-structured interviews with the head of the IT audit department.

An interview protocol was developed commencing with open-ended questions regarding general subjects, like the role of IT auditing in the banks, the professional background of IT auditors, the years of existence of the IT auditing function, etc.

Table 1 Characteristics of the banks analysed

Variables	Case study 1	Case study 2
Reporting line of IT audit manager	Chief audit executive	Chief audit executive
Number of employees in IT audit department	30	17
Employees in IT audit versus employees in IA unit	15 %	13 %
Years of existence of IT auditing department	More than 20 years	More than 20 years
IT auditing % outsourced	0 %	0 %

More specific questions relating to the objectives of IT auditing and the activities carried out were also examined. A sample of the questions posed is given below:

1. What are the objectives of your IT audit department?
2. What are the activities your IT audit department currently performs? What changes do you expect in the next 5 years for your auditing activities?
3. Who are your main stakeholders? What do you think they expect from your department?
4. What are the critical success factors of your activity?

The analysis of these qualitative data was based on the analytical protocol recommended by Miles and Huberman [27].

More specifically, the interviews were transcribed and read through several times to identify the themes. Since the interview questions were categorised under headings prior to the interview, this process itself helped align the themes drawn from the literature with the answers to the questions. The interviews lasted on average 1 h and they were completed in July 2013.

Documents like the IT audit charter, the IT audit manual, the organizational chart of the IT audit function were read through to gain a general understanding of the demographics and other significant contextual factors pertaining to that particular organization.

Next, the most important observations were summarised and sent back to the interviewees to obtain their confirmation.

4 Empirical Results

As discussed in the research method section, an analysis of the interview transcripts was undertaken to develop the themes. The themes extrapolated from the interviews pertained to issues raised from the literature review.

4.1 Objectives of the IT Audit Department

The findings suggest that the objectives of IT auditing have changed over the years. While, at an early stage, the creation of the EDP audit function was driven by the necessity to ensure the effectiveness of general and application controls over the IT system, nowadays the scope of this activity has expanded to provide assurance on the governance and management processes regarding IT systems.

> The IT audit function has been set up during the eighties. Initially, it was a technical unit whose task was to evaluate and improve control over the IS infrastructure and applications. Today the scope of theIT auditing function has expanded. In summary, the current purpose is to assess the capacity of IT systems to help the business unit and company achieve their objectives. (Case study 1)

> The IT audit unit has existed for over 20 years and its development has gone hand in hand with the more pervasive use of IT resources in the business process. The role of the IT audit department has changed from a review of the technical aspects of the IT system to the monitoring of all IT processes and supervision of the management of IT-related risks. (Case study 2)

These changes reflect the fact that investment in IT systems has increased over time. IT is increasingly perceived as a critical asset for the competitiveness of a bank and financial regulators asked the banks to enhance their internal control systems concerning IT processes.

> The growth in IT investments has emphasised the need for the CEO and senior managers to understand the value delivered by these investments, ensure whether IT meets business requirements and assess users’ satisfaction with IT resources. (Case study 1)

The evolution of the expectations of the main stakeholders determined the need to revise the objectives of the IT audit function. There has been an extension of the scope of this activity, that should continue to analyse risks and control at a technical level, to review IT security controls and be able to support the senior management in understanding the value created by IT systems.

> In particular, the objectives of IT auditing are: (1) to assess the effectiveness of the control of the design, development and management of IT systems in order to assess the reliability, integrity and availability of information and its capacity to support the business processes, (2) to monitor IT-related risks and the measures implemented to mitigate those risks; (3) to assure the adequacy and effectiveness of IT security strategies, policies and tools. (Case study 2)

> Senior managers expect IT auditors to support them in the assessment of the capacity of IT systems to improve the efficiency and effectiveness of the business process and ensure the integrity of the information used for processing operations. (Case study 1)

4.2 Activities Performed

The results regarding IT auditing activities are summarized in the following tables.

The list provided in Fig. 3 has been used to evaluate the IT activities carried out. The tables show the interviewees’ evaluation of the fact that they are currently performing the activities proposed and their opinion on whether they expect the effort devoted to these activities will increase, stay the same or decrease in the next 5 years.

The findings show that today the involvement of the IA unit in IT governance is limited to risk assessment. Both the interviewees declared they are monitoring risk assessment and risk management processes in order to understand if the risks associated with IT processes and infrastructures have been identified and managed accurately. It is interesting to highlight that the goal of the analysis is to cover all the risks associated with IT systems (Table 2).

As highlighted by the interviewees, even though IT security risk is probably the main IT risk, it is also important to analyze those situations that may have a negative impact on the effectiveness of the IT processes. Regarding the other activities that are part of IT governance, most of them today do not fall into the domain of the IT auditing unit. However, the interviewees expect to play a more important role in the future in order to meet an increasing demand of consulting and assurance services from the senior management and the IT function.

Regarding IT management controls, the interviewees highlighted that the auditing of information security controls is vital in the current environment and they expect the time they spend on these activities to increase in the future. The massive use of e-banking and the need to protect the confidentiality, integrity and reliability of the data and information processed make the review of the control of IT security risks one of absolute priority for IT auditing. Security controls also play an important role to mitigate the reputational risk (Table 3).

When considering IT standards, Case Study 1 shows the need to improve the policies adopted by the company to regulate the development of its IT systems, the acquisition of hardware and software, and IT documentation. This activity is not performed in Case Study 2, and there is no expectation to see this engagement included in future audit plans.

Both interviewees declared they perform a regular assessment of the management of IT systems in their business group. This assessment mainly focuses on the disaster recovery plan and the business continuity plan (Table 4).

Considering technical controls, the respondents indicated that IT auditors regularly perform these activities.

Regarding system software controls, the interviewees highlighted that their audit programs envisage the review of the controls related to the management of the operating system, the database management system and other programs used by the bank to process transactions. They expect the importance of this activity to stay the same in the upcoming years.

Moreover, auditing involves the review of IT application controls, which are used to handle operations that include processes like payment, lending, accounting, etc. Even in this case, the interviewees believed that the importance would remain the same in the upcoming years.

Table 2 IT governance activities

		Case study 1		Case study 2	
		Today	Future perspectives	Today	Future perspectives
Governance	Strategic alignment	No	Increase	No	Stay the same
	Risk management	Yes	Increase	Yes	Increase
	Value delivery	No	Increase	No	Stay the same
	Resource management	No	Increase	Yes	Increase
	Performance measurement	No	Increase	No	Increase

Table 3 IT management activities

		Case study 1		Case study 2	
		Today	Future perspectives	Today	Future perspectives
Management	IT Standards	Yes	Stay the same	No	Stay the same
	Management and organization	Yes	Stay the same	Yes	Stay the same
	Security controls	Yes	Increase	Yes	Increase

Table 4 IT technical activities

		Case study 2		Case study 2	
		Today	Future perspectives	Today	Future perspectives
Technical	Systems software controls	Yes	Stay the same	Yes	Stay the same
	Systems development controls	Yes	Increase	Yes	Stay the same
	Application-based controls	Yes	Stay the same	Yes	Stay the same

4.3 Stakeholders of IT Auditing

When considering the stakeholders of IT auditing, the interviewee pointed out that they serve multiple stakeholders.

Interviewees were asked to indicate which are the most important stakeholders.

> To provide a ranking on our most important stakeholder, I have to indicate:
>
> 1. Chief Operating Officer
> 2. Chief Risk Officer
> 3. Chief Financial Officer
> 4. Head of IT department. (Case study 1)

When considering relationships with these stakeholders, the interviewees indicated that they submit a quarterly report to their stakeholders with a summary of IT audit results and with an overall assessment of IT controls, the main IT risks that require further action and the remediation plan defined to reduce the risks down to an acceptable level.

Other recipients of the IT audit reports are the Chief Audit Executive and External Auditors.

Regarding the second interviewee, the answer was that

> the main stakeholders of the IT audit activities are:
> 1. Business line managers
> 2. The IT department
> 3. The IT security unit
> 4. Risk Management
> 5. The Internal Audit unit". (Case study 2)

Unlike Case Study 1, the IT audit department does not have a direct relationship with the Senior Management of the bank, but they interface with the head of the IA unit. The findings of IT audits are reported to the Chief Audit Executive (CAE), who, in his turn, includes the assessment made by the IT audit unit in an aggregate report on the internal control system, which is submitted to the appropriate member of the Senior Management and control governance.

When functional relationships with the Board of Director were considered, both interviewees indicated that they were managed by the CAE. The assessment of IT controls is part of the overall assessment of the internal control system, which is submitted by the CAE to the Board members.

The interviewee indicated that the more extensive use of IT made the assessment of the control over these system much more important in order to provide the CEO, the Board of Directors and the Audit Committee with an overall assessment of the adequacy of the whole internal control system.

IT controls are an important part of the actions taken to mitigate operational and reputational risks. These findings may help explain why the Chief Operating Officer and the Chief Risk Management are considered two important clients of IT auditing activities, as they provide these figures with the information they may use to monitor how these risks are managed.

The IT department is often considered the traditional auditee. Both interviewees highlighted they have a cooperative relationship with their IT department.

> During the last year, our IT audit unit provided the IT department with many consulting activities regarding, for example, the testing of the software developed internally by the IT function. (Case study 2)

The interviewees considered the CFO as an important stakeholder for activities focused on the control of financial reporting. For this activity, they also indicated that another recipient of the audit report is the external auditor. Since the introduction of the Italian SOX (Law 262/2005), which requires CFOs to publicly disclose the results of the assessment of their internal financial reporting control system, the IT audit plan includes the test that this unit carries out to support the CFO in performing that assessment.

4.4 Critical Success Factors of IT Auditing

The fourth theme analysed regards the critical success factors that influence the capability of the IT auditing activities to add value.

According to one interviewee, the critical success factors that add value are:

- *The Senior Management's support*
- *Leadership*
- *Communication skills*
- *The presence of a strong control environment in the organization*
- *The capacity to understand the company's IT risks and, based on this assessment, to set up the audit plan* (Case study 1)

As highlighted by the second interviewee, the capacity of IT auditors to generate value is affected by:

- *An expert and well trained audit staff*
- *Top managers' support*
- *The ability to understand problems (risks) related to the IT system and provide valuable recommendations*
- *The ability to build positive relationship with the IT department* (Case study 1)

It is worth noting that both IT auditors consider the support of the Senior Management and the ability to understand IT system-related risks to be a critical variable for adding value. Moreover, they both highlighted some behavioural skills—i.e. leadership, communication skills, capacity to build a positive relationship with the IT department.

5 Conclusions and Further Research

This article provides empirical evidence on the objectives of the IT audit department, the activities performed, the stakeholders served, and the critical success factors for the ability of IT audits to add value.

Regarding the objectives, we found that the scope of the IT auditing function has expanded during the year. While, in the past, the objective was mainly focused on the review of general and application controls, nowadays Senior Managers expect IT auditors to support them in the evaluation of the effectiveness of the IT system, as well as in the assessment of IT security controls.

Risk assessment and information security are two of the most performed IT auditing activities. Regarding IT risks, our interviewees highlighted that they are trying to adopt a holistic approach where all types of risks are considered in their assessments. IT security represents a priority to protect the banks against the cyber-attacks and ensure the integrity of the information processed. Therefore, the IT security audit is the primary activity performed.

Our interviewees said they expect the importance of both these activities to increase in the future.

When considering the stakeholders of IT auditors, the interviewees highlighted that the number of customers they serve has increased over time. The findings of our survey suggest that they consider executive managers as their main customers. They do not directly report to the Board of Directors and Audit Committee. However, their assessment is part of the overall evaluation report of the internal control system that is submitted by the Chief Audit Executive to the Board.

The interviewees highlighted that the capacity of IT audits to add value depends on three main factors. The first concerns the characteristics of the environment where IT auditors operate, because the support received by the IT audit unit from the CEO and the Senior Management is crucial for the success of the work performed by IT auditors. The second factor is the capacity of IT auditors to stay in touch with the organisation and understand the main risks posed by its IT system. The third factor is connected with behavioural skills, such as leadership and relationship building.

This study has two main limitations. First, we analysed only two case studies, a condition that does not offer sufficient ground for a generalization of the research findings. Secondly, our findings reflect the perspective of a single observer, even though we have tried to mitigate this limitation by analysing the company's documents during the project.

Our paper contributes to the literature on IT auditing and may suggest that IT auditing is a promising area for future research. Future researchers should undertake large-scale surveys to analyse the characteristics of IT auditing activities in banking or other sectors.

References

1. CBOK: Common Body of Knowledge IN Internal Auditing. Project in Progress. The Institute of Internal Auditors, Altamonte Springs, FL (2010)
2. Alkafaji, Y., Hussain, S., Khallaf, A., Majdalawieh, M.: Characteristics of an Internal Audit Activity. The Institute of Internal Auditing Research Foundation, Altamonte Springs (2011)
3. Allegrini, M., D'onza, G., Melville, R., Selim, G., Sarens, G.: What's the Next for Internal Auditing. The Institute of Internal auditing research foundation, Altamonte Springs (2011)
4. Lacity, M.C., Willcocks, L.P., Feeny, D.F.: IT outsourcing: maximize flexibility and control. Harvard Bus. Rev. **73**, 85–93 (1995)
5. Ang, S., Straub, D.W.: Production and transaction economies and IS outsourcing: a study of the U.S. banking industry. MIS Q. **22**, 535–552 (1998)
6. Vasarhelyi M., Romero S., Kuenkaikaew S., Littley, J.: Adopting continuous audit/continuous monitoring in internal audit. ISACA J. **3**, 1−5 (2012)
7. Champlain, J.J.: Auditing Information Systems. Wiley, Hoboken (2003)
8. Weber, R.: EDP Auditing: Conceptual Foundations and Practice. McGraw-Hill, New York (1998)
9. Pathak, J.: Information Technology Auditing: an Evolving Agenda. Springer, Berlin (2005)
10. Buchanan, S., Gibb, F.: The information audit: an integrated approach. Int. J. Inf. Manag. **18**, 29–47 (1998)

11. Senft, S., Gallegos, F.: Information Technology Control and Audit, 3rd edn. Auerbach Publications, Taylor & Francis Group, Auerbach (2009)
12. Wright, C., Freedman, B., Liu, D.: The IT Regulatory and Standards Compliance Handbook: How to Survive an Information Systems Audit and Assessments. Elsevier, Burlington (2008)
13. Omoteso, K., Patel, A., Scott, P.: Information and communications technology and auditing: current implications and future directions. Int. J. Auditing. **14**, 147–162 (2010)
14. Moeller, R.R.: IT Audit, Control, and Security. Wiley, Hoboken (2010)
15. IT Governance Institute (ITGI): Cobit 4.0, Rolling Meadows, USA (2005)
16. IT Governance Institute (ITGI): IT control objectives for Sarbanes Oxley and board briefing on IT governance. Rolling Meadows, USA (2003)
17. Henderson, J.C., Venkatraman, N.: Strategic alignment: leveraging information technology for transforming organizations. IBM Syst. J. **38**, 472–484 (1993)
18. Adams, P., Cutler, S., McCuaig, B., Rai, S., Roth, J.: Sawyer s Guide for Internal Auditors, 6th edn. The IIA Research Foundation, Altamonte Springs, Florida (2012)
19. Chambers, A., Rand, G.: The Operational Auditing Handbook. Auditing, Business and IT Process, 2nd edn. Wiley, Chichester (2011)
20. Roth, J.: Academic culture, business culture and measuring achievement differences: internal auditing views. Educational policy studies dissertations, digital archive. Georgia State University, Atlanta (2012)
21. Bou-Raad, G.: Internal auditors and a value-added approach: the new business regime. Manag. Auditing J. **15**, 182–187 (2000)
22. MihretD, G., Woldeyohannis, G.Z.: Value-added role of internal audit: an Ethiopian case study. Manag. Auditing J. **23**, 567–595 (2008)
23. Stoel, M.D., Muhanna, W.A.: IT internal control weaknesses and firm performance: an organizational liability lens. Int. J. Acc. Inf. Syst. **12**, 280–304 (2011)
24. Teo, T.S.H., Wong, P.K., Chia, E.H.: Information technology (IT) investment and the role of firm: an explanatory study. Int. J. Inf. Manage. **20**, 269–286 (2000)
25. Sarens, G., De Beelde, I.: Building a research model for internal auditing: insights from literature and theory specification cases. Int. J. Acc. Auditing Perform. Eval. **3**, 452–470 (2006)
26. Yin, R.K.: Case Study Research: Design and Methods. SAGE Publications, London (2003)
27. Miles, M.B., Huberman, A.M.: Qualitative Data Analysis, 2nd edn. Sage Publications, London (1994)