Audit Methodology for IT Governance

Mirela GHEORGHE
Academy of Economic Studies, Bucharest
mirelaghe@gmail.com

The continuous development of the new IT technologies was followed up by a rapid integration of them at the organization level. The management of the organizations face a new challenge: structural redefinition of the IT component in order to create plus value and to minimize IT risks through an efficient management of all IT resources of the organization. These changes have had a great impact on the governance of the IT component. The paper proposes an audit methodology of the IT Governance at the organization level. From this point of view the developed audit strategy is a strategy based on risks to enable IT auditor to study from the best angle efficiency and effectiveness of the IT Governance structure. The evaluation of the risks associated with IT Governance is a key process in planning the audit mission which will allow the identification of the segments with increased risks. With now ambition for completeness, the proposed methodology provides the auditor a useful tool in the accomplishment of his mission.

Keywords: *IT Governance, Corporate Governance, IT Audit Process, IT Risk*

1 Introduction

The continuous development of the new IT technologies was followed up by a rapid integration of them at the organization level. IT becomes an essential issue in strategic development and increasing performances of any organizations. The acclaimed advantages induced by IT component are in balance with new IT relevant risks. The rapid cadence of the technological change asks for a timely IT decisions with a thorough understanding of the risks and opportunities associated with the IT phenomena. The management of the organizations face a new challenge: structural redefinition of the IT component in order to create plus value and to minimize IT risks through an efficient management of all IT resources of the organization. The evolution of the present IT environment is a natural process according to which business environment should adapt. This way it must integrate the best techniques and tools to provide transparency and relevant data in order to reveal, as an example, which are the priorities in IT projects development, in investments for meeting the organization aims and creating extra value for organization.

Well publicized problems of Enron, World Com, in United States, have determined in the last years some adjustments in corporate governance, including the issue of security and IT audit.

In 2002, the Sarbanes Oxley (SOX) law was adopted, which has directed the attention, among other issues, over IT audit and its role on assuring the accuracy of the financial auditors. In Europe, the Basel II Committee on Banking Supervision recommends conditions that should be fulfilled, like the size of capital, credit exposures, improvement of the credit and operational risk management and the management information systems through clearly defined requirements. All these changes have had a strong impact in the governance way of the financial institutions, with great implications in the

IT Governance uses the premises of the corporate governance, which are extended in IT area. This fact guided the boards of the organizations to implement processes and structures which allowed the organizations to sustain the objectives and strategies through IT component to.

The IT auditors are in charge with the assessment of the IT Governance efficiency, with the degree of implementation of this procedure. IT auditors (independent or from the inside of the organization) can perform a number of key roles [2]:

- initiating IT governance programs: explain IT governance and its value to management;
- assessing the current state: provide advice and assist with current-state assessments, gap priorities.
- planning IT governance solutions
- monitoring IT governance initiatives
- helping make IT governance business as usual: provide objective and constructive input, encourage self-assessments, and provide assurance to management that governance is working effectively.

2 IT Governance Conceptual Framework

Significant literature in governance area reveal that government processes can be lined up in three groups: Enterprise Governance, Corporate Governance, and IT Governance.

Enterprise Governance has been described as "the set of responsibilities and practices exercised by the Board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly" [6].

Corporate Governance has been defined as "the ethical corporate behavior by directors or others charged with governance in the creation and preservation of wealth of all stakeholders" ([12]). The Australian Stock Exchange Corporate Governance Council considers corporate governance to be "the systems by which companies are directed and managed. It influences how the objectives of the company are set and achieved, how risk is monitored and assessed, and how performance is optimized" [1].

IT Governance has been defined by the ITGI "IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives" [6].

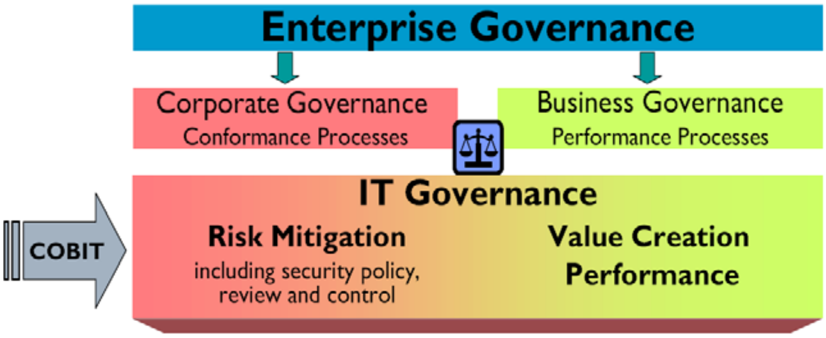

Fig. 1. Relation between Enterprise Governance, Corporate Governance and IT Governance [8]

Van Grembergen defines IT Governance as follows: "IT governance is the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT" [18].

Literature contains many other definitions. Despite the apparent disagreement between scholars, the IT Governance definition stressed "the red thread" that IT should sustain the organization objectives.

Van Grembergen's definition reveals that IT management remains a main actor within the IT Governance processes. Despite the association between IT management and IT governance, the two concepts remain different. IT management is in charge with providing effective IT services, with supplying and management of IT services and products. On the other hand IT governance is much broader and focuses on performing and transforming IT to meet demands of the business and the business' customers.

IT Governance Institute reveals that IT governance is part of much broader notion of Corporate Governance. Lining up in this order the two concepts, IT governance should follow the principles of corporate governance, i.e. effective, transparent and accountable.

IT Governance reflects broader corporate governance principles while focusing on the management and use of IT to achieve corporate performance goals. Because IT outcomes are often hard to measure, firms must assign responsibility for desired outcomes and assess how well they achieve them. IT Governance shouldn't be considered in isolation because IT is linked with other key enterprise assets (financial, human, intellectual property, etc). Thus, IT Governance might share mechanisms (such as executive committees and budget processes) with other asset governance processes thereby coordinating enterprise wide decision making processes [12].

3 IT Governance Focus Area

In practice IT Governance supports the business, adding plus value through IT component and IT risks minimization. In order to achieve such purposes IT Governance should cover five principal domains (in ISACA vision [6]):

- IT Strategic alignment
- Value delivery
- Risk management

- Resource management
- Performance measurement

A. Aligning IT strategy with business strategy

This first domain of IT Governance has the starting point in designing an IT strategy according with the overall strategy of the organization. Thus, starting to the organization's strategic plan IT strategy committee should lay down an IT strategy in line with the business objectives. In particular, IT governance practices should:

- ensure that IT strategy is aligned with business strategy
- ensure that IT delivers against the strategy through clear expectations and measurement
- allocate IT investments budgets in accord with the business objectives
- ensure that technology investment decisions are aligned with business goals.
- provide high-level direction to create competitive advantages that parallel compliance processes
- direct IT strategy by addressing the level and allocation of investments, balancing the investments between supporting and growing the enterprise and by making considered decisions about where IT resources should be focused
- ensure a culture of openness and collaboration among the business, geographical and functional units of the enterprise.

B. Value Delivery

Starting from the premises of the corporate governance, underlining that “a company, in first place, have to aim the maximization of the value of their shares on long term”, the implementation of the new IT techniques have to add value to organization by the quality of the services, expenses optimization, offer of pertinent and useful data delivered timely. IT value delivery is defined as “delivery on time, within budget and with the benefits that were promised. In business terms, this often translates into: competitive advantage, elapsed time for order/service fulfillment, customer satisfaction, customer wait time, employee productivity and profitability” [6].

IT Governance should target a proper quality of the IT services combining the resources from the budget and the time factor.

The governance practices for IT value delivery are:

- ensure that IT plans proceed on schedule
- ensure the completeness, quality and security of IT investments
- monitor IT investments for adequate returns
- ensure bankable benefits through IT services.

C. Resource Management

IT resource management is concerned with the management of IT resources and the organization of IT infrastructures within a corporation. This critical dimension of IT Governance processes aims to provide high level direction for sourcing and use of IT resources, to oversee the aggregate funding of IT at the enterprise level and to ensure that there is adequate IT capability and infrastructure to support current and expected future business requirements [3]. Another important aspect of this domain is the issue of project management. Management of new IT projects must be properly governed as these projects have considerable impact on the financial position and strategic direction of the organization.

The governance practices for IT resource management are the following:

- allocate IT resources in correlation with business priorities
- implement adequate controls which allow to identify over fulfilled IT infrastructures
- sustain an adequate investment in staff education, development and training for IT operations and developments

D. Risk Management

Specialized authors define in their writings risk management as being “the process of identifying the vulnerabilities and threats from the framework of an organization as well as designing procedures in order to minimize the impact of them on IT resources”. The risk on organization level cannot be eliminated; it will exist all the time; the management of the organization is responsible with minimizing it to an acceptable level. Risk management should be a continuous process which begins by assessing the level of exposure of the organization and identifying the main incident risks. Once identified, risks have to be minimized using control procedure and finally residual risk should be adjusted at acceptable level.

We will underline that the governance practices for IT risk management are:

- analyze and asses IT risks
- monitor efficiency of internal controls
- implement necessary controls to minimize IT risks
- put in place procedures to ascertain the transparency about the significant risks to the enterprise
- consider that a proactive risk management approach can create competitive advantage
- Insist that risk management be embedded in the operation of the enterprise

- Ascertain that management has put processes, technology and assurance in place for information security to ensure that:
  - Business transactions can be trusted
  - IT services are usable, can appropriately resist attacks and recover from failures
  - Critical information is withheld from those who should not have access to it.

E. Performance Measurement

Performance measurement is concerned with determining whether IT systems have achieved the goals set for them by the Board and senior management. For IT performance measurement, IT governance practices should:

- Define and monitor measures together with management to verify that objectives are achieved
- Measure IT performances through metrics, adequate indicators.

Implementing the IT Governance framework any organization should balance internal factors as well as external relevant factors, such as:

- *The fact of technological development:* The fast development of the domain requires that decisions related to IT be made on a timely basis, with full understanding of the risks associated with the IT challenges.
- *The fiscal scrutiny:* Large IT projects need expensive spending causing sometimes doubt and accountability for discretionary waste of financial resources.
- *Innovation and control over IT:* In cases where the innovation (new IT projects) is supported by IT, it may run counter to the objective of exerting control over the IT environment.
- *Up to date infrastructure:* Technology infrastructure becomes out of date over time. Keeping it up to date is a must for every department.

In conclusion, we can state that government practices associated with the five fundamental domains are material factors in the decision making process. Subsequent to objectives self-imposed, IT Governance achieves the alignment of the IT investments with business objectives, assures a responsible use of the IT resources, and assures that IT performances are within the borders of the approved budget and IT strategic plan. Following its principles IT governance provide a decreasing of the IT risks trough a continuous scrutiny of the threats and weaknesses of the system improves IT organizational performance, compliance, staff development and outsourcing initiatives.

4 Policies and Procedures for Efficient IT Governance Implementation

IT governance doesn't follow a unique pattern in implementation but it have to use the best practices in this field: COSO, COBIT, ITIL, ISO 27002 (ISO 17799), ISO 38500, etc.

There are several different IT Governance models that have been developed, some driven from a strategic view points and others developed from tactical processes such as project management. Each has its strengths and weaknesses; the business and IT management must select the appropriate governance model based on the unique needs of the business.

COSO was established in 1985 to support The National Commission on Fraudulent Financial Reporting. In COSO approach internal control is a process undertaken by the entity's board of directors or management in order to give a reasonable assurance for the fulfilling of the objectives within the some specific categories: effectiveness and efficiency of operations; reliability of financial reporting; compliance with applicable laws and regulations.

The COSO internal framework comprises five areas of interests which cover the activity of the managers in charge with the business:

Control environment. This issue sets the framework for the action of all the other components of internal control. Control environment factors comprise the integrity, ethical values, delegation of authority as well as the management's operating style in relation with entity's human resources.

Risk assessment. The entity encounters many risks from inside or outside of the organization. Such risks should be appraised and assumed. Risks are related with the objectives of the organization and in this context risks should be assessed. Following this assessment the risks should be managed.

Control activities. This issue covers the policies implemented to ensure the pursuing of the management directives. Such controls assure that necessary actions are taken to avoid risks that threat the achievement of current objectives. Control activities comprise a diverse range of tasks such as verifications, approvals, as well as reconciliations, reviews of operating performance or security of assets.

Information and communication. This issue ensures the information circuit within the framework of organization. Exchange of information, using the implemented procedures for communication, permit the feedback as well as the reporting of data, interaction in the benefit of the business, but whistler blowing too. Effective communication should cover the relation with all external parties, such as shareholders, customers, suppliers and regulators.

Monitoring. This issue addresses the assessment of the system's performance over time. Through this process the weaknesses of internal control are detected and analyzed in order to correct them und improve continuous the system's behavior.

COBIT (Control Objectives for Business & Related Technology) distinguish itself as a well recognized framework for IT governance and auditing accounting IT systems. It is designed as an accessible guide for management, users, auditors and all the persons who use the computer for their business in order to ensure them confidentiality, integrity and availability of data and information.

COBIT framework consists of a set of high level control objectives structured on four fields: planning and organizing, acquisition and implementation, services providing and maintaining, as well as monitoring. The assembly of the four fields includes a number of 34 IT processes, which one has associated a high level control objective. By considering the 34 control objective the process owner can ensure that an appropriate control system is achieved in IT environment. Beside these high level control objectives COBIT comprises detailed control objective (318), with recommendation status, that permit a "refinement" of examination that provide supplementary elements of assurance for management.

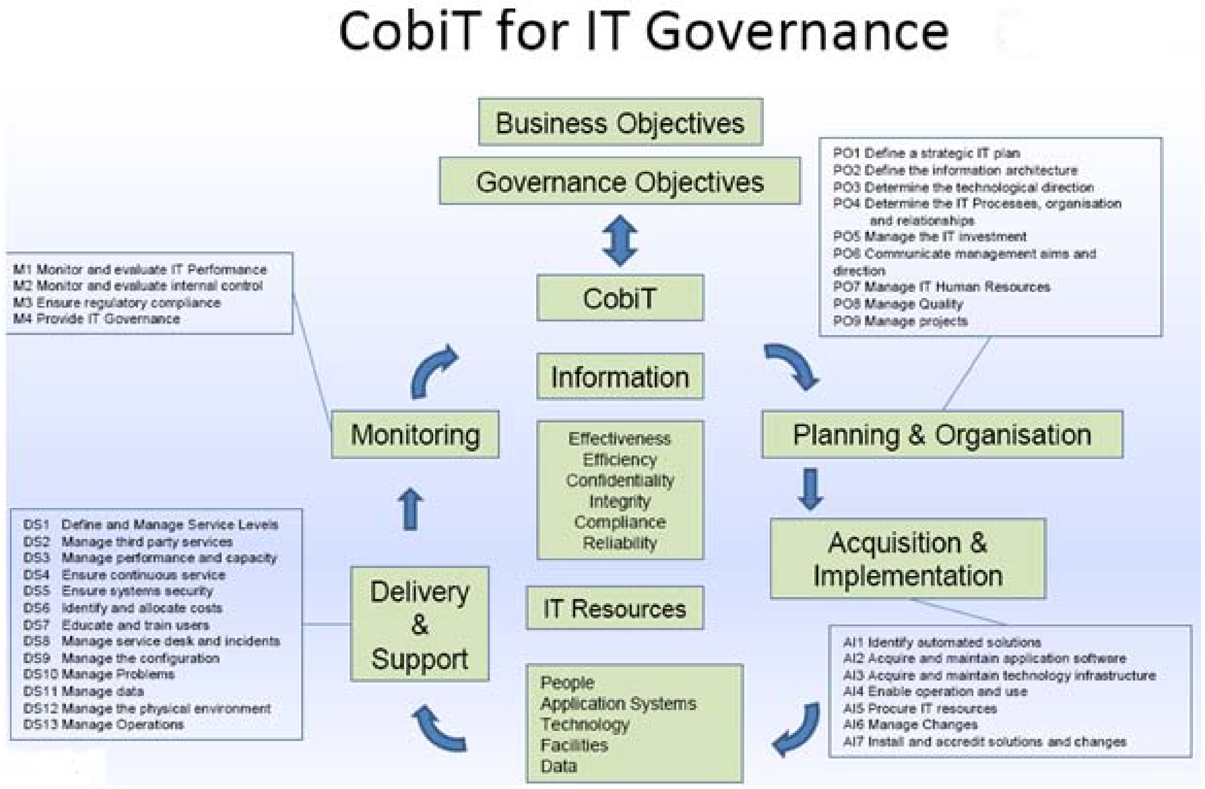
CobiT for IT Governance
Business Objectives
Governance Objectives
CobiT
Information
Effectiveness
Efficiency
Confidentiality
Integrity
Compliance
Reliability
IT Resources
People
Application Systems
Technology
Facilities
Data
Monitoring
Planning & Organisation
Acquisition & Implementation
Delivery & Support
M1 Monitor and evaluate IT Performance
M2 Monitor and evaluate internal control
M3 Ensure regulatory compliance
M4 Provide IT Governance
PO1 Define a strategic IT plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Determine the IT Processes, organisation and relationships
PO5 Manage the IT investment
PO6 Communicate management aims and direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Manage projects
DS1 Define and Manage Service Levels
DS2 Manage third party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure systems security
DS6 Identify and allocate costs
DS7 Educate and train users
DS8 Manage service desk and incidents
DS9 Manage the configuration
DS10 Manage Problems
DS11 Manage data
DS12 Manage the physical environment
DS13 Manage Operations
AI1 Identify automated solutions
AI2 Acquire and maintain application software
AI3 Acquire and maintain technology infrastructure
AI4 Enable operation and use
AI5 Procure IT resources
AI6 Manage Changes
AI7 Install and accredit solutions and changes

Fig. 2. CobiT for IT Governance [6]

Control objectives are defined in a general manner, independent from technical support, but it is accepted that some special technical environment can require a distinct approach of control objectives. Therefore, it have to be mentioned that objectives consists of statements on results or desired goals that should be reached through implementation of specific control procedures within IT activities.

COBIT documentation comprises other measurement parameters for the performances of IT system and analysis of IT controls too, as being: maturity prototypes, critical success factors, key goals and key performance indicators.

ITIL (Information Technology Infrastructure Library) – represents *de facto* standard, at world level, for IT services management. Its objectives focus on aligning IT services with present and future necessities of the organizations, improvement of the quality of the delivered services and long term cost reduction for delivered services.

ITIL focuses on 7 main directions:

1. *Service Delivery*: covers the strategic processes associated with planning and delivery of quality IT services.
2. *Service Support*: involves processes associated with daily support and maintenance activities.
3. *Information and Communications Technology (ICT) Infrastructure Management*: covers all processes from the identification of business requirements through testing, implementation and operation of ICT components.
4. *Planning to Implement Service Management*: covers project-management type processes related to organizational change and planning, implementing and improving service management ;
5. *Application Management*: involves processes throughout the application lifecycle;
6. *The Business Perspective*: describes processes concerned with ways IT personnel can better align their roles and services with the organization to better achieve business objectives;
7. *Security Management*: covers processes associated with risk identification and management and security of IT services.

ISO 17799 known today as **ISO 27002** *"Information Technology – Code of best practice for information technology management"* represents a guide for implementing a set of policies, practices and procedures in order to consolidate the information security administered by an organization. Implementation of this standard represents a competitive advantage for any organization proving that information security is a well controlled process.

ISO/IEC 27002 requires that management:

- Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities and impacts;
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable; and
- Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

ISO 38500 "Corporate governance of information technology" lays down a set of rules for upper level of organizations in order to support them to fulfill their legal, regulatory, and ethical obligations in respect of their organizations' use of IT.

The new standard is based upon six key principles:

1. *Responsibility*. Members within the organization, including those with responsibility for actions shall understand and accept their capacities in respect of both supply of, and demand for IT.
2. *Strategy*. The strategic plans for IT shall satisfy the current and ongoing needs of the organization's business strategy.
3. *Acquisition.* IT acquisitions shall be fulfilled with appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.
4. *Performance.* IT shall meet the current and future business requirements.
5. *Conformance.* IT shall comply with all mandatory legislation and regulations.
6. *Human Behaviour.* IT policies, practices and decisions shall observe the current and evolving needs of all the "people in the process".

ISO 38500 laid down precise tasks about IT governance for directors. Three directions shall be observed: Evaluating, Directing and Monitoring. The implementation of IT governance itself shall follow a clear approach [7]:

- IT governance shall be aligned with sound Corporate Governance practices,
- IT governance shall obey the enterprise's approach in the border area of Corporate Governance
- It shall regulate all the issues related with enterprise's IT activities
- It shall be designed on principles and objectives ease to understand and follow by all the stakeholders.

ISO 38500 assist the higher level of the enterprise (decision making level) to monitor and asses IT activities to meet the IT requirements in order to support the development of the organization.

5 Methodology for Audit

The aim of this research is to reveal an audit methodology of IT Governance of an organization. From the methodological point of view, the research started from theoretical framework provided by literature review, requirements of international IS audit "IT Governance" updated with Guide 18 "IT Governance" and Guide 39 "IT Organization" laid down by ISACA.

The framework of the mission will follow the specific steps of every IS audit process:

a. **IT AUDIT OBJECTIVES**. The objectives of an IT Governance assessment audit should focus on appraisal of the level of alignment and integration of the IT strategy with the business strategy, assessment of the output of the IT component and plus value provided for organization.
b. **SCOPE OF THE AUDIT.** The IS auditor should include in the scope of the audit the relevant processes for planning and organizing the IT activity and the processes for monitoring that activity. The scope of the audit should include control systems for the use and protection of the full range of IT resources.
c. **PLANNING.** At this point, IS auditor should accomplish an assessment of the IT Governance structure, a thoroughly documentation in order to obtain a general understanding of the processes which enable the IT governance structure.
d. **PERFORMANCE OF AUDIT WORK.** In order to gather the most relevant and specific proves, IS auditors test, analyze and assess critical areas identified in planning step, which can be:
   - Business Strategic Planning Process
   - IT Strategic Planning Process
   - IT Service Management,
   - IT Investments Management
   - IT Project Management
   - IT Risk Management
   - IT Performances Measurement Process
   - Compliance with standards and legal rules applicable
e. **REPORTING.** IT Governance audit guide recommends that audit report on IT governance should include [9]:
   - a description of the key procedures that top-level management has established to provide an effective IT governance system and the related supporting documentation,
   - information on any major uncontrolled risks,
   - information on any ineffective or inefficient control structures
   - information on any noncompliance with the organization's policies or any relevant laws and regulations
   - The IT auditor's overall conclusion on the IT governance, as defined in the terms of reference
f. **FOLLOW-UP**. The IS auditor should returns within the organization to observe the way his recommendations, made in audit report, were implemented.

Checklist activities

The activities of the audit team, in order to achieve de steps revealed, should comprise:

Identifying the domains (target) and the specific audit objectives

General objectives of an IT Governance audit mission comprise IT Governance structure assessment and appraisal of the level of alignment between IT strategy and business strategy. After the moment the general objective is laid down, should be formulated the specific objectives which define requirements and criteria for ongoing audit.

In this way, the research proposes the following specific audit objectives and material risks associated with IT Governance.

Thus, we can state relevant criteria addressed in audit process are based on:

1. IT strategy alignment with organizational business strategy
2. IT governance structure, with competences and responsibilities associated to every department
3. Identifying IT costs and decision for IT resources allocation: investments decision, IT developed projects, controls implemented in order to mitigate IT risks.
4. IT performances assessment and monitoring.

Planning

Within this step, IS auditors should undertake some specific procedures:

- To study the IT governance structure. Auditor should analyze encountered organizational structure (Senior Management, Executive Management, Steering Committee, Chief Information Officer) with competences and responsibilities.
- To study IT organizational structure and staff management. Auditor should analyze incompatible IT function segregation, staff management policies (continuous staff training).
- To study organizational governance strategy (organizational strategy plan)
- To study organizational IT Governance strategy (IT plan, tactical plan subordinated to strategic plan, IT budget).
- To analyze and assess alignment and integration between IT strategy and objectives and organization strategy.
- To assess IT Governance structures performances (executive management, senior management and employees)
- To study IT infrastructure in order to assess the support for the IT objectives.

- To study IT investments plan, IT development projects, outsourcing policies.
- To study provided IT services.
- To study IT risk assessment methodology, risks monitoring and controls implemented for risk mitigation
- To study security policy for safeguarding organization assets, business continuity plan, recover after disasters.
- To study IT performances indices computed by entity.
- To assess IT Governance associated risks (see Table 1), to assess these risks for indentifying critical area.

Table 1. IT risks area associated to auditable area for IT Governance

No.	Auditable area	Specific audit objectives	Material risks associated with IT Governance
1.	IT strategic planning process	▪ Development strategic plan of IT system ▪ IT tactical planning associated with IT strategic plan ▪ Competences and responsibilities in compliance with strategic plan activities	▪ IT strategy planning risks, ▪ IT/business misalignment risks, ▪ Deficient IT policies and procedures risks, ▪ Communication with staff organization associated risks ▪ IT approved budget surpass
2.	IT Organizational Structure and Staff Management	▪ IT Department organizational analysis ▪ Responsibilities laid down by job descriptions ▪ Segregation of incompatible competencies ▪ Continuous professional training of the IT staff assessment system	▪ Non segregation of competencies risk ▪ Risk associated with continuous professional training of the IT staff
3.	IT Service Management, IT Investments Management	▪ IT investments planning and monitoring ▪ IT investments quality, completeness and security ▪ service level agreement (SLA) Management ▪ planned return for provided IT services	▪ Risk planning IT investments ▪ IT investments risk (i.e.: unauthorized software/hardware purchases) ▪ Risks associated with agreements undertaken with clients IT services risks (i.e. : IT services undelivered in time)
4.	IT Project Management	▪ project management methodologies used ▪ The project management controls applied ▪ The integration of IT and business staff along the various stages of the projects ▪ Change management methodologies used for large projects, ▪ Application development methodology and practices, and the controls applied over the development process ▪ Infrastructure support ▪ IT activities, including application development and maintenance and infrastructure support, have been outsourced.	▪ IT project risk management ▪ IT project failure (abandoned or put aside projects) ▪ software development or acquisition risks, ▪ change management procedures and associated risks, ▪ risks associated with deficient IT policies and procedures (security risks) ▪ Infrastructure risk
5.	IT Risk Management	▪ IT risk management programme ▪ Quantitative/quality IT risks assessment methods ▪ Implemented controls analysis for mitigating risks Internal IT audit ▪ Policy for assets security and business continuity ▪ Business continuity plan	▪ Inadequate methods for assessing IT risks ▪ Insufficient implemented controls for mitigating risks (Risks associated with internal control) ▪ poor internal IT audit practices ▪ Lack of registry for IT incidents business continuity and disaster re-

		▪ IT incident registry	covery risks
6.	Performance IT Measurement	▪ Performance indices computing process, inadequate indices ▪ Management performances assessment	▪ Risk associated with IT performances indices ▪ Risk associated with IT performance monitoring ▪ Lack of IT management assessment process
7.	Internal policies compliances with applicable rules and standards	▪ IT organizational policy, internal processes and procedures ▪ software licenses situation within the system ▪ Internal policies compliances with standards, rules and best practices in IT area.	▪ legal and regulatory risks ▪ compliance risk

In order to obtain a general understanding of the processes which enable the IT governance structure, IT auditor should analyze relevant documents of the entity [10]:

- IT strategies, plans and budgets – they provide evidence of planning and management s control of the IS environment and alignment with the business strategy.
- Security policy documentation
- Organization charts – the charts illustrate a division of responsibility and give an indication of the degree of segregation of duties within the organization.
- Job description – These descriptions define the functions and responsibilities of position throughout the organization. Furthermore, job descriptions give an indication of the degree of segregation of duties within the organization and may help identify possible conflicting duties.
- Steering committee reports – these reports provide documented information regarding new system projects.
- Operations procedures – these procedures describe the responsibilities of the operation staff.
- System development and program change procedures

After the analysis of revealed documents, in order to obtain relevant information, IT auditor activities should be completed with interviews with senior management, selected staff and IT users. The paper proposed a pattern for assessment questionnaire of the IT Governance (see Table 2).

Table 2. Questionnaire model for IT Governance assessment

No	Question	Yes	No
1.	Is the IT strategy plan aligned to business strategic plan?		
2.	Is there regular communication between the CIO (Chief Information Officer) and CFO (Chief Financial Officer)?		
3.	Are the IT investment decisions aligned to business goals?		
4.	Does the CIO define and communicate the role of IT to the rest of the organization?		
5.	Is IT staffed adequately, with right skills and competencies?		
6.	Is the percentage of revenue spent on IT compared to the industry average?		
7.	Do the CIO & management consider value delivery from IT systems to be important?		
8.	Does the organization have an IT steering committee?		
9.	Is the IT investments high quality, comprehensive and safe?		
10	Are IT services delivered on time and offers the quality expected?		
11	Do IT projects have a clear budget and timeline?		
12	Does the board obtain regular progress reports on major projects?		
13	Are the business priorities and IT resource allocation controlled so as to ensure effective IT performance?		
14	Does the organization take a regular inventory of its IT resources?		
15	Is a risk management policy, assessment and mitigation practice followed for IT?		
16	Does the organization have a business continuity plan in place?		
17	Are the security and business continuity processes regularly tested?		
18	Does the organization have a policy for 3rd party contacts?		
19	Are sufficient IT resources and infrastructure available to meet required enterprise		

	strategic objectives?		
20	Does the organization performs analysis and evaluation of IT risks?		
21	Does the organization monitor the effectiveness of internal controls?		
22	Does the CIO work together with IT strategy audit committee about major IT risks?		

On the basis of the gathered data the auditor will perform an analysis and ranking of the IT Governance specific risks. This procedure supports the identifying of critical area of the audit system that is to be verified and tested.

Performance of audit work

On the basis of an articulated audit process, the mission focus on performing some compliance tests of the policies, managements' practices with standards and relevant rules in the area as well as some material tests for assessment of IT governance structure efficiency. This testing process is not complete but it focuses on critical area identified in planning step.

As an example we reveal specific IT auditor action for every IT Governance audit domain.

- **For assessment IT strategic planning process**, IT auditor should consider whether:
  - there is a clear definition of IT mission and vision,
  - there is a strategic information technology planning methodology in place,
  - the methodology correlates business goals and objectives to IT business goals and objectives, this planning process is periodically updated (at least once per year),
  - this plan identifies major IT initiatives and resources needed
- **For assessment IT organizational management,** IT auditor should**:**
  - Verify IT structure of the organization in order to assure the command chain and responsibilities for IT operations of the organization and to assure the segregation of incompatible competencies.
  - Verify if employment and lay off procedure are clear and comprehensible.
  - Verify IT staff training policy.
- **For assessment IT delivery process and IT investments planning process,** IT auditor should:
  - Verify and assess the management for services provided of third parties.
  - Assess service level agreement (SLA) Management - examine how well the knowledge in the help desk function is managed
  - Examine all SLA reports and review and examine the contract to ensure that other aspects of IT service management, such as capacity management and configuration management
  - Assess the approval process and the priority of the IT investments.
  - Assess the realization of benefits to the business from investments in IT
- **For assessment the project management (**inclusive application development methodology and practices**)**, IT auditor should consider :
  - project management methodologies used
  - The project management controls applied
  - Application development methodology ,
  - managing IT infrastructure and change management
  - IT activities, including application development and maintenance and infrastructure support, have been outsourced.
- **For assessment IT risk management,** IT auditor should verify:
  - The process of assessment of weaknesses and IT threats.
  - Assessment methods for IT risks.
  - Reporting procedure for security incidents.
  - Business continuity plan (tested and timely updated)
- **For assessment IT Performance process,** IT auditor should verify:
  - IT performance indices are adequate.
  - IT management performance indices.
  - IT performances monitoring process.

6 Conclusions

The research has started from scholars' analysis of the IT Governance concept as well as from ISACA IT audit standards: IT Governance Standard, IT Governance Guide and IT Organization Guide. The proposed audit methodology, in this paper, allows classifying the relevant risks associated with IT Governance, risks that should be assessed for revealing critical area within the system. The activity of identifying of these risks was achieved in seven main domains: IT strategic planning process, IT organizational Management, IT delivery process and IT investments management, IT project Management, IT risk management, IT performance process, legal compliance. Analysis and assessment on these domains provide IT auditor an opinion on alignment level between IT strategy and business strategy, on IT Governance structure's efficiency, in order to mitigate IT risks and IT resources management. Proposed methodological framework, with now ambition for completeness, provides IT auditor a useful tool in the accomplishment of his mission.

References

[1] ASX Corporate Governance Council, *Principles of Good Corporate Governance and Best Practice Recommendations*, 2003.

[2] G. Hardy, "The Role of the IT Auditor in IT Governance," *Information Systems Control Journal*, 2009.

[3] G. Hardy, "Coordinating IT Governance - A new Role for IT strategy committees," *Information Systems Control Journal*, Vol. 4, 2003.

[4] H. Gray, "Is there a relationship between IT Governance and corporate governance," *Information Systems Control Journal*, 2004.

[5] M. Gheorghe, "IT Governance Principles," *Journal of Accounting and Management Information Systems*, No.18, 2006

[6] IT Governance Institute, *Board Briefing on IT Governance*, 2001, retrieved September, 2003, Available at: http://www.itgi.org.

[7] IT Governance Institute, *ISO/IEC 38500:2008 Adoption*, 2008, Available at: http://www.itgi.org.

[8] Institute de la Gouvernance des Systems d'Information, *The place of IT Governance in the Enterprise Governance*, 2005.

[9] ISACA, *IS auditing standard - IT Governance, IS auditing guideline - IT Governance*, 2005, Available at: www.isaca.org.

[10] ISACA, *CISA Review Manual*, 2008.

[11] NCC (The National Computing Centre), *IT Governance. Developing a successful governance strategy - A Best Practice guide for decision makers in IT*, 2005.

[12] P. Weill and J. W. Ross, "IT Governance on One Page," *CISR Working Paper*, No. 349, 2004.

[13] R. Peterson, "Information strategies and tactics for information technology governance," in *Strategies for Information Technology Governance*, 2004.

[14] R. S. Roussey, "Buoying Investor Confidence," *Marshall Magazine*, 2003.

[15] G. Selig, *Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management*, Van Haren Publishing, Holland, 2008.

[16] S. Hamaker, "Spotlight on Governance," *Information Systems Control Journal*, 2003.

[17] W. Van Grembergen and S. De Haes, "IT Governance and Its Mechanisms," *Information Systems Control Journal*, 2004.

[18] W. Van Grembergen, "Introduction to the Minitrack: IT Governance and its Mechanisms," *In proceedings of the 35th Hawaii International Conference on System Sciences (HICSS)*, 2002.

[19] W. Van Grembergen and S. De Haes, "Information Technology Governance Best Practices in Belgian Organisations," *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006.

Mirela GHEORGHE has graduated the Polytechnic Institute Bucharest in 1991 and the Faculty of Accounting and Management Information Systems within the framework of Academy of Economic Studies Bucharest in 1997. She holds a PhD diploma in Economics from 2004 and she had gone through all didactic positions, holding now the academic position of Professor. She is the author of 8 books and over 25 journal articles in the field of IS audit, IT Governance, IT security, IT multidimensional analysis.