Auditing IT Governance

Florin-Mihai ILIESCU
Info-Logica Silverline S.R.L.
office@infologica.ro

Effective IT governance helps ensure that IT supports business goals, optimizes business investment in IT, and appropriately manages IT-related risks and opportunities. Organizations that realize the IT is no longer a support process and embeds value and risks need a structured approach for better managing Information Technology, enable its capability to deliver added value enterprise wide and for setting up a risk management program to address new risks arising for usage of IT in business processes. In order to assess if IT Governance is in line with industry practices, IT Auditors need a good understanding of processes and applicable standards, particular audit work programs and experience in assessing potential problem indicators.

Keywords: *IT Governance, Audit, ISACA, CGEIT, Val IT, Value Governance, Portfolio Management, Investment Management*

1 Introduction

Auditing IT Governance needs more business knowledge than regular Information Systems (IS) audits because the IS auditor has to evaluate how IT is enabling the business strategy. IT is not longer seen as support process, but because a project is not enough to respond itself to a business outcome, multiple projects should managed together as programs. The paper makes a brief presentation of IT Governance practices, the Val IT Framework and the IS Auditor Process in order to explain the approach and the purpose of the Audit Work Program.

The Audit Work Program helps the IS Auditor to conduct his engagements, but each organization and project has its own characteristics and the work program should be tuned accordingly.

For organizations that don't use global standards and frameworks such as CobiT or Val IT within IT Function, most of the topics of the audit work programs might not be applicable. In such cases I recommend to use the Planning and Organization domain practices from CobiT (http://www.isaca.org/cobit) available for free download, to benchmark the organization against with first, and draw general recommendations for implementing IT Governance.

Organization's culture plays a great role in succeeding in managing value from IT enabled Investments. Additional processes, Val IT propose 22 governance processes need to be carried out by executives, requiring good understanding and specific relationships and organizational structures.

2 IT Governance

IT Governance is a concept that stared to be developed in 1998 when ITGI has founded and is a set of relationships and processes designed to ensure that the organization's IT sustains and extends the organization's strategies and objectives, delivering benefits and maintaining risks at an acceptable level.

Some of the IT Governance practices concerns IT Management, but the term governance is used because like other governance subjects, is the responsibility of the board and executives and it is not an isolated discipline or activity, and to ascertain that IT should be addressed organization wide, being integral to enterprise governance. The business units have a responsibility to work in partnership with IT to ensure that their business requirements are met. The purpose of IT governance is to direct IT endeavors, to ensure that IT's performance meets the following objectives [1]:

- Alignment of IT with the enterprise and realization of the promised benefits;
- Use of IT to enable the enterprise by exploiting opportunities and maximizing benefits;
- Responsible use of IT resources;
- Appropriate management of IT-related risks.

IT governance should start with setting initial objectives in terms of delivering desired benefits in line with the global strategy, effective and efficient use of resources, and maintaining risk at an acceptable level. The outcome of this process of setting the objectives for IT Governance should be formalized in an IT strategy document. The board should then set up the initial direction that

can be further developed in IT tactical plans in order to set up the IT Activities in line with IT Strategy, to deliver what the organization is expecting from IT.

Because of its complexity and because it requires more technical insight than other disciplines, IT is neglected by most boards in their strategic and risk management initiatives. But, Ineffective IT governance is likely to be a root cause of the negative experiences many boards have had with IT [1]:

- Business losses, damaged reputations or weakened competitive positions;
- Deadlines not met, costs higher than expected and quality lower than anticipated;
- Enterprise efficiency and core processes negatively impacted by poor quality of IT deliverables;
- Failures of IT initiatives to bring innovation or deliver the promised benefits.

Fundamentally, IT governance is concerned about two things: IT's delivery of value to the business and mitigation of IT risks. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained. [1]

3 Domains

The main area of interest of IT Governance is IT and Enterprise alignment. In Romania, most of the organizations have not developed a strategic approach for IT investments. The IT struggled to support growing businesses with minimum investment. However this is mostly true for private sector. In public sector many acquisitions in IT have not been delivered any outcomes, or the capabilities delivered were far from expected.

IT Strategic Alignment has to answer whether an enterprise's investment in IT is in line with its strategic objectives and thus building the capabilities necessary to deliver business value.

The IT strategy articulates the enterprise's intention to use IT, based on business requirements. Linkage to the business aims is essential for IT to deliver recognizable value to the enterprise. When formulating the IT strategy, the enterprise must consider:

- Business objectives and the competitive environment;
- Current and future technologies
- Costs;
- Risks;
- IT capabilities;
- Cost of current IT;
- Past failures and successes.

Once these issues are clearly understood, the IT strategy can be translated in:

- Business functions: functional requirements need to be delivered by applications and IT services;
- Application architecture: logical structure of applications and data in order to deliver required functions

Value Delivery, another governance area is addressing issues of how to optimize the costs while delivering the expected benefits. In business terms, this is often translated into: competitive advantage, elapsed time for order/service fulfillment, customer satisfaction, customer wait time, employee productivity and profitability [1]. The value is perceived different at different levels of the company, and is harder to be perceived at financial level where can be more precisely measured, therefore is important to have adequate metrics for each level where IT is a business enabler. To be successful, enterprises need to be aware that different strategic contexts require different indicators of value. This means that it is important to establish the value measures in concert between the business and IT.

Risk Management should address all the risks related with using information technology in business processes. Because IT is critical and has an active role in creating added value, risk should be managed by the board by:

Defining the accepted level of risk;

Communicating the risk management policies;

Defining the responsibilities for risk management;

Insisting on embedding the risk in operations;

Dependent on the type of risk and its significance to the business, management and the board may choose to:

- Mitigate - Implement controls (e.g., acquire and deploy security technology to protect the IT infrastructure);
- Transfer - Share risk with partners or transfer to insurance coverage;
- Accept - Formally acknowledge that the risk exists and monitor it;
- Avoid - Deciding not to undertake the initiatives inducing a specific risks (e.g., not opening a branch in a war zone);

If none of these options are considered for a certain risk, the risk is ignored. A successful risk management program should ensure that all risks

are identified and addressed.
Resource Management should ensure the optimal investment, use and allocation of IT resources (people, applications, technology, facilities, data) in servicing the needs of the enterprise. [1] This includes good sourcing practices, what should be performed in-house and what is more efficient to be outsourced. Outsourcing ensures most of the time effectiveness, accessing from a wide range of providers, services and skills, but is not always efficient, cost and dependency on a certain provider, also risks with vendor failure, confidentiality and protecting intellectual property should be addressed.
Performance Measurement concerns tracking project delivery and monitoring IT services. The biggest challenge of measuring the performance of IT the intangible nature of the benefits delivered. Traditional measurement techniques offer only a financial perspective, which offer only a limited relevance of IT performance. A system downtime, for most of the business, excepting the online services, will not be translated at all in financial statements.
Balanced scorecards is a complex tool that can be used to translate strategy into action to achieve goals with a performance measurement system that goes beyond conventional accounting, measuring those relationships and knowledge-based assets necessary to compete in the information age: customer focus, process efficiency and the ability to learn and grow.
Another measuring technique, widely used for measuring performance of IT and supporting investments in technology is Applied Information Economics (AIE). AIE is the practical application of scientific and mathematical methods to the IT and business decision process, is a synthesis of techniques from a variety of scientific and mathematical fields. The tools of economics, financial theory, and statistics are all major contributors to AIE. But in addition to these more familiar fields, AIE includes Decision Theory - the formulation of decisions into a mathematical framework - and Information Theory - the mathematical modeling of transmitting and receiving information. It is important to emphasize, however, that even though AIE is a theoretically well-founded set of techniques, it is a very practical approach. Every proper application of AIE keeps the bottom line squarely in mind. All output from the AIE project is in support of specific practical business objectives. [2]

4 Global best practices

IT Governance practices consist of policies, procedures, processes recommended for achieving optimal results. Because they have been widely used and have proven good results are usually referred as global best practices, or general accepted practices. The term “global best practice” is sometimes avoided also because there was a trademark of Andersen.
Board should be aware of global best practices in order to set-up a successful IT Governance program. Such practices have to identify for each IT Governance area of interest:

- IT Strategic Alignment, such as formalized business objectives, up to date IT strategy, linkage between business objectives and IT initiatives;
- Value Delivery: IT tactical plans, clear benefits for each level of the organization: infrastructure (systems uptime), applications (degree of automation), operational (productivity), financial (income);
- Risk Management: defined responsibilities for risk management, risk analysis methodology, defined strategies for addressing risks, continuous monitoring of threats, occurrence and impact;
- Resource Management: sourcing strategies, human management practices, user manuals, segregation of duties, time reporting, infrastructure life cycle management, acceptable usage policies.
- Performance Measurement: relevant and measurable metrics, continuous monitoring and reporting, follow-up policies, root cause analysis and problem management, benchmarking against industry practices and proven standards or frameworks.

To address this increasing demand for a practical IT investment and management framework, IT-GI—working with other thought leaders in the global business and IT community—has undertaken the Val IT initiative.

5 Val IT Framework

The Val IT framework is a comprehensive and pragmatic organizing framework that enables the creation of business value from IT-enabled investments. Designed to align with and complement COBIT, Val IT integrates a set of practical and proven governance principles, processes, practices and supporting guidelines that help boards, executive management teams and other enterprise leaders optimize the realization of value from IT investment. [3]

The IT governance audit program is going to use Val IT Framework as a best practice, therefore is important to have a good understating of key terms used in Val IT publications:

- Project – A structured set of activities concerned with delivering a defined capability (that is necessary but not sufficient to achieve a required business outcome) to the enterprise based on an agreed-upon schedule and budget;
- Program – A structured grouping of interdependent projects that are both necessary and sufficient to achieve a desired business outcome and create value. These projects could involve, but are not limited to, changes in the nature of the business, business processes, the work performed by people, as well as the competencies required to carry out the work, enabling technology and organizational structure. The investment program is the primary unit of investment within Val IT.
- Portfolio – Groupings of 'objects of interest' (investment programs, IT services, IT projects, other IT assets or resources) managed and monitored to optimise business value. The investment portfolio is of primary interest to Val IT. IT service, project, asset or other resource portfolios are of primary interest to COBIT.

Val IT supports the enterprise goal of creating optimal value from IT-enabled investments at an affordable cost, with an acceptable level of risk and is guided by a set of principles applied in value management processes that are enabled by key management practices and are measured by performance against goals and metrics. [3]

6 Information Systems Audit Process

Either is carrying out an internal audit, or an external audit, the audit should be performed following up a formal plan designed to meet the audit objectives. For an internal audit function, a plan should be developed/updated, at least annually, for ongoing activities. The plan should act as a framework for audit activities and serve to address responsibilities set by the audit charter. For an external IS audit, a plan should normally be prepared for each audit or non-audit assignment. The plan should document the objectives of the audit. [4]

An audit plan should take into consideration the objectives of the auditee relevant to the audit area and its technology infrastructure. When auditing IT Governance, the IS auditor should also consider relationships within the organization (strategically, financially and/or operationally) and obtain information on the strategic plan, including the IS strategic plan. [5]

In order to issue an IT Audit report and to state an opinion, there should be a proper planning of the engagement, appropriate staffing, and relevant evidence to state the findings, proper documentation of the report and dissemination of findings to the stakeholders.

The planning should conclude in an audit program and procedures. Following steps should be followed in order to ensure success of the audit engagement:

- First of all IS Auditor has to gain an understanding of the business's mission, objectives, purpose and processes. Knowledge about particular industry's value chain and organization's business model can support this understanding critical in IT Governance auditing.
- Identify organization structure, strategy committees and IT oversees responsible;
- Identify IT organization structure, role of each IT entity and key positions such as: IT Manager/CIO, Information Security Offices/CISO, Applications Development Team Leader, Infrastructure Team Leader, Third-parties;
- Identify policies and procedures;
- Evaluate risk assessment and privacy impact analysis.
- Perform a risk analysis. IS auditors should use the selected risk assessment techniques in developing the overall audit plan and in planning specific audits. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as: The nature, extent and timing of audit procedures, the areas or business functions to be audited, The amount of time and resources to be allocated to an audit. The IS auditor should consider each of the following types of risk to determine their overall level: Inherent risk, Control risk and Detection risk. [6]
- Conduct an internal control review. Auditing projects should include consideration of internal controls either directly as a part of the auditing project objectives or as a basis for reliance upon information being gathered as a part of the auditing project. [6]
- Set the audit scope and audit objectives;
- Develop the audit approach or audit strategy;

- Assign personnel resources to audit and address engagement logistics;
- Develop and document an audit plan;
- Develop an audit program and procedures.

Scheduling of audit activities should be agreed with management in order not to hinder operational processes.

This audit program should be documented in a manner that will permit the IS auditor to record completion of the audit work and identify work that remains to be done. As the work progresses, the IS auditor should evaluate the adequacy of the program based on information gathered during the audit. When the IS auditor determines that the planned procedures are not sufficient, the IS Auditor should modify the program accordingly. [5]

7 IT Governance Audit Work Program

The purpose of the audit work program is to support IS auditors in carrying out an engagement whose purpose is to assess the IT Governance efforts undertaken by an organization to maximize the IT enabled benefits while maintaining risks under control.

This section presents a general audit work program, therefore to use it, the IS Auditor should be familiar with IT Governance practices in order to select and develop audit objectives and tests relevant for the audited organization and to interpret the findings with professionalisms and due care.

The IS auditor should obtain information on the IT governance structure, including the levels responsible for: Governing the enterprise, setting the enterprise strategic directions, assessing performance of the Chief Executive Officer/executive management in implementing enterprise strategies, assessing the performance of senior management and subordinates who report on the strategies in operation (including the knowledge, information and technology involved), determining whether the enterprise has developed the skills and IT infrastructure required to meet the strategic goals set for the enterprise, assessing the enterprise´s capability to sustain its current operations. [7]

The IS auditor should identify and obtain a general understanding of the processes which enable the IT governance structure to perform the its functions, including the communication channels used to set goals and objectives to lower levels (top down) and the information used to monitor its compliance (bottom-up). [7]

The IS auditor should obtain information on the organization's information systems strategy, including: plans to fulfill the organization's mission and goals, strategy and plans for IT and systems to support those plans, approach to setting IT strategy, developing plans and monitoring progress against those plans, approach to change control of IT strategy and plans, IT mission statement and agreed goals and objectives for IT activities and assessments of existing IT activities and systems. [7]

The work program uses Val IT Framework as a best practice in order to benchmark the findings. As defined in there aforementioned framework, following domains will be evaluated part of the IT Governance Audit:

- Evaluate Value Governance, having the purpose to determine the integration of value management within the enterprise, whether strategic directions are clearly set, portfolios required to support new investments and resulting IT services, assets and other resources are defined, value management is improved on a continual basis, based on lessons learned;
- Evaluate Portfolio Management, in order to assess whether resource profiles are established and managed, investment thresholds are defined, new investments are evaluated and prioritized, the overall investment portfolio is managed and optimized, portfolio performance is monitored and reported.
- Evaluate Investment Management, to determine if business requirements are met, investment programs are developed and clear understood, alternative approaches to implementing the programs are analyzed, each program is defined and documented, a detailed business case is maintained, including the benefits' details, throughout the full economic life cycle of the investment, clear accountability and ownership are assigned, each program's performance is monitored and reported.

The audit program developed below lists specific tasks for evaluating each domain.

7.1 Value Governance Audit Tasks

Following processes should be evaluated to assess the maturity of Value Governance within an IT Governance program:

- VG1 Establish informed and committed leadership.
- VG2 Define and implement processes.
- VG3 Define portfolio characteristics.
- VG4 Align and integrate value management with enterprise financial planning.

- VG5 Establish effective governance monitoring.
- VG6 Continuously improves value management practices.

Val IT can be used to benchmark the findings resulted from performing the tasks presented in Table 1, on a six levels maturity scale: 0 - Non-existent: when the enterprise sees the IT function as a supplier and a cost to be minimized, 1 - Initial when the enterprise recognizes that IT is both a cost and an investment, 2 - Repeatable when there is increasing awareness amongst business and IT management of the need for a more formalized governance framework, 3 - Defined when the business and IT functions understand the governance requirements to select and execute new investments, deliver the resulting IT services efficiently, and ensure optimal allocation of IT resources, 4 - Managed when there is a shared commitment between the business and the IT function to optimize the contribution of individual IT investments and services to business value, 5 - Optimized when value management is part of the corporate culture. The business and IT functions work in partnership to continually optimize and report on the portfolios of IT investments, and resulting services, assets, and other resources [3].

Table 1. Value Governance Audit Tasks

Proc. Ref.	Audit Tasks	Key Control
VG1	IT Strategy is documented and incorporates feedback from board. Leadership commitment is proven by initiatives supporting the IT strategy. Lesson learned are incorporated in the IT strategy. Business objectives are linked to IT strategic initiatives. CIO attends executive board meetings at which IT's contribution to enterprise goals is discussed. Strategic objectives are achieved rather than changed or not met.	IT Strategy
VG2	Accountabilities and practices are set up in governance framework. The governance framework covered by processes stating activities, owners, and areas of improvement. Processes are documented and include goals and metrics. Roles are established, communicated and accepted explicitly for investment decision making, program sponsorship, program management, project management, service delivery and associated support roles. IT strategy committee is set-up. IT planning committee is established. IT architecture board is established. Committees meet regularly and meeting minutes are available.	Value Management Process IT Strategy Organization
VG3	All types of portfolio are recognized and defined and categorized. Each category is evaluated according to predefined criteria to support fair, transparent, repeatable and comparable evaluation. Benefits are determined for each portfolio: degree of strategy alignment, financial benefits, intangible benefits, risk of non-implementation, risk of not meeting the expected outcomes. Requirements for stage-gates and other reviews of each type of portfolio are defined. Ongoing contribution to value is assessed according to reviewing requirements.	Portfolio categories and evaluation criteria
VG4	Practices are defined for setting budgets. Business cases are documented and sufficiently comprehensive. IT funding is known for future periods as well as the implications for the enterprise of costs. Financial planning practices are reviewed regularly.	Value management budgeting requirements Business case development guidelines
VG5	Performance indicators are defined, including metrics and benchmarks. Key metrics are reviewed, agreed to, by IT, business functions and stakeholders. Progress against targets is reported. Management action are initiated and controlled.	Key measurements monitored Reporting requirements
VG6	Lessons learned from value management are documented. Management plan changes.	Lessons learned

An organization is succeeding in managing value if the IS auditor finds out that Value Governance processes are effective. Key controls, if formalized can be used as starting point of the evaluation, however it has to be understood how the thinks are carried out in reality, documented or not.

7.2 Portfolio Management Audit Tasks

Following processes should be evaluated to assess the maturity of Portfolio Management within an IT Governance program:

- PM1 Establish strategic direction and target investment mix.
- PM2 Determine the availability and sources of funds.
- PM3 Manage the availability of human resources.
- PM4 Evaluate and select programs to fund.
- PM5 Monitor and report on investment portfolio performance.
- PM6 Optimize investment portfolio performance.

Val IT can be used to benchmark the findings resulted from performing the tasks presented in Table 2, on a six levels maturity scale: 0 - Non-existent: when There is no awareness that IT-enabled investments should be managed as a portfolio, 1 – Initial when some business functions apply portfolio management practices in isolation within their scope of activities, 2 - Repeatable when there is increasing awareness of the need to manage IT-enabled investments as a portfolio, 3 - Defined when there is a general understanding of portfolio management practices and business cases are required for all programs, 4 - Managed when board and executive management are fully committed to portfolio management and regularly review performance of the portfolio, 5 - Optimized when portfolio management practices are part of the corporate culture. The portfolio is continuously monitored and proactively adjusted to optimize its value [3].

Table 2. Portfolio Management Audit Tasks

Proc. Ref.	Audit Tasks	Key Control
PM1	Opportunities for IT to influence and support the business strategy are understood and communicated. Investment mix is appropriate. Resources needed to support the business strategy are identified.	IT opportunities Investment initiatives
PM2	Funding is available and committed. Actual spend to date is known. Options for obtaining additional funds are identified.	Budget
PM3	Inventory of business and IT human resources. Current and future demand for business and IT human resources is determined. Tactical plans for business and IT human resources are maintained. Resources required, how resources will be reassigned, acquired or developed.	Tactical HR Plan
PM4	Each program business case is evaluated and scored. Stage-gates for each individual program's full economic life cycle are determined.	Investment programs
PM5	Management reports are provided for review. Status reports are performed on objectives achieved, risks mitigated, deliverables and performance.	Management reports Status reports
PM6	Investment portfolio is reviewed on regular basis Business changes are reflected in investment programs.	Portfolio performance

Management should seek to optimize the performance of the portfolio, establishing successful trends in line with strategy. Organization should be able to incorporate any external or internal changes of business environment into the investment portfolio, to manage the performance and adjust it based on new requirements.

7.3 Investment Management Audit Tasks

Following processes should be evaluated to assess the maturity of Investment Management within an IT Governance program:

- IM1 Develop and evaluate the initial program concept business case.
- IM2 Understand the candidate program and implementation options.
- IM3 Develop the program plan.

- IM4 Develop full life-cycle costs and benefits.
- IM5 Develop the detailed candidate program business case.
- IM6 Launch and manage the program.
- IM7 Update operational IT portfolios.
- IM8 Update the business case.
- IM9 Monitor and report on the program.
- IM10 Retire the program.

Val IT can be used to benchmark the findings resulted from performing the tasks presented in Table 2, on a six levels maturity scale: 0 - Non-existent: when the enterprise sees IT as an end in itself and the focus is on delivery of technology, 1 – Initial when there is some recognition of the need to improve the governance of technology investments but the focus is usually on costs of technology, 2 - Repeatable when there is increasing management awareness of the need to take a business value view of IT-enabled investments, 3 - Defined when management understands the need to manage IT-enabled investments as programs, and is increasingly aware of the importance of managing organizational change, 4 - Managed when board and executive management are committed to investment management and there are clear responsibilities and accountabilities for all stakeholders, 5 - Optimized when board and executive management are proactive in regularly reviewing program performance and executive management assigns accountability for managing full economic life-cycle costs, financial and non-financial benefits, and risks.[3]

Table 3. Investment Management Audit Tasks

Proc. Ref.	Audit Tasks	Key Control
IM1	Investment opportunities are recognized. Business outcomes are described in initial program conceptual business cases. New ideas adopted are rewarded.	Conceptual Business Cases
IM2	Analysis of the alternatives to a candidate program is performed.	Candidate program documentation
IM3	All resources needed for delivering programme's expected business outcomes are documented. Roles and responsibilities are assigned.	Program plan
IM4	Financial and non-financial benefits are known for the entire life-cycle of the programme. Business benefits are specific, measurable, achievable, relevant and time-bound (SMART).	Benefits realization plan.
IM5	Detailed program business cases are developed. Technical aspects are approved by CIO.	Detailed Business Cases
IM6	Program is managed, monitoring its performance against key criteria. Remedial actions plans are taken when required.	Resource allocation and status reports.
IM7	Contents of all IT portfolios affected by the investment program are updated.	Updated of IT portfolios.
IM8	Current status of the program is reflected in the business case.	Updated Business Case.
IM9	Schedule, funding, completeness and quality of functionality, user satisfaction, and the status of business and IT function internal controls are monitored.	Performance reports
IM10	Lessons learned are documented. Active investment portfolio does not include completed programs.	Active investment portfolio

Management should understand the importance of managing the IT enabled investments as programs, as business benefits might not be tracked at project level. Organizational change has to be involved to see IT investments from a business value perspective, and business case development should be supported by standard modeling tools.

8 ISACA and CGEIT

ISACA was founded in 1969, incorporating as the EDP Auditors Association. In 1976 the association formed an education foundation to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field. Today, ISACA has more than 86,000 members worldwide in more than 160 countries and cover a variety of professional IT-

related positions: IS auditor, consultant, educator, IS security professional, regulator, chief information officer and internal auditor.

Since its inception, ISACA has become a pacesetting global organization for information governance, control, security and audit professionals. Its IS auditing and IS control standards are followed by practitioners worldwide. Its research pinpoints professional issues challenging its constituents. Its Certified Information Systems Auditor (CISA) certification is recognized globally and has been earned by more than 70,000 professionals since inception. The Certified Information Security Manager (CISM) certification uniquely targets the information security management audience and has been earned by more than 10,000 professionals. The Certified in the Governance of Enterprise IT (CGEIT) designation promotes the advancement of professionals who wish to be recognized for their IT governance-related experience and knowledge and has been earned by more than 200 professionals [9].

The newly released certification, Certified in Risk and Information Systems Control (CRISC) designation is for IT professionals who identify and manage risks through the development, implementation and maintenance of information systems (IS) controls. These professionals help enterprises accomplish business objectives such as effective and efficient operations, reliable financial reporting, and compliance with regulatory requirements.

ISACA Romania Chapter (www.isaca.ro) has about 250 members that can benefit from ISACA global resources, significant discounts to ISACA's publications and events and offer the possibility to take any exam for obtaining certifications issued by ISACA, in Romania.

CGEIT is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. It is designed for professionals who have management, advisory, or assurance responsibilities. This certification will benefit the individual, through recognition of their professional knowledge and competencies; skill-sets; abilities and experiences, and will enhance their professional standing. It will also add value to the enterprises they support through the demonstration of a visible commitment to excellence in IT governance practices.

9 Conclusions

Val IT Framework is currently on of the best practices for IT Governance. IT Governance can serve as a vehicle for enhancing the contribution of IT to the organization, can decrease the IT expenditures, can strengthen the internal controls, and can prove if adopted the organization's interest for continuous performance improvement.

In the present context, when most of the organizations don't have a structured approach for IT management practices, the IS Role should be primarily in educating the organizations and drawing recommendations for adopting a business value perspective for IT enabled investments, programs linked to benefits stated in business cases well documented, and a value governance framework based on an IT strategy, with clear vision and objectives, short and long rage tactical pan, clear responsibilities for managing value across the organization.

In the end, the IS Auditor should answer to three basic questions: Value Governance - Is there in place an organization structure to manage value? Portfolio Management - Are IT enabled investments tracked to benefits? Investment Management - Is performance of IT initiatives managed and monitored?

References

[1] IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, pp. 11, 14, 19, 24, 28.

[2] Environmental Protection Agency, *Applied Information Economics (AIE) Analysis Of The Desktop Replacement Policy*, pp. 4.

[3] IT Governance Institute, *The Val IT Framework 2.0*, pp. 6.

[4] Information Systems Audit and Control Association, *IS Auditing Standard, Planning.*

[5] Information Systems Audit and Control Association, *IS Auditing Guideline, Planning*.

[6] Information Systems Audit and Control Association, *IS Auditing Guideline, Use of Risk Assessment in Audit Planning.*

[7] Information Systems Audit and Control Association, *IS Auditing Guideline, IT Governance.*

[8] Information Systems Audit and Control Association, *CISA Review Manual*, 2009.

Florin-Mihai ILIESCU, CISA, CISSP, has graduated the Faculty of Computer Science, University Politehnica of Bucharest in 1999. He holds a Master of Science diploma in Computers' Architecture and he is Certified Information Systems Auditor (CISA) and Certified Information Systems Security Professional (CISSP). Currently he is General Manager of Info-Logica Silverline SRL (www.infologica.ro) a company he started in 2004 specialized in IT Audit and Consulting. For his contribution to CISA Review Manual and CISA Exam Study Materials he has awarded with "ISACA Certificate of Appreciation". In 2009, Florin has been elected Membership Director of ISACA Romania Chapter.