IS Audit Considerations in Respect of Current Economic Environment

Vlasta Svata
Department of Systems Analysis
Faculty of informatics and statistics
University of Economics in Prague
W. Churchilla 4, 130 67 Praha 3
vlasta.svata@vse.cz

DOI: 10.20470/jsi.v2i1.79

Abstract: Accountancy organizations, regulatory bodies, standard setters, and other international organizations have developed guidance, articles, frameworks and resources on issues related to the global financial crisis. Now there is a clear and widely accepted need for more rigorous governance over companies’ systems of internal control. Historically there exist many different activities aiming to support effective enterprise governance (legislative acts, best practices, standards, frameworks). But all these activities may have reinforced the already-existing focus on enterprise governance, but they did not necessarily bring clarity to the topic. Therefore we can currently notice some changes aiming to improve the adoption and adaptation of best practices and standards within the area of enterprise governance. The paper discusses the changes in the Enterprise Governance of IT/IS, audit/assurance evolution, and intended Cobit improvements.

Key words: Taking Governance Forward, Cobit 5, IS audit, IS assurance, enterprise governance of IT, Information Reference Model, theory of rational expectations

1. Introduction

Business is subject to continuous changes implicated by technological advances, globalization and internationalization, and the way entities are organized and conduct their business. Management’s increasing responsibility over corporate accounts, and unprecedented competitive pressure have also increased the danger of fraudulent information mainly in financial reporting. The scandals and financial failures of recent years have been a force driving change, especially in the attitudes of market regulators. Most information systems today are affected by one or more regulations, and some would argue that industries as a whole are over-regulated. That is particularly true in industries such as banking and insurance. There are many valid reasons for regulations, especially when it comes to information systems. A significant portion of business processes and activities in most organizations depends completely on information systems, and could not function without them.

In this situation internal and IT auditors are in a unique professional position. Their traditional and primary duty is to inspect and verify that business processes and practices are carried out as required by various regulatory bodies. Additionally, the main output of an audit activity is an audit report that describes risks, control deficiencies, and breach of existing controls. Auditors also can assume the role of trusted advisor and suggest ways to improve existing processes and add new processes, tools, and best practices that improve performance and reduce operating costs.

Therefore currently we can notice some new activities and changes in the IS audit environment. They can be presented through the next main activities:

- moving from IT governance to enterprise governance of IT
- integration of advanced enterprise governance frameworks into one complex best practice COBIT 5
- understand the limits of audit/assurance activities and thus enhance their application and practices.
- COBIT: different views of enterprise governance arose, leading to confusion on the relationships among them. This is currently the incentive for the new initiative aiming to formulate the more integrated and advanced framework of enterprise governance of IT and
thus open the wide discussion of all interested parties which should result in the new version of Cobit.

- IS Audit/Assurance: corporate reporting and the auditing profession are heavily involved in the process of business recovering from the last financial scandals. There have been calls for enhanced audit practices as well as regulations helping to prevent or predict similar financial problems. But the question is, weather the audit can meet such expectations.

2. Enterprise Governance of IT

Many entities have proposed various definitions of governance, in which they tend to be focused on a particular view or type of governance, activities or roles. The following high-level definition of governance is proposed, to cover all types and views:

Governance is the framework, principles, structure, processes and practices to set direction and monitor compliance and performance aligned with the overall purpose and objectives of an enterprise [4].

In this definition, the enablers of governance are “framework, principles, structure, processes and practices”; the activities are “set direction and monitor compliance and performance.”

Recently we can notice new features in IT Governance interpretation. The old concept of „Governance“ was defined based on layers, from which the next three were the most important: Corporate, Enterprise and IT (Figure 1).

The reason for this top-down decomposition of governance principles was derived from the historical sequence of the events and related standards forming the idea of Governance (e.g. OECD Principles of Corporate Governance, SOX, COBIT, COSO, COSO-ERM, ITIL V3, ISO 27000). Even to the fact, that it was stressed, that each governance level depends heavily on the next two levels, there was no unified framework which can help those, involved in governance, to answer the questions: who is accountable and responsible for governance, what should be done and why, and what kind international good practices, standards and guidance documents can be applied?

Figure 1: The old concept of Governance based on layers

The reason for this top-down decomposition of governance principles was derived from the historical sequence of the events and related standards forming the idea of Governance (e.g. OECD Principles of Corporate Governance, SOX, COBIT, COSO, COSO-ERM, ITIL V3, ISO 27000). Even to the fact, that it was stressed, that each governance level depends heavily on the next two levels, there was no unified framework which can help those, involved in governance, to answer the questions: who is accountable and responsible for governance, what should be done and why, and what kind international good practices, standards and guidance documents can be applied?

Figure 2: Enterprise Governance of IT [4]
The initiative called The Taking Governance Forward (TGF) should help answer these questions. It is based on the new framework Governance “On Page” which defines three primary views of governance:

- **Enterprise governance** is the overarching view of governance and applies to all enterprises. It is the highest level view of the governance framework; all governance views within it must be constructed in such a manner as to support the outcomes it defines. The term “corporate governance,” which some people use interchangeably with “enterprise governance,” is reserved for governance specific to corporations only and very often is based on legal and regulatory compliance. Therefore, enterprise governance is considered to be more generic and to take a wider view.

- **Entity governance** deals with a specific line of business within the enterprise (e.g., the MP3 line within a consumer electronics corporation), a specific function within the enterprise (e.g., compliance) or a specific entity within the enterprise (e.g., a branch office in a multinational corporation).

- **Asset management** ensures that those managing the critical asset report back to the owners of the asset. It should be noted that the term “assets,” as used in this initiative, is not to be confused with only those assets appearing on a financial statement. These assets can be tangible (e.g., people, technology, capital, facilities, equipment) or intangible (e.g., intellectual property, processes, brand, reputation, knowledge, legal structures). Portfolio, program and project governance reside in this view.

Figure 2 takes the generic governance views and customizes it for the enterprise governance of IT, which incorporates business governance of IT and functional governance of IT. In the context of IT corporate governance focuses on corporate legal and regulatory compliance issues that relate to IT; entity governance focuses on IT function issues, and/or asset governance on IT asset issues. Combination of entity and asset management called business governance of IT is sometimes referred to as “demand” side of governance and it addresses ensuring that IT is aligned with and supports the business strategy (can be supported by Val IT framework); functional governance of IT can be referred as the “supply” side and it ensures that IT function operates effectively and efficiently to deliver IT services (can be supported by COBIT, ITIL).

3. **COBIT Evolution**

The best practice COBIT which is the most recommended standard for IT Governance implementation has already 14 years history:

- In 1996, the first edition of COBIT was released.
- In 1998, the second edition added “Management Guidelines”.
- In 2000, the third edition was released.
- In 2003, an on-line version became available.
- In December 2005, the fourth edition was initially released.
- In May 2007, the current 4.1 revision was released.
- In early 2011 the first Cobit 5 deliverable will be available.

Currently COBIT 5 is designed in alignment with the mapping initiative TGF and development activities will take place throughout the remainder of 2010.

COBIT 5 will be a major strategic improvement providing the next generation of ISACA’s guidance on the enterprise governance of IT. Building on the more than 15 years of practical usage and application of COBIT by many enterprises and users from the business, IT, security and assurance communities, COBIT 5 will be designed to meet the current needs of stakeholders and align with the most up-to-date thinking in enterprise governance and IT management techniques.

Based on limited information about the new version of Cobit, the main differences comparing with Cobit 4 is the concept of one integrated framework encompassing different models.

Till now, Cobit 4, Val IT, Risk IT and ITAF\(^1\) frameworks were separated each other even to the fact they followed the same philosophy. Cobit 5 will be consolidated into a single overarching framework

---

\(^1\) ITAF – Information Technology Assurance Framework - provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programmes and develop effective reports.
integrating all above frameworks. A new product set will be developed recognizing that the content will need to be presented, readable and usable in practice for diverse range of stakeholder needs (external, internal – owners, governing body, management).

This new more complex concept of Cobit 5 need to be supported by new architecture. The core part of this architecture is a database repository – knowledge base, which will ensure, that all the available components are complete, consistent, properly organized and easily maintained in the future. Furthermore the knowledge base will have links to external standards and best-practice sources. This part of architecture will be accompanied by next two parts – layers, so the final architecture will have next three layers [5]:

- **Cobit 5 stakeholders** – This layer considers stakeholders for IT and their needs and objectives. These needs provide a lens to the knowledge base and through this lens relevant content of Cobit 5 knowledge base is selected and converted either in products or customized deliverables.
- **Cobit 5 knowledge base** – This layer contains complete set of knowledge contained in Cobit 5 including all domain – and process – related information. This information is structured using the models and components defined in the Cobit 5 metadata.
- **Cobit 5 metadata** – This layer contains the description of all components used in Cobit 5 and the relationships between them.

![Figure 3: Cobit 5 architecture](image)

Users of Cobit 4 are already familiar with the Process Model and the Maturity Model. New version of Cobit will introduce other models which are either new one (e.g. Information Reference Model) or are taken from another frameworks and aligned to Cobit 5 (e.g. Risk Model, Value Model, Resource Model, Control Model, Organizational Structures Model or Behavioural and Skills Model).

As an example the Information Reference Model is briefly described. Its new proposal represents one of the most complex model which attempts to describe all important information dimensions.

Cobit 4 deals with the next information criteria:

- **Effectiveness** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
Confidentiality concerns the protection of sensitive information from unauthorised disclosure.

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.

Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

Cobit 5 defines information as the step between Data and Knowledge on the information life cycle. The dimensions of information are enlarged to next levels:

- **Information criteria** to which information should conform:
  - Privacy
  - Regulatory
  - Security (Confidentiality, Integrity, Availability)
  - Quality (Consistency, Clarity, Completeness, Timeliness, Accuracy, Relevance, Reliability)

- **Information stakeholders**: Who have an interest in the information, e.g., for conformance reasons? Special impact will be on the stakeholder type and stakeholder role (Owner, Custodian, Sender, Receiver).

- **Information purpose**: Information can serve many purposes, e.g., operational information, or instructions, or monitoring information, etc. It is possible to express the purpose in terms of the TGF communication flows between different roles.

- **Information attributes** that can be used to further describe and manage information, e.g., lifespan, context, access channels, etc.

- **Information type**: Is it current or old information, what is the nature of the information?

- **Information use**: By whom is the information used? By which business processes? Which actions can be performed on it?

New architecture of Cobit 5 should result in the new set of publications (Figure 4). The initial and core publication will be Cobit 5 Framework. It will provide a comprehensive and clear description of the Cobit 5 purpose, how it can be used and what other products will support better governance and management of IT.

Following the initial framework publication Cobit 5 will consist of a set of publications which will be created by selecting or filtering of specific content from the Cobit 5 repository. They will respect the different views of process owners and IT professionals responsible for specific areas and roles. Thus there will be available publications specific from different point of views (objectives, enabler, functional, organizational, responsibility).

Last type of publications will be guidelines enabling a common approach to both implementation and assurance. (e.g. Implementing and Continually Improving IT Governance and IT Assurance Guide).

4. **IS Audit/Assurance Limitations**

The word ‘audit’ is being used in the Czech Republic as well as in the other countries with growing frequency. In addition to financial audit, which are the original and trendsetting type of audit, there are now environmental audits, information systems audits, management audits, forensic audits, data audits, intellectual property audits, medical audits, teaching audits, technology audits, stress audits, democracy audits and many others besides. More generally, the spread of audits and other quality assurance initiatives means that many individuals and organisations now find themselves subject to audit for the first time and, regardless of protest and complaint, have come to think of themselves as auditees. Indeed there is a real sense in which all advanced countries have become an ‘audit society’[1].
Audit in general is defined as a systematic process of objectively obtaining and evaluating evidence regarding assertions about business actions and events to ascertain the degree of correspondence between those assertions and established criteria, and communicating the results to interested parties. It is a form of attestation service in which the auditor issues a written report expressing an opinion about whether the financial statements are in material conformity with generally accepted principles or other recognized criteria [2].

Last few years we can notice the trend to substitute the term audit by the term “assurance”. The objective of an assurance initiative is for an assurance professional to measure or evaluate a subject matter that is the responsibility of another party. For IT assurance initiatives, there is generally also a stakeholder involved who uses the subject matter but who has delegated operation and custodianship of the subject matter to the responsible party. Hence, the stakeholder is the end customer of the evaluation and can approve the criteria of the evaluation with the responsible party and the assurance professional. The conclusion of the evaluation provides an opinion as to whether the subject matter meets the needs of the stakeholder (Figure 5). Assurance is thus much broader concept than auditing. Assurance also covers evaluation activities not governed by internal and/or external audit standards and thus helps executives to approve, whether the subject matter is able to attain the stated goals.
Currently, focusing on the IS/IT area, we can distinguish between next most often applied types of evaluation: assurance, compliance audit, operational audit, financial audit and IT Audit or assurance. The differences in goals and used criteria are shown in the **Figure 6**.

<table>
<thead>
<tr>
<th>Type of evaluation</th>
<th>Goal</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assurance</td>
<td>Effectiveness – relevance to business objectives</td>
<td>Stated strategic goals</td>
</tr>
<tr>
<td>Compliance audit</td>
<td>Compliance to regulations</td>
<td>Law, ISO/IEC standards, best practices, etc.</td>
</tr>
<tr>
<td>Operational audit</td>
<td>Efficiency – optimal use of resources</td>
<td>CBA, BSC</td>
</tr>
<tr>
<td>Financial audit</td>
<td>Financial effectiveness – relevance to stakeholders expectations</td>
<td>Fairness of the financial statements and prevention of fraud</td>
</tr>
<tr>
<td></td>
<td>Compliance with specified accounting and audit criteria</td>
<td>International and national law dealing with accountancy</td>
</tr>
<tr>
<td></td>
<td>Efficiency of internal control systems over financial reporting</td>
<td>ISA, COSO, INTOSAI</td>
</tr>
<tr>
<td>IS Audit/Assurance</td>
<td>IS Effectiveness –Relevance to business and IT objectives,</td>
<td>Stated IT goals</td>
</tr>
<tr>
<td></td>
<td>Compliance to IT regulations</td>
<td>Law dealing with IT aspects (e.g. protection of personal data), ISO/IEC 27000, ISO/IEC 24000, ITIL, COBIT VAL IT, IT BSC</td>
</tr>
<tr>
<td></td>
<td>Efficiency – optimal use of resources, risk management</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 6: Different types of evaluation**

Trying to apply these types of evaluation in practice, we can face many problems. Going through professional or public communication media, we can register many statements dealing with either the call for some kind of audit as a reaction to some problem or the criticism, that specific audit (audit firm or auditor) did not fulfilled the expectations of the stakeholders. The frequency of such statements usually increases in the time of financial scandals or crisis.

Owing to the fact, that theory provides a cornerstone for explaining auditing/assurance practices, next part of paper provides short introduction to the theory and problems of auditing in general.
Auditing has evolved in the capital market economy. The original purpose of audit was to assure that honest and accurate accounting for money and property has been performed in the affairs of government and business as well. In the 1920s and 1930s, Professor Theodor Limperg of the University of Amsterdam presented a set of auditing concepts, which became known as the theory that inspires confidence. Later this theory was called the theory of rational expectations [2]. This dynamic theory explains how evolving society’s needs for reliable financial information results in the changes in the auditor’s function and methods. The auditor should be governed by the rational expectations of those who may use his/her report. These expectations should not be disappointed (general auditing norm), but in the same time auditor should not arouse greater expectations in his/her auditor’s report than his/her examinations (tools, practices) justifies. Furthermore, Limperg focuses on the social responsibility of the independent auditor and the mechanism for ensuring that audits meet society’s needs. He views auditor as the independent professional acting as a confidential agent for society. Auditor thus must have authority to ask all information about the subject matter but in the same time he/she must be responsible and knowledgeable enough to assess the materiality of the problems (deviations) and publish only information relevant to the stakeholder’s expectations. In 1960s Mautz and Sharaf [6] attempted to highlight the scientific nature of auditing. In their view, the status of auditing as a science depends upon the term “science”. If we conceive science as an organized body if knowledge, then auditing can lay some claim to meeting the requirements. If science is interpreted to mean the application of a method requiring the rigorous weighing of evidence and the application of a systematic method to a variety of situations, again auditing may qualify. But if we accept as science only those fields with the power to explain, predict, and control given phenomena, then auditing falls well short [2]. Mautz and Sharaf believed that to obtain a comprehensive view of auditing, one should see it as a five-level structure (Figure 7).

Even to the fact, that under some circumstances audit can be viewed as a separate discipline, auditing like any applied field has become so concerned with the problems of practice that auditors sometime
neglect theoretical aspects. The reasons making theoretical concepts in relation to audit difficult are perhaps the next one:

- Audit and assurance is an emerging principle of social organization which is empowered by each financial crisis. Audit practices have grown because of changes in public sector management and newly prominent ideals of quality, governance and accountability. And yet paradoxically, while audit technologies have contributed to managerial concerns about ‘performance’, the performance of audit itself is far from being unambiguous and free from public dispute.

- Audit has the ethical as well as the economical dimension. The auditor is not merely an economic agent which reduces the risk of unfair communication between two parties and thus is adding value to business processes. He/she must have moral mission which must be somehow safeguarded by regulations or otherwise.

- Audit is linked to ideals of organizational transparency and accountability. They provide comfort to stakeholders who are remote from day to day practices. But in doing so, they cannot merely use criteria like international external or internal standards, best practices or frameworks. They must provide assurance, that those standards are applied within the context of stated business, regional, national or international strategy depending on the level of audit.

- Audits are usually publicly visible when they fail. The cost of audits are high but the benefits are ambivalent and a source of controversy. Furthermore, the main aim of audit is to improve the accountability, but the accountability for the audit itself is limited.

5. Conclusion

Current global financial and business catastrophes launched the fundamental changes in the IS auditing. The changes in the understanding the IT Enterprise Government Framework are the base for the new version of best practice Cobit and both of them result in the new more broader concept of IS Assurance. This changes deal mainly with the theoretical concepts, but in case they will be approved and accepted as the new standards, norms, best practices, they will without any doubts influence the everyday management practices in many enterprises. Whether they will bring intended improvements in business process operation and IT value delivery we are not able to say now, and we have to wait several years.

[2] An Introduction to Auditing and Assurance, Chapter 1, vig.pearsoned.co.uk/catalog/uploads/Soltani_C01.pdf, 2010

JEL Classification: M15