IT Governance

The IT Governance Audit (IGA)

Open Universiteit

faculteit Managementwetenschappen

Cursusteam

ir. H.B.F. Hofstee, *cursusteamleider* en *auteur* Open Universiteit

prof. dr. R.J. Kusters, *auteur,* Open Universiteit

Programmaleiding

prof. dr. R.J. Kusters, Open Universiteit

Disciplineleiding

prof. dr. R.J. Kusters, Open Universiteit

Werkboekonderdeel

The IT Governance Audit (IGA)

Productie

Open Universiteit, Heerlen

Eerste druk september 2012

Cursuscode B.70.3.3.2

Inhoud

1 Introduction

An audit is a recognized management technique. A typical audit will provide a structured process that enables the depiction and analysis of a specific target area in an organisation in order to understand / improve and/or to achieve a specific purpose.

Best developed and known are financial audits. These are typically carried out by external and certified auditing organisations. Their objective is to assure that the financial statements of an organisation (e.g. balance sheets, income statement, cash flow statement) provide a fair representation of the operational and financial condition of the organization (Flesher, 1996).

Nowadays the processes that result in these financial statements are heavily supported by information systems (e.g. the finance module of an ERP system). And indeed all (or at least nearly all) data used to calculate these statements are stored in databases (and/or spreadsheets). Following this, a shift in focus from auditing these financial statements towards including auditing in the procedures, data and associated information systems can be observed. This is the competence area of the electronic data processing (EDP-) auditor.

Following the Enron (2001), Worldcom (2002), Parmalat (2003), Ahold (2003) and Lehman Brothers (2008) financial scandals, an increased focus on this area can be seen. A typical example is the American Sarbanes-Oxley (SOX) legislation (2002)[1]. This legislation requires the management of all companies registered in the USA to ensure appropriate internal controls of financial reporting. The general interpretation is that the IT function must make sure there are appropriate internal controls in place. This is especially relevant when making any changes to any software system that plays a significant part in financial controls or reports. It is supported by explicit SOX audits. Many foreign (e.g. Dutch) companies have to proof they comply to the SOX regulations by carrying out a SOX audit since they e.g. have a registration at the New York Stock Exchange.

This example shows that the area of IT is often target of specific audits. In this paper the concept of an IT Governance Audit (IGA) will be introduced as a framework that can be used in this course. The objective of an IT Governance Audit is to show that the organization's management is dealing appropriately with its IT resources, given the importance IT has for this organization.

This paper is structured as follows. Section 2 will discuss general characteristics of an audit. Section 3 looks at some of the audits that can be found in the IT field. Section 4 discusses the added value of an IGA and positions such an audit against other IT area audits. Section 5 presents the characteristics of an IGA.

2 Audit characteristics

A number of issues / characteristics surrounding audits can be distinguished. In this section we will discuss a number of these. The following characteristics are discussed:

- Type of audit

[1] A United States federal law which set new or enhanced standards for all U.S. public company boards, management and public accounting firms. In various European Countries similar rules and / or guidelines exist or new European Union regulations are under construction.

- Benefits
- Reference
- Process

2.1 Type of audit

Looking at the purpose of an audit, two different categories can be distinguished: the *compliance* audit and the *advisory* audit.

The compliance audit has as primary purpose to show (proof) that an organization complies with some (external imposed) set of requirements. The SOX audit is a typical example of a compliance audit. Its purpose is to show that the organization has internal control standards set that are of sufficient quality and are adhered to in the organization. Other typical examples can be found in the quality management area, where many standards exist (e.g. ISO 9000 for general process quality), along with associated audits. The requirement to show compliance often implies that the audit has to be carried out by an external independent agent.

An advisory audit has as primary purpose to provide advice to management regarding e.g. the problems and appropriateness of systems and practices in an organization. A typical example of an advisory audit in the area of IT is the information audit. Its purpose is the identification of the users' information needs as well as how well these needs are met by the information services department (St. Clair, 1995). An advisory audit typically is a 'once in a while' type of activity that helps understand how well an organization is performing in a specific area. Since the result of such an audit is likely to support the future direction of the organization, it is closely linked to strategic planning. As such it is in principle an internal activity, although regularly outside consultants are invited to carry out such an audit.

The distinction between compliance and advisory audits is not as clear as this discussion might suggest. The results from a compliance audit can also be used to give advice to management. In fact, in the field of quality the benefits of an ISO 9000 compliance audit might be an ISO certification document, but its stated objective is to allow the organization to achieve a better control of process and product quality. Similarly, shareholders of a company don't require a SOX audit to comply with the law, but to show that their investments are managed in a safe manner. The results of an, in principle externally oriented, compliance audit can very well be used for internal improvement activities. Similarly, the results of a, primarily internally oriented, advisory audit can, if the audit has been well structured, planned and executed, support the organization externally. E.g. by showing prospective customers that the organization is seriously addressing a relevant and recognized problem area such as customer responsiveness.

2.2 Benefits

A number of different benefits from an audit can be distinguished. The following list is derived from (Botha & Boon, 2003) and (Buchanan & Gibb, 1998, 2007, 2008).

Benefits for the staff involved can be:

- Awareness

    - Identifying costs and benefits of information resources.
    - Identifying opportunities to use information resources for strategic competitive advantage.
    - Creating awareness of the importance of information resource management and defining the management role
- Understanding
    - Integrating IT investments with strategic business initiatives.
    - Identifying information flows and processes.
- Involvement
    - Developing an integrated information strategy and/or policy.
    - Monitoring and evaluating conformance with information-related standards, legislation, and policy guidelines.
- Training

Benefits for the organizational issue that is being audited, can be:

- Understanding
- Analysis
- Improvements
- Certification

2.2.1 Staff Benefits

For the staff involved in a well-structured, well-planned and well-executed audit a first benefit (at least from the point of view of the employer) is *awareness* and *understanding* regarding the issues being audited. If process quality is deemed by management to be an important issue, increasing the awareness and understanding of the staff involved in this issue is an important contribution. Because, without this, a complex issue such as process quality will not advance in the organization.

Closely related is the next step of *involvement*. If awareness and understanding of the issue is achieved, the likelihood of a staff feeling involved and taking responsibility for the issues increases.

Finally, both the audit process as well as the results of the audit is useful for *training* purposes, since they provide an accurate picture of the current state of affairs that can be communicated as part of a training process. One can think of the introduction of new employees or a refresher course for existing staff members.

2.2.2 Organizational issue related benefits

To achieve *understanding* of the audit subject is a primary objective of an advisory audit and at least a secondary objective of a compliance audit. The audit provides a valid and accurate picture of reality that can be used as a sound basis for further discussion, analysis and/or decisions.

Analysis and analysis-based diagnostics are mentioned (Botha & Boon, 2003) as the most important benefit of an audit. Analysis of the current situation allows identification of strong points that need to be treasured and weak points that need to be dealt with.

Based on such an analysis structured *improvement* can be undertaken to deal with these issues. A final benefit is that of *certification*. Executing a SOX audit might be beneficial for the functioning of the financial control system, in the end there exists a legal obligation to show through certification that the organization complies to the SOX requirements. Less legally binding, an ISO 9000 certificate will be very useful for an organization engaged in heavy competition to convince potential customers.

2.3 Reference

An ISO9000 compliance audit is based on an explicit reference: the ISO9000 standard. The purpose of the audit is to assure that both procedures and actual practices in the organization comply to the requirements set in the ISO-standard.

Similarly, a SOX audit is often based on an explicit comparison with a reference. Both the COBIT (http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx) and COSO frameworks (http://www.coso.org) are in use for this purpose. Although the current COSO framework is not approved as the standard, it seems however to be the framework most companies are using to comply with the legal requirements.

It is obviously easier to audit something when the objective is to compare an existing situation with an explicit reference. Such a reference may be used as a basis for the description of the current situation since it points out what to look for. And in a next step it makes analysis in principle fairly straightforward, since this is reduced to identifying gaps between what is expected to exist, based on the reference, and what is actually available in the current situation.

On the other hand this also exposes a danger inherent in this approach. If the audit is being reduced to a mere 'form completion exercise', chances are that this is not done very carefully and thoroughly.

The benefits mentioned above mainly rely on an audit being well planned and executed and depend on people who are actually willing to think carefully and thoroughly about the audit results.

Not all audits use an explicit reference. (Botha & Boon, 2003) describe a number of information auditing approaches where no explicit reference is provided and selection of facts as well as their interpretation is left to the particular auditor. Intermediate approaches also exist.

As an example one may look at the information audit as designed by (Buchanan & Gibb, 1998). They suggest a number of reference frameworks that might be used, but leave the final decision to the discretion of the auditor. In a later publication the authors (Buchanan & Gibb, 2007) refer to an information audit taxonomy from three perspectives: a strategic perspective, a process perspective and a resource perspective. This taxonomy provides the auditor with the flexibility to focus on one or

more individual components dependent upon individual circumstances and requirements. However, in general the proper use of a relevant reference would make sense.

2.4 Process

Since an audit is usually not carried out routinely, it should be well prepared, planned and executed. Please note that an audit does not take place in a vacuum. There is always a specific reason to start an audit, and the resulting report should not be the end of the affair, but in essence the start of new activities. In these new activities the actual processes of strategy development, strategy based planning and organizational change has to be dealt with. This remains outside the current discussion.

Design of an audit process, specifically tailored to the target organization, is therefore normal practice. Standard (compliance) audits usually have well defined process plans available that only need to be altered slightly to fit with local requirements. In other cases a more explicit design of the process is required. Specific design of audit processes will be determined to a large degree by the specific scope and objective of the audit (Buchanan & Gibb, 2007).

However, in general, based on various audit approaches as discussed in (Botha & Boon, 2003) and (Buchanan & Gibb, 2008), the following seven methodological stages are summarized:

- *Setup*: design of the scope and objective of the audit, together with the reference to be used, project planning, preparation of business case, endorsement, organizational communication, and preliminary analysis.
- *Review*: strategic analysis (internal and external), organizational (cultural) analysis, determine data requirements, available sources, and the means of gathering the data.
- *Survey*: plan the activities, select participants, gather data by survey of information users, identification and inventory of information resources, mapping of information flow.
- *Account:* cost, business benefit and/or value of information resources.
- *Analysis*: use the data gathered to analyse them (if possible with respect to the reference used) and draw conclusions.
- *Report:* production and dissemination of information audit findings and recommendations
- *Guide* organizational information management policy and/or information strategy development, implementation of recommendations, establishment of the IA as a cyclical process, and monitoring and control.

3 Audits in the IT field

In principle anything can be the subject of an audit. And indeed, many different types of audits are in common use. We already mentioned the finance and quality related audits that enjoy widespread usage. Also, within the field of IT a large diversity of (standard based) audits can be found. A (non exhaustive) list of methods will be presented to show the diversity in audit approaches currently available in the IT area.

For this purpose the IT area will be subdivided into three sub areas:

1. The strategic information management area (this area focuses on processes and products of strategic information management).

2. The system development area (this area focuses at processes and products of system development).

3. The infrastructure and system management area (this area focuses on processes and products aimed at managing the existing IT resources).

3.1 The strategic information management area

In this area several variants of an information audit are used. An information audit involves identification of user information requirements and how effectively these are met. In addition to this, the costs and benefits of information resources to the organization are determined. The final purpose of such an audit is to determine if the IT resource contributes to achieving the organizational objectives. This type of audit uses no specific reference. The analysis is therefore at least difficult and possibly subjective. Botha and Boon (2003) provide a good overview of the literature in this field.

They identify the following variants of basic information audits described above.

- *The communication audit* focuses on organizational information flow patterns.

- *Information mapping* focuses on the identification and use of organizational information resources.

- *The information systems audit* investigates the way in which technological tools are used to manage information resources.

In their information audit taxonomy Buchanan and Gibb (2007) refer to this area as 'the strategic perspective': the strategic perspective focuses upon the realization of strategic objectives through mapping and analysis of the relationship from organizational mission to information resources.

3.2 The systems development area

In this area a number of fairly generally accepted standards exists that can be used as a reference. More information can e.g. be found in (Hughes & Cotterell, 2006). Two approaches focus at project management. *The Project Management Body of Knowledge* is a general overview of relevant knowledge in this field. It is supported by the project management institute and served as the basis for certification of project managers. A similar standard, *Prince2*, is sponsored by the UK government and is used commonly in Europe.

The Capability Maturity Model Integration (CMMI) is an approach that looks at software development process maturity, indicating the sophistication and quality of the process. The CMMI is maintained by the American Software Engineering Institute and is worldwide in use as the basis for process improvement activities as well as process audits aimed at assessing the current status and identifying future improvement actions.

Closely related is the *ISO9000:2000 standard* for assessing the quality management system, guiding software development. This standard focuses on measurement based continuous improvement by

targeting customer requirements, staff quality and process quality in conjunction. The standard is not developed specific for software development but is being applied there.

A reference for assessing software product quality is the *ISO9126 standard*. It provides a language describing relevant software quality characteristics and adds to that an extensive set of metrics that support their operationalization. A separate standard *ISO14598* describes the procedures that should be carried out when assessing a software product to the ISO9126 standard.

3.3 The infrastructure and system management area

In this area a number of standards provide *best practice based reference process descriptions* that can be used both for assessing a current situation as well as for identification of improvement activities. Further information can be found in (Santana Tapia, 2006), from which the following section is quoted.

The first three standards are related to the model of *IT service management* introduced by (Looijen, 1998). The model identifies the following three areas of IT management and associated standards.

1. *The Technical management* area is responsible for maintenance and management of the technical IT infrastructure. This infrastructure consists of all the used automation resources to store, process and provide data and information. Technical management consists of the technical components of the automated information systems, the equipment, the basic programs and communication systems, including related procedures and documentation. A management framework for this area is ITIL. ITIL, the *Information Technology Infrastructure Library* is a set of best practices for IT service management. ITIL is supported by the UK government and is acquiring general acceptance in Europe. ITIL provides businesses with a customizable framework of best practices to achieve quality service and to overcome difficulties associated with the growth of IT systems.

2. *The Application management* area is responsible for the maintenance of the application programs and databases. Application management corresponds to the function of a software house: producing, maintaining and adapting application designs and programs. This is the working area of ASL. ASL, *the Application Service Library*, is a framework for application management that is also based on best practice processes. It is maintained by the ASL foundation and rests on the assumption that the quality of primary process is directly linked to the quality of the supporting IT systems. ASL is intended to simplify the process of application management by providing best-practices processes to do it.

3. *The Functional management* area is on behalf of the user organization responsible for maintaining and controlling information of the organization. From the perspective of the user organization and the business process, this management area has as goal to support the organization and the business process by means of the management of the information. BiSL is a framework for functional management and information management. BiSL (*Business Information Service Library*) is, like ITIL and ASL, a set of recommendations for organizations to work more efficiently. The framework describes the planning of the operational functional management and information management, on the basis of best practices. This process model underlines the importance of the role of information management and functional management in organizations for the connection between IT and business processes. This

framework provides guidelines for processes and activities that are necessary for a proper information provisioning structure within organizations.

In their information audit taxonomy Buchanan and Gibb (2007) refer to this area as 'the resource perspective' (the resource view focuses on identification, classification, and evaluation of information resources) and 'the process perspective' (the process perspective focuses upon work flow and associated information flow through modelling of organizational processes).

4 The IT Governance Audit (IGA)

In this paper we want to introduce the concept of an IT Governance Audit (IGA). The objective of IGA is to show that the organization is dealing appropriately with its IT resources, given the importance of IT for this organization.

4.1 Key questions to be answered

The goal of an IGA is to focus on the organization as a whole, take a step back from the details of everyday actions and problems and try to answers these two key questions in conjunction:

I. What is the importance of IT for this organization?

II. Are the main decisions regarding management of IT taken appropriately?

The questions are related, since an organization where IT currently has little or no strategic impact will require different answers to these key questions when compared to an organization where IT is the main strategy enabler.

Answering question I is therefore a prerequisite in order to be able to answer question II. Answering these questions will support an organization in its strategic decision making processes and allow it to prepare its objectives and basic management structures in such a way that the organization is able to cope with the continuing impact that changes in IT will / can / is likely to have on its internal and external functioning.

4.2 Is another type of audit needed?

Realizing the large number of audit types / audit references as presented in the previous section, the question might rise why another type of audit is needed. The answer to this is simple: none of the currently available IT audit approaches are aimed at this level.

ITIL provides best practice procedures for IT infrastructure management processes. ASL and BiSL provide best practice process information aimed at technical application management processes. These approaches are clearly aimed at the more tactical and operational aspects of IT management rather than the strategic aspects aimed for in an IGA.

The information audit approaches described by (Botha & Boon, 2003; Buchanan & Gibb, 1998, 2007, 2008) come closest to the purpose of an IGA. Its purpose is the identification of the users' information needs as well as how well these needs are met by the information services department (St. Clair, 1995). These approaches do aim at the strategic level.

And indeed, in the methodology described by (Buchanan & Gibb, 1998) is included an approach toward providing answers for key question I (see the guidelines for the 'identify' stage). However, when looking at key question II it can be seen that the information audit approaches choose to audit the current information *resource* situation. There is no doubt that an audit of the current information resources is a worthwhile activity (see e.g. (Botha & Boon, 2003)). However, we feel that this provides a limited, static view of the current situation and it certainly provides no clear picture of the ability of an organisation to cope with changes in the (IT) environment.

4.3 Strategic alignment

IT as one of the primary production assets is a continuously and fast evolving technology. This means that such issues as *strategic alignment* will need to be adapted on a continuous basis to new circumstances. An audit showing how the current information resources are coping with the current situation provides little or no information on how the organisation will be able to cope with the situation (the) next year(s).

An alternative is to focus on the more general IT alignment decisions (Henderson & Venkatraman, 1993) that guide both the current and the future ability of the organization to deal with changes in IT in a continuously and fast changing environment. The current information resource situation can be seen as the result of a series of strategic management decisions in the past. These decisions might have been seen as strategic at the time they were taken. They might have been perceived as strategic afterwards, or, in a worst case situation, were the result of inactivity that has resulted in default decisions, that could afterwards be seen to have been of strategic importance.

A future situation will develop over time, and is based again on a series of strategic decisions. It is our contention that insight in the way the organization will be able to identify the need for these strategic decisions and take appropriate action, is guided by the basic IT Governance choices that have been made. An IGA audit will provide information on what these basic choices are and support management in the weighing the pros and cons of the various options.

In essence the IGA addresses a part of the strategic alignment model(Henderson & Venkatraman, 1993), c.f. **Figure 1**). Key question I focuses on the I/T strategy quadrant: are the main (strategic) decisions regarding management of IT (Technology Scope, Systemic Competences, I/T Governance) taken appropriately. Key question II focuses on aspects of the functional integration axis: what is / should be the position of IT in the organization. As illustrated in **Figure 1** these two key questions together (I and II) provide a solid understanding of the current (strategic) IT Governance situation.

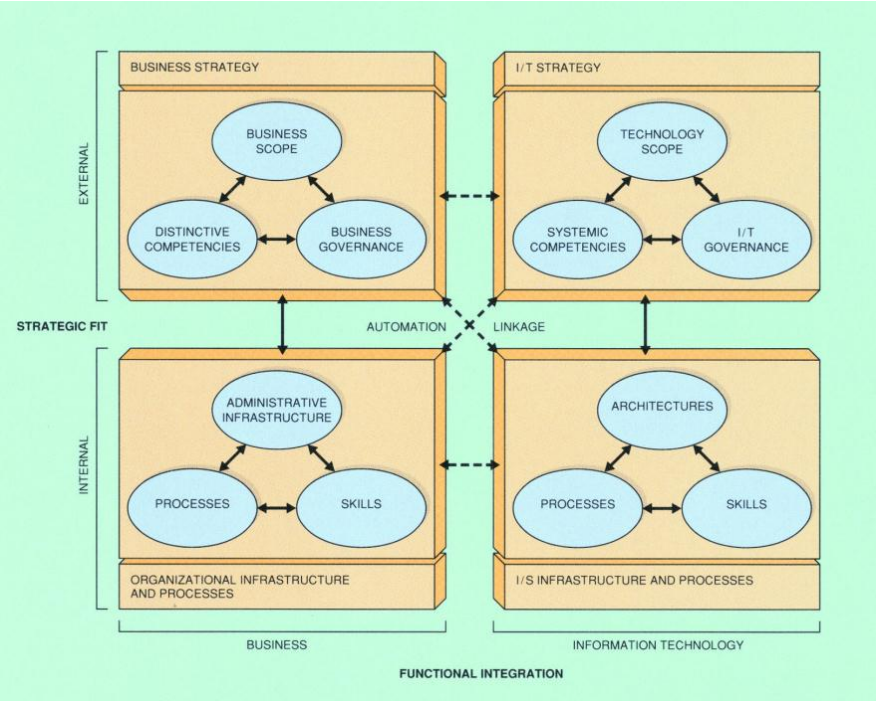

Figure 1 Strategic Alignment Model (Henderson & Venkatraman, 1993)

5 IGA characteristics

An IGA can be described according to the same characteristics as given in section 2

- Type of audit
- Benefits
- Reference
- Process

5.1 Type of audit

An IGA can be characterized as an *advisory* audit, since no standard exists against which compliance can be tested. Its objective is to advice management whether the right choices with regard to the key questions I and II have been made. In addition it can provide the basis for changes in the recognition of the role of IT for the organization as well as leading to new decisions regarding the main IT Governance arrangements.

5.2 Benefits

Apart from certification, all benefits mentioned before in the section on audit characteristics (section 2) are applicable to an IGA.

5.3 Reference

No formal reference exists that can be used in an IGA. In fact, this area is still being researched and new insights appear at a regular basis. However, a significant body of literature is being produced that can form the basis for the development of a reference.

For instance a starting point for a reference for key question I is provided in the papers by (Buchanan & Gibb, 1998, 2007, 2008). Also newer additions might be looked for. This is typical of what can be expected. Since insights into this field are constantly being developed and extended any reference will soon be outdated. This implies that a reference will need to be redeveloped regularly, based on state of the art materials.

These state of the art materials can be found in the academic press. Furthermore, some relevant books exist that receive updates on a regular basis. A good example is the book by (Applegate, Austin, & Soule, 2009). This book, with new editions coming out on a regular basis, provides a good basis for a reference. In earlier editions the authors explicitly mentioned that the book could be seen as the basis for an IT Governance Audit[2]. In later editions, this was not referred to anymore, but the authors never explicitly dropped this perspective. In our view it still can fulfill this function.

5.4 Process

The normal process, as described before in the section on audit characteristics, can in principle be applied. Two specific issues warrant discussion. First, since no wide recognized and accepted reference exists, the process step of reference selection will often lead to reference development. As was mentioned before, in (academic) educational environments (Applegate et al., 2009) can efficiently serve as the basis for such a reference development activity. If necessary additional academic literature can be searched and used for the construction of more specific reference models[3].

A second issue deals with the analysis phase. In the audit characteristics section (section 2) it was said that analysis of the current situation allows identification of strong points that need to be treasured, and weak points that need to be dealt with. However, given that key question I is not aimed inward but has an explicit external focus, analysis should also look at opportunities that invite further action and threats that require addressing. This means that analysis can take the form of a SWOT-analysis (Dyson, 2004; Hill & Westbrook, 1997; Weihrich, 1982).

[2] Applegate et.al., 5th edition, page 15: "…An analysis of these areas for a firm, complete with appropriate recommendations, is referred to as an IT management audit…."

[3] In this course a *reference model* is defined as the *frame of reference* used in the audit constructed on the basis of academic literature. It consists of a set of logical and consistent statements derived from literature on what is wise and sound to decide on IT management issues and/or on what needs to be present in a certain quantity or quality, in a specific situation.

6 References

Applegate, L. M., Austin, R. D., & Soule, D. L. (2009). *Corporate Information Strategy and Management. Eighth Edition. Text and Cases.* (8 ed.). New York: McGraw-Hill Irwin.

Botha, H., & Boon, J. A. (2003). The Information Audit: Principles and Guidelines. *Libri, vol. 53*, pp. 23–38.

Buchanan, S., & Gibb, F. (1998). The Information Audit: An Integrated Strategic Approach. *International Journal of Information Management, Vol. 18*(No. I,), pp. 29~47.

Buchanan, S., & Gibb, F. (2007). The information audit: Role and scope. *International Journal of Information Management, In Press, Corrected Proof*.

Buchanan, S., & Gibb, F. (2008). The information audit: Methodology selection. *International Journal of Information Management, 28*(1), 3-11.

Dyson, R., G. (2004). Strategic development and SWOT analysis at the University of Warwick. *European Journal of Operational Research, 152*(3), 631-640.

Flesher, D. L. (1996). *Internal auditing standards and practices: A one semester course*. Altamonte Springs: Institute of Internal Auditors.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: leveraging information technology for transforming organizations. *IBM Syst. J., 32*(1), 4-16.

Hill, T., & Westbrook, R. (1997). SWOT analysis: It's time for a product recall. *Long Range Planning, 30*(1), 46-52.

Hughes, B., & Cotterell, M. (2006). *Software Project management (Fourth edition)* (4 ed.): McGraw-Hill.

Looijen, M. (1998). *Information Systems Management, Control and Maintenance*. Deventer: Kluwer Bedrijfsinformatie.

Santana Tapia, R. G. (2006). IT process architectures for enterprises development: A survey from a maturity model perspective. Enschede, Netherlands: Centre for Telematics and Information Technology, University of Twente.

St. Clair, G. (1995). Ask the customers. *The one-person Library: a newsletter for Librarians & Management, 22*(20), 6-8.

Weihrich, H. (1982). The TOWS Matrix -- A Tool for Situational Analysis. *Long Range Planning, 15*(2), 54-66.