IT as driver of Control Rationalization

How can organizations determine the potential for rationalizing controls based on IT?

P. Weel (9981160)
O. Helmond (9981169)

EDP Audit opleiding
Vrije Universiteit Amsterdam

University counsellor: T. de Boer
Company counsellor: H. Bootsma
# TABLE OF CONTENTS

1. **PRELIMINARY INVESTIGATION**................................................................. 4  
   1.1. Introduction ..........................................................................................4  
   1.2. SOX year one experiences .................................................................4  
   1.3. The way forward ..................................................................................5  

2. **RESEARCH APPROACH**.................................................................. 7  
   2.1. Introduction ........................................................................................7  
   2.2. Reason for Research ...........................................................................7  
   2.3. Problem definition ..............................................................................7  
   2.4. Conceptual Model ...............................................................................8  
   2.5. Research Method ...............................................................................9  

3. **INTERNAL CONTROL PERSPECTIVE**........................................... 10  
   3.1. Risk based versus rule based ..............................................................10  
   3.2. COSO ................................................................................................10  
   3.3. Types of controls ...............................................................................11  
   3.4. How Internal Control influence IT based control rationalization ..........13  
   3.5. Summary ............................................................................................15  

4. **ORGANIZATION PERSPECTIVE**..................................................... 16  
   4.1. Introduction ........................................................................................16  
   4.2. Structures in five ..............................................................................16  
   4.3. Implications of Mintzberg for IT based control rationalization ..........17  
   4.4. Summary ............................................................................................18  

5. **IT PERSPECTIVE**............................................................................ 20  
   5.1. Introduction ........................................................................................20  
   5.2. Cobit as a starting point ....................................................................20  
   5.3. Strategic alignment ..........................................................................22  
   5.4. Value delivery ..................................................................................23  
   5.5. Resource management & Performance measurement .......................26
5.6. Risk management ........................................................................................................ 27
5.7. Summary .................................................................................................................. 29

6. CONCLUSION .............................................................................................................. 30
6.1. Results of analysis .................................................................................................... 30
6.2. Focus point model ................................................................................................... 31
6.3. Reflection ................................................................................................................ 33

LITERATURE .................................................................................................................... 34

APPENDIX I: TERMINOLOGY ....................................................................................... 37

APPENDIX II: THE COSO LAYERS EXPLAINED ....................................................... 39

APPENDIX III: STRUCTURES ACCORDING TO MINTZBERG ................................. 42

APPENDIX IV: DIMENSIONS IN STRUCTURES IN FIVE ........................................... 43

APPENDIX V: MATURITY LEVELS ACCORDING TO COBIT 4.0 ............................... 46
1. Preliminary investigation

1.1. Introduction
This thesis focuses on the regulation Sarbanes Oxley\(^1\), its impact on organizations to comply with these rules, its impact on IT and the opportunities for IT in this context moving forward. In this chapter a preliminary investigation is described. This investigation is used as input for the research approach which is described in the next chapter. We performed the preliminary investigation by reviewing the past, present and future for Sarbanes Oxley\(^2\). In this process an emphasis has been put on IT.

1.2. SOX year one experiences
The Public Company Accounting Reform and Investor Protection Act of 2002, or in short the Sarbanes Oxley Act, is not only the quickest defined law in American history (2 months) but also one with a big impact on all public companies in the US. The Act requires them to develop new practices related to corporate governance and financial reporting. The main objective of the Act is restoring the public's trust in the capital markets. One of the most challenging aspects of the Act’s requirements involves the responsibilities the CFO carries for internal controls. This article is commonly known as section 404. This section requires that public companies take responsibility for maintaining an effective system of internal control.

After the first year of SOX, several researches have been performed to measure the efforts to become compliant with the Sarbanes Oxley Act. One of the most named attention point of these evaluations was the level of compliance costs. When the Act was passed in 2002, the Securities and Exchange Commission (SEC) estimated that compliance with SOX would cost $91,000 per company (excluding consulting and audit fees)\(^3\). That was bad guesswork. A survey by Financial Executives International (FEI) concluded that public companies have incurred greater than expected costs to comply with section 404 of the Sarbanes Oxley Act. The average total cost was about 50 times the SEC estimate\(^4\): $4.36 million; this is 39% more than the $3.14 million companies had expected to pay, based upon a July 2004 FEI cost survey. Their total costs of compliance averaged $1.34 million for internal costs, $1.72 million for external costs, and $1.30 million for auditor fees.

The key highlights of a research paper\(^5\) confirm the high costs made: 60% of companies with revenues greater than $20 billion invested more than 100,000 hours in Section 404 related activities (excluding the external auditor hours). Among 70% of companies surveyed by Ernst & Young, a large audit firm, Section 404 related costs were over 50% higher than original estimates.

More recent studies show the same trend: According to an AMR Research of January 2006 one-third of companies reported that SOX spending exceeded expectations in 2005; none of the companies

---

\(^1\) The Sarbanes-Oxley (SOX) act was introduced into the USA following the massive bankruptcies of Worldcom and Enron and an alleged $7 trillion loss in US stock market capitalisation, after investors lost faith in the transparency of corporate financial practices. Sections 302 and 404 of the SOX act specifically require public US companies to establish, implement and evaluate their internal controls for purposes of financial statement reporting and operational integrity.

\(^2\) For purposes of this thesis, the terms “Sarbanes-Oxley,” “the Act,” and “SOX” all refer to the Sarbanes-Oxley Act of 2002 in its entirety, including all sections of the law enacted by Congress, all associated rules promulgated by the Securities and Exchange Commission and all related standards issued by the Public Company Accounting Oversight Board.

\(^3\) SEC Final Rule, August 2003; http://www.sec.gov/rules/final/33-8238.htm

\(^4\) FEI Survey on Sarbanes-Oxley Section 404 Implementation; October 2005

\(^5\) Emerging Trends in Internal Controls, Fourth Survey and Industry Insights – E&Y (Ernst & Young) Business Assurance and Advisory Business Services - September 2005

TextBox 1:
"We know the costs are real, but let’s remember that this is also an investment for the future. As any good business person knows, you invest time and effort and money, and then you reap the benefit of what you’ve done ... Sarbanes-Oxley compliance is an investment in every company, it is an investment in our financial system, and it is an investment in the strength of the United States capital markets.”

Rep. Michael Oxley, R-Ohio, March 10, 2005
Speech: Sarbanes-Oxley: Making the Investment, Reaping the Rewards (Georgetown University Law Center Corporate Counsel Institute)
reported lower than anticipated expenses. 83% of the companies expect SOX expenditures to stay the same or increase in 2006\(^6\). The study calculated the current average cost of SOX compliance which is $1 million per $1 billion in revenue.

Main conclusion which can be made is that the costs and efforts to implement and assess internal controls to comply with SOX are high and are far exceeding the expected. This is recognized as such by the initiators and upholding organization of the legislation. Still, they believe profoundly in the act (see also textbox 1 and 2).

"Are all these changes worth the cost and effort? The cost is heavy – they’ve been underestimated for the most part, and it’s hard to measure the benefits. But given the massive scandal that led to Sarbanes-Oxley, the system had to be tightened. "Our capital markets run on faith and trust. Being able to report that a company has in place "strong internal controls" strengthens public confidence. If that’s the case, I think it’s worth the cost.”

Donald Nicolaisen, Chief Accountant, SEC, November 19, 2004
BNA Daily Report for Executives

Textbox 2

1.3. The way forward

1.3.1 PCAOB and SEC\(^7\) response

In response to the concerns of public companies management and the large audit firms, the SEC and PCAOB have worked collaboratively in developing new Section 404 related proposals. This resulted in guidance for management’s evaluation of internal control over financial reporting (ICFR) and other related amendments to existing rules by the SEC\(^8\) and a new auditing standard (Audit Standard 5), intended to supersede the former standard (Audit Standard 2) of the PCAOB\(^9\). With these new guidance’s companies have the ability to change their approach to comply with SOX.

By analyzing and comparing the new SEC guidance with the former guidances, we can conclude the following:

- the new guidance is described as principle-based (as opposed to detailed guidance) and is intended to assist companies of all sizes in completing their annual evaluations in an effective and efficient manner;
- the SEC emphasized that its guidance is intended to be scalable, flexible, and based on a top-down, risk-based approach;
- the form and extent of required documentation to support the assessment will vary based on the size, nature, and complexity of the company;
- the guidance clarifies that management and the auditor are permitted to have different testing approaches;
- management should consider factors such as interaction of different controls and compensating controls in determining if a deficiency, or combination of deficiencies, is a material weakness;
- management’s evaluation of deficiencies should be based on both quantitative and qualitative factors and should consider certain “strong indicators” in determining whether a deficiency is a material weakness.

The PCAOB’s auditing standard 5 supersedes the former standard and is intended to achieve three principles:

- focus the audit on the matters most important to internal control of Financial Reporting;

---

\(^6\) Sarbanes-Oxley Section 404 Costs and Implementation Issues: Survey Update – January 2006
\(^7\) SEC stands for Securities and Exchange Commission. It is a United States government agency having primary responsibility for enforcing the federal securities laws and regulating the securities industry/stock market. PCAOB stands for The Public Company Accounting Oversight Board which is a private-sector, non-profit corporation to oversee the auditors of public companies. Its stated purpose is to ‘protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports’.
eliminate unnecessary procedures;
scale the audit for smaller companies.

Looking at the major changes compared to the former standard, in specific the structure of the PCAOB standard, the following can be concluded:

- the standard raises the profile of the importance of professional judgment;
- the standard permits the ability of experience to be considered in concluding on low risk areas;
- the standard preserves the requirement for a single standard for all public companies;
- the standard recognizes the importance of scaling work based on size and complexity of the company.

When the guidance is read with the perspective of how a company can reduce compliance costs without jeopardizing the compliance the following steps need to be taken (refer to appendix I - terminology for definition of terms):

1. pinpoint Company Level Controls that effectively mitigate location/account risks;
2. consider qualitative risk factors (e.g., susceptibility of loss due to errors or fraud), not just quantitative significance;
3. risk rate business units and business lines considering qualitative risk factors;
4. risk-rate processes and major classes of transactions using qualitative risk considerations (e.g. non-routine transactions);
5. confirm that relevant financial reporting risks (including fraud and GCC's) are identified, and risk-rate control objectives;
6. develop the most effective and efficient controls and develop efficient test plans.

1.3.2 The definition of control rationalization
Based on the new rules and year one experiences we notice in our practice that companies have a need to “rationalize” their internal controls in year 2, to reduce the efforts it takes to comply with the Sarbanes-Oxley act and eventually reduce their compliance costs. We have defined control rationalization for this thesis as follows:

Control rationalization is the continuous process of designing the most effective and efficient controls, to address risks. It includes applying a top-down, risk-based approach, eliminating unnecessary controls, using of risk-based testing plans, optimizing the design of company-level and automated controls, and strategically standardizing and centralizing controls.

This definition contains different elements, including a top-down, risk-based approach but also optimize automated controls. This element will be highlighted in this thesis.
2. Research Approach

2.1. Introduction
In the preliminary investigation we introduced the Sarbanes Oxley Act and its impact on companies to comply with this Act. Most of the Dutch companies completed their first year of SOX compliance in 2005. As discussed earlier in the preliminary investigation, most companies indicated that project costs far exceed the expectations of the companies CFO’s.

Surveys disclosed reasons such as the absence of clear guidance, focusing too much on process level instead of applying a top-down risk based method and a lack of a consistent, methodical approach. Even in the best cases, abundant opportunities for reducing costs while maintaining compliance were not fully exploited.

Companies indicated that for the second year under the Sarbanes Oxley Act they will focus more on costs. One way to reduce the cost is to rationalize control frameworks. We defined control rationalization as a continuous, systematic approach driven in a top-down, risk based manner. One important element of the control rationalization approach is to increase reliance on IT controls.

2.2. Reason for Research
In this thesis we want to pick out the IT element of control rationalization. After the first year most companies had the perception that they documented and tested too many General Computer Controls (GCC’s). This has been, in part, confirmed by the SEC’s most recent publication of guidance on SOX. Furthermore companies chose manual controls instead of automated controls within their process control frameworks. As part of rationalizing their complete internal control structure, companies can leverage the advantages of IT controls. They can consider for example enabling internal control functionalities in their Enterprise Resource Planning (ERP) systems. Many articles state that automated controls reduce human error as well as the costs of manual testing, which improves the compliance effectiveness and at the same time it lowers compliance costs. 10.

These advantages sound fair, but how easy is it for companies to achieve these benefits? What if a company is fully decentralized and the IT environment does not meet the required maturity? This thesis will address these questions. How can organizations determine the potential for rationalizing controls based on IT?

2.3. Problem definition
This research will mainly focus on how to determine what potential organizations have to optimize the role of IT in a control rationalization process. The problem definition is defined as follows:

**How can organizations determine the potential for rationalizing controls based on IT?**

In detail:

**Organizations:** Public companies which are listed on the Stock Exchange in the United States and therefore are required to comply with the Sarbanes Oxley act.

**Potential:** expressing the possibilities and abilities of companies.

**Rationalizing Controls:** continuous process of designing the most effective and efficient controls, to address risks (for further explanation refer to chapter

---

10 L. Ditmar, Governance & Compliance; driving IT priorities, Financial Executive, February 2006, page 51

“... Simply complying with the rules is not enough. They should make this approach part of their companies’ DNA. For companies that take this approach, most of the major concerns about compliance disappear. Moreover, if companies view the new laws as opportunities – opportunities to improve internal controls, improve the performance of the board and improve their public reporting – they will ultimately be better run, more transparent, and therefore more attractive to investors.”

William Donaldson, SEC Chairman
Remarks at National Press Club, July 30, 2003
1.3.2) which is required to comply with the Sections 302 and 404 of the SOX act.

**Based on IT:**

optimization of the design of automated controls with the aim to optimize the effectiveness and efficiency of managing risks.

Subsequently the following sub questions need to be answered to come to a final conclusion:

1. How do we define control rationalization and what is the relation to the IT component?
2. How can internal control characteristics contribute to IT based control rationalization?
3. How can the organizational characteristics contribute to IT based control rationalization?
4. How do IT characteristics contribute to IT based control rationalization?
5. How can the characteristics of the IT, organization and internal control perspectives be used to assess the potential for IT based control rationalization?

We performed our research from a SOX perspective, meaning that we identified factors that are relevant for companies which have to comply with SOX. However control rationalization is not a concept only used by those companies. Therefore the outcome of our research can also be used by companies that want to give IT a more prominent role in their internal control framework. Since our focus is on the control rationalization process in relation to SOX compliance, only controls for managing financial reporting risks have been taken into account.

**2.4. Conceptual Model**

As described earlier, the new guidance from the SEC in Audit Standard No. 5 clearly states that the internal control over financial reporting is intended to be a principle-based guidance which fits companies of all sizes and is intended to be scalable, flexible, and based on a top-down, risk-based approach.

With this statement, the SEC says that the organization itself is an important factor for effective and efficient internal control program. Furthermore the SEC states that the way internal control management is carried out in the organization determines the effectiveness and efficiency of the internal control program. These two areas could have a relation with control rationalization as this is the process of developing an effective and efficient internal control framework. The focus of our thesis is on the role of IT in this process and therefore we limit our research to IT-related aspects, when identifying key indicators and elements that support the process of control rationalization.

Based on the above, we will focus our research on three perspectives: internal control management, organization, IT and. We’ve integrated these into the following conceptual model.

![Conceptual Model](image)

Our assumption is that the three perspectives provide insights for determining the potential for IT based control rationalization. By using these insights and identifying the mutual dependencies, a model with focus points for determining the potential of IT based control rationalization will emerge.

The exploration of the internal control perspective will be performed to identify how internal control elements influence IT based control rationalization. By using the COSO model we are able to identify different layers of control and how these layers, and the way they are used by companies, influence the potential of rationalizing controls with IT. The rationale for using COSO is that it is a generally
accepted control framework that guides organizations to structure their activities in becoming and staying compliant.

The exploration of the organization perspective will be performed by using insights of Mintzberg\textsuperscript{11}. The rationale of using Mintzberg is that this theoretical model is a good starting point to characterize organizations as it is focused on effectiveness of organizations. Furthermore it is a well proven model to define aspects of organizations. With his theory we are able to identify how the type and dynamics of an organization influence IT based control rationalization.

The exploration of the IT perspective will be performed by using Cobit as a starting point. The rationale for using Cobit is that it is a framework used by managers to align IT control requirements with the business risks and helps organizations to increase efficiency. The relation between automated controls and general computer controls will be identified. Furthermore how these general computer controls and maturity of the IT organizations influence IT based control rationalization will be explored.

2.5. Research Method
The research strategy applied will be a reflection of a development. The objective of this reflection is to define success factors for the research object, in our case elements that help determining the potential of IT based control rationalization.

This research will be performed by means of desk research. Input for the desk research include: publications and articles on SOX Compliance, control rationalization, PCAOB and SEC guidelines, the COSO integrated framework, ISACA and ITGI publications on IT and SOX compliance and Cobit 4.0.

In the next chapters we will describe the results of the analyses from the three perspectives (internal control, organization and IT) and the interrelations between these factors. Based on the outcome of these analyses we will build a focus point model which helps an organization to determine the potential of IT based control rationalization.

\textsuperscript{11} In his work 'Structures of Fives' ('Organisatiestructuren' in the Dutch print) Mintzberg identifies relevant parameters for effective organizations. This is done in combination with a mapping of typical organizational structures. (Mintzberg, 2001)
3. **Internal Control perspective**

In this chapter we will describe three elements which we assume are of main influence on control rationalization from the internal control perspective. We will start with describing the risk based versus rule based approach and analyze the advantages of adopting a risk based approach. Secondly the concepts of internal control will be described including entity and process level controls. Furthermore the COSO framework will be introduced.

In the second part of the chapter we will combine the three elements with regard to their role in control rationalization.

Outcome of this chapter is how an internal control approach and different layers of internal control, have influence on a control rationalization process in general and on IT based control rationalization in special.

3.1. **Risk based versus rule based**

During the first year of SOX compliance most companies have adopted the method of implementing 'best practices' as is published by several research companies. This approach was adopted through the rule based approach which was dominant. In a rule based approach all elements, as described in the Act, are covered without making a distinction of the importance for the company. Companies wanted to avoid the risk of not complying, as initially it was not clear what the SEC was going to rule with regard to the assessments of internal controls. E.g. low risk areas were treated the same as high risk areas.

As time progressed it became more and more clear that the SEC is open for arguments. That is, a company should be able to show that applicable risks are covered sufficiently. Realizing this, it became clear that a risk based approach can be adopted. This view is confirmed by the PCAOB via the frequently asked questions released on 16th of May 2006 (Question number 38).

The starting point of a risk based approach is that management carefully analyses their company and processes and identifies risks. Moving forward using this approach, internal controls can be identified which cover the risks defined earlier. Following, the organization can work to set up a lean and balanced internal control framework.

An advantage of a risk based approach concept is that a company constantly risk rate all elements such as business units, control objectives and accounts. The risk based approach is only focusing on significant accounts on the financial statement, identifying the business units and processes related to those accounts and implement an internal control program for the related process risks. The risk based approach enables companies to adjust the level of internal control on the risk identified for a certain process, business unit and account. The way to control a low risk area can differ from a high risk area, for example in the types of controls used. In the next sections of this chapter we will explain the different types of controls and introduce the COSO model as a supporting framework.

3.2. **COSO**

The Sarbanes Oxley Act emphasizes the importance of internal controls in general. The act requires organizations to use and implement a for their organization suitable internal control framework. The Audit Standard 2 released by the PCAOB states the following:

"Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework established by a body of experts that followed due-process procedures, including the broad distribution of the framework for public comment."

Furthermore the PCAOB states that COSO is a generally accepted control framework, however companies are free to use other frameworks:

"In the United States, the Committee of Sponsoring Organizations ("COSO") of the Treadway Commission has published Internal Control – Integrated Framework. Known as the COSO report, it provides a suitable and available framework for purposes of management's

12 PCAOB 'Questions 38 – 55’, May 16 2006, Question no.: 38
Using the concepts of the COSO framework makes it easier to link the internal control activities to SOX because of the fact that the PCAOB based its work on COSO. The basic lay out of the COSO model consists out of five elements and is depicted in the figure below. The different layers are explained in appendix II.

![Figure 2: Five layers of COSO](image)

Active using the elements of the COSO framework guide organizations to structure their activities in becoming and staying compliant. The COSO model is generic for organizations. For IT control environments specific frameworks have been set up in line with the COSO model:

- Cobit 4.0: this framework will be introduced in chapter 5 (the IT perspective) and focuses on IT control environments in general
- ‘IT Control Objectives for Sarbanes-Oxley’: in a specific document, the IT Governance Institute has set up a ‘guide’ for SOX and IT control environments (latest version dating September 2006).

There is no clear distinction as to which perspective is best practice. Both Cobit 4.0 and the ‘IT Control Objectives for Sarbanes-Oxley’ are set up by the IT Governance Institute. With regard to the application of the frameworks they acknowledge each other as good drivers for control although the use of the documents can vary under specific circumstances (e.g. the IT Control Objectives for Sarbanes-Oxley’ is set up especially for SOX circumstances).

### 3.3. Types of controls

Companies can adopt different kinds of controls. Well known terms in this respect are company level controls, entity level controls, entity wide controls and process level controls.

The PCAOB describes company-level controls (PCAOB AS 2.53) as controls that are associated with the control environment, centralized processing, period end financial reporting, and monitoring results of operations. Company Level Controls may reside at the entity-level and at the process-level and may include all five COSO components. Company Level Controls and Entity Level Controls are synonymous with each other.

In case a control is applicable for the entire organization and not only a specific part of the organization it is called an entity wide control. Controls that are effective in achieving process-level control objectives are process level controls.

Entity level controls can be recognized by the fact that they cover specific parts of a company, generally business units/entities. Process Level Controls typically cover the ‘Control Activities’ layer of the COSO model. The entity level controls can cover all COSO layers but traditionally focus on Control

---

15 Cobit 4.0
Environment, Risk Assessment, Information & Communication and Monitoring. The logic of the control types is depicted in figure 4.

An organization has the ability to leverage the Entity Wide Controls as much as possible. When a company is able to replace non-entity wide controls by entity wide controls they have the benefit of not having several different process level controls on different business units or entities.

As an illustration we introduce organization ‘A’ using little entity wide controls (figure 6). This organization might be in control of their risk. However, ‘A’ will have to maintain a lot of local controls. E.g. for each business unit they need to make sure that the Information & communication is organized well enough, the control environment has to be maintained etc. However effective it does not look like an efficient and ‘cost effective’ approach.

Let’s now consider organization ‘B’ (figure 5). Looking at the organizational structure and business this organization is identical to organization ‘A’ except for one difference: organization ‘B’ focuses on the use of Entity Wide Controls. With just a couple of controls the most important risks are basically covered. Only very specific controls are left on the entity and process level.

The following arguments/assumptions can be used for having as much entity wide controls as possible:

- to increase the efficiency of the controls assurance processes;
- to prevent inefficiency costs of ‘inventing the wheel’ at multiple levels (redundancy);
- to standardize/harmonize the internal control approach within the organization;
- to enable a better insight into the control framework of specific entities;
- to stimulate the exchange of good and best practices concerning implementation and maintenance of controls.
Application controls vs. manual controls

As described above one of the main control types are process level controls. A distinction can be made between manual controls and application controls.

We define manual controls as controls performed manually by natural persons, commonly as part of a procedure or work instruction, subject to the inherent risk of human error. We define application controls, which are often also called automated controls as controls that are embedded within software programs to prevent or detect unauthorized transactions. When configured appropriately, or used in combination with other manual controls, application controls support the completeness, accuracy, authorization and existence of processing transactions.

When controlling a business process either manual controls, application controls or a combination of both can be used. From experience advantages of application controls are identified:

- Automated controls are less vulnerable to error or manipulation or other potential performance problems that are associated with people-based controls.
- Automated controls can decrease costs by positively impacting the extent, nature and timing of testing for regulatory compliance. That is, a lesser number of sample items are required because the likelihood of an exception is low (extent); automated controls are often easier to test than manual controls (nature); and certain application controls can be benchmarked so that testing frequency can be rotated over a reasonable period of time.

Based on these advantages companies are searching for possibilities to leverage the application controls. A research paper of Gartner confirms this. They looked at the future plans of companies and indicated that automation is one of the key drivers for rationalization. Quite some arguments for the use of automated controls have been used in the last few years. Some parties have been trying to substantiate their claims by making statements as:

"...identified a plan that would allow the client to reduce its ongoing compliance costs by 40% while creating a compliance function to sustain savings over time. Control rationalization and top-down risk-based analysis will save 10% per year in testing expense. Another 10% will be saved by implementing automation and monitoring tools-replacing manual, detective controls with automated, preventative controls. An additional 20% in annual savings will be realized by centralizing and standardizing controls through a shared services approach for business sub-processes."

To this moment no proven cases are known. However, predictions and logic suggest that automated controls will reduce compliance costs in the end. Investigation by Gartner revealed that financial benefits of automation will overshadow the IT organization’s own compliance needs. One of the main arguments used in this research is:

"The more that compliance can be automated and made inherent in systems, the more time then that management can direct to those activities that advance the company’s performance and profit. Five years from now, it is not too much of a stretch to say that the CIO will have more responsibility for the company’s compliance activities than the CFO."

3.4. How Internal Control influence IT based control rationalization.

After we described the difference between a rule based versus risk based approach and the types of controls used to comply with SOX, we can now move into answering our question: what are, from an internal control perspective focus points to use for determining the potential for IT based control rationalization? The answer can be given by combining the information from the first part of this chapter.

When a company uses a risk based approach the benefits for control rationalization, in general, are:

- Mitigate risks effectively as all business units, processes and control objectives are risk rated by using thorough risk assessments.

---

17 Audit Standard 5; paragraphs B28-B33.
19 Gartner, ‘Survey on Sarbanes-Oxley Compliance Practises Within IT Organizations and Business’, September 14 2006
20 Gartner, ‘Survey on Sarbanes-Oxley Compliance Practises Within IT Organizations and Business’, September 14 2006, P. 19
- No over-control of risks as the company adjusts the level of control to the risk ratings.
- More effective use of control types as based on the risk level process level controls can be replaced by more high level controls such company level controls

The risk based approach has the following influence on IT based control rationalization:
- As the risk level of each control objective is clear, companies will focus more on the effective level of control, which could mean that application controls get a more important role (e.g. if a process is over controlled by a manual and application control and one control can be removed, the application control could be preferred because of its advantages).

The use of different types of controls has the following influence on IT based control rationalization:
- When a company is aware of the different types of control it can be used to make smart choices. Entity wide controls are preferred over non entity wide controls and automated controls are, in general, preferred over manual controls.

When taking the six bullets noted above into account, we conclude that whether a company uses a risk based approach and how different types of controls are used, give insights whether they are able to pinpoint the process level controls which can be leveraged to automated controls.

**Evaluating the internal control approach**

In the prior sections we identified that the approach for internal control has an influence on the potential of IT based control rationalization.

An internal control approach that uses a risk based approach logically includes thorough risk assessments. The results of the risk assessments are risk rated processes, business units and control objectives. The next step will be to evaluate the existing control framework on types of control. Controls which do not apply to relevant risks can be filtered out. For all relevant risks an evaluation is required to identify the most effective controls to mitigate the risks. The first focus is on 'promoting' entity level and process level controls to entity wide controls. The next step is to identify opportunities for automating process level controls. In the figure below we depicted the sequence of these process steps.

![Figure 6: Risk Based internal control approach](image)

**Interdependencies with the IT and organization perspectives**

How the internal control mechanism is used by a company strongly depends on how the company is organized and how the IT structure has been laid out.

Depending on the structure of the organization it can be beneficial to translate local controls to entity wide controls. In this way the company level controls are leveraged to a maximum. Under normal circumstances this strategy is not feasible for organizations which are decentralized to a high degree. Processes can differ so much that it will only take more effort to come up with company level controls than to maintain the local controls. Therefore the organizational conditions should be taken into account and will be discussed in the next chapter (the organization perspective).

The way a company can use internal controls and how they can rely on automated controls relates to the way IT is organized, managed, controlled and vice versa. This is of importance for control rationalization as it is necessary to be able to support on general computer controls. Cobit clearly states that there should be a match between the risk appetite and control environment of a company (one of the COSO layers) and the IT policies:
**PO6.1 IT Policy and Control Environment:**

Define the elements of a control environment for IT, aligned with the enterprise’s management philosophy and operating style. These elements include expectations/requirements regarding delivery of value from IT investments, appetite for risk, integrity, ethical values, staff competence, accountability and responsibility. The control environment is based on a culture that supports value delivery while managing significant risks, encourages cross-divisional co-operation and teamwork, promotes compliance and continuous process improvement, and handles process deviations (including failure) well.

Additionally they emphasize the alignment between the IT risks and the organization’s risk management and internal control framework.

**PO9.1 IT and Business Risk Management Alignment:**

Integrate the IT governance, risk management and control framework with the organization’s (enterprise’s) risk management framework. This includes alignment with the organization’s risk appetite and risk tolerance level.

In chapter 5 (the IT perspective) we will further discuss the alignment between the IT risks and the organization’s risk management.

### 3.5. Summary

Initial efforts by companies to become compliant with SOX was by adapting a rule based approach which resulted in cost ineffective control frameworks which were hard to maintain. The new Audit Standard promotes the use of a risk based approach to comply with SOX.

The analyses in this chapter taught us that whether a company uses a risk based approach has an influence in the potential for IT based control rationalization. Furthermore we concluded that the use of different types of controls and mitigate risks with these types of control in a certain sequence also has an influence on the effectiveness of IT based control rationalization. Solely transforming manual controls into automated controls will not lead to the most effective approach, as the risk is there that a company is transforming controls that are redundant or which could be more easily being transformed to another type of control.

The insights of how the organization uses a risk based approach and different types of control contribute in determining the potential for IT based control rationalization. These insights do not stand alone but need to be combined with the business and IT perspective in order to come to an overall approach on IT based control rationalization.
4. Organization perspective

In the previous chapter we analyzed the internal control perspective. During this analysis we already noted that internal control management has a dependency with the characteristics of an organization. In this chapter we will further analyze this. We will determine what a good way to characterize an organization is and how these characters have an impact IT based control rationalization.

4.1. Introduction

In order for organizations to work effectively, coordination is required. Some general definitions for ‘organization’ can be used to illustrate the necessity of coordination:

- 'a group of people who work together'\(^{21}\)
- 'An organization is a formal group of people with one or more shared goals.'\(^{22}\)

In the next section Mintzberg will be introduced as a leading theoretical framework. We believe that this theoretical model is a good starting point to characterize organizations. Furthermore it is a well proven model. Next, the implications of the insights of Mintzberg will be discussed. In the third and final section a method will be introduced for assessing key indicators of organizations that have an influence on the potential of IT based control rationalization.

The main advantages to use Mintzberg’s ‘Structures in Five’ are to:

- identify all characteristics of a company in a methodical way;
- define bottlenecks for changing an organization;
- distinct a typology for the organization. This will enable the organization to identify basic constraints and opportunities for improvement;
- the typology can serve as an indicator on the flexibility of the organization. In addition 'switches and buttons' are provided for organizational change via the design parameters.

4.2. Structures in five

In his work ‘Structures in Five’ (2001)\(^{23}\) Mintzberg illustrates that the effectivity of organizations is depending on its organizational structure. The organizational structure, in its turn, is determined by aspects like age and size of the company.

These two indicators can typically be used to come up with a first assessment of what an organization is expected to be like. E.g. when taking General Electric (GE) as an example one is talking about an old and big organization. In terms of Mintzberg this would lead us to expect a bureaucratic organization. Standardization is key and the expectation for GE to be flexible in adapting changes is considered to be low. This expectation does not necessarily need to be true; it’s merely based on two aspects of which the details are generally known: size and age.

Mintzberg refined his insights on the effectiveness of organizations. He identified 5 general structures for organizations:

1. The Simple structure
2. The Machine bureaucracy
3. The Professional Bureaucracy
4. The Divisionalized form
5. The adhocracy

Organizations can always be associated with these organizational structures. Commonly, organizations will consist of a combination of structures. Each structure, or combination of structures, has its own characteristics on organizational effectiveness. This includes ‘opportunities’ as well as ‘threats’. E.g. within the adhocracy one of the threats is that top management wants to implement formal procedures for the entire company. As one of the typical identifiers of the adhocracy is that employees determine their own work methods and are, in general, not willing to adopt stringent rule sets from top management, this intention is bound to fail even before it’s implemented. Thus, using the insights of Mintzberg management is capable of making intelligent choices on the point of organizational changes.

\(^{21}\) wordnet.princeton.edu/perl/webwn
\(^{22}\) en.wikipedia.org/wiki/Organization
\(^{23}\) In this context a reference is made to the Dutch print dated 2001. The original was printed in 1983 under the title ‘Structure in 5’s: Designing Effective Organizations’ (Prentice-Hall)
For a more elaborate overview of the organizational structures and its characteristics we refer to appendix III and IV. With regard to the organizational structure level Mintzberg identifies five basis elements which indicate the general structure. These are: Strategic management, Technostructure, Middle management, Support staff and Technical core (see figure 3).

For each configuration the balance between these elements will be different as is shown in appendix III. Furthermore, as refinement, Mintzberg defined more specific dimensions for the configurations.

These dimensions are of interest for this thesis because of two reasons:

1. First of all the dimensions provide insight into the current set up of the organization and thereby on its behavioral characteristics. E.g. an organization dominantly typed as an ‘Adhocracy’ has little to no ‘hard’ procedures and is hard to control via formalization of procedures due to it’s dominant culture compared to the ‘Machine Bureaucracy organization’.

2. Secondly one of the dimensions identified by Mintzberg is the ‘Design Parameters’. This dimension provides “tools” which can be used to change the organization.

A complete overview of the dimensions is depicted in Appendix IV. The specific dimensions are subdivided into three groups:

- design parameters (design elements which can be configured by management as desired);
- functioning parameters (elements which are determined by the design parameters);
- environmental parameters (external factors which can not, or hardly, be influenced by the organization).

4.3. Implications of Mintzberg for IT based control rationalization.

In the triangle of internal control, IT and organization, the last perspective does not necessarily provide elements and/or aspects which always need to be addressed. It provides a tool set which can be used in the process of control rationalization.

By performing an analysis based on Mintzberg’s theory a company can characterize its organization and check how a control rationalization approach fits with these characteristics. First the basic configuration needs to be identified. This means that the results and the practical implications can be mapped to the table as depicted in Appendix IV.

Following this step a first insight is available on the threats, weaknesses, strengths and opportunities of the organization and their internal controls. To further detail, a SWOT analyses methodology can be used.

Based on the initial analyses the organization can go back to the internal control process goals. The original goals can be re-assessed and where necessary adjusted. After this, the organizational

24 SWOT stands for Strengths, Weaknesses, Opportunity, and Threat. The SWOT analyses originated from Albert Humphry from the Stanford University in the 1960’s. The SWOT analyses focuses on analysing situations based on internal and external factors. It can be applied to any circumstance if necessary. Most important aspect of applying SWOT in a useful way is by integrating it into a more structured approach. In this sense, applying SWOT analyses into the control rationalizing effort is pregnant with meaning. It gives a clear indication of the why and how of organizational changes in relation to control rationalization.
structure analyses can be picked up again. Via another SWOT, the organization can now map goals to actions and, if necessary, can adjust goals based on impossibilities coming to light.

The starting point for an analysis of the organization should be the internal control perspective as described in chapter 3. From the internal control perspective a 'Soll' scenario can be set up which can be used as benchmark in the SWOT analyses.

Looking at the IT perspective it becomes apparent what the link between IT and the organization is. Questions such as the extend to which IT is centralized and what tools are used within the organization are the main connectors.

When a company wants to change certain characters to leverage the control rationalization process, it should be noted that only the design parameters can be used. In essence these are the only variables which can be influenced. For more detail on the elements and their impact we refer to appendix IV.

The process above can be depicted as follows:

![Figure 8: The organizational process](image)

**An example to clarify the above:**

A typical organization shaped as a Simple Structure tends to be based on a low level of planning and control, have a basic technical environment and to mainly work in an informal manner. This is typical for young and small organizations which are still in an early phase of organizational development.

The organizational characterization using Mintzberg and the SWOT analysis shows a centralized structure of the organization, which enables the implementation of entity wide controls. This can be identified as strength for the company.

A weakness is the fact that the organization is rather small and might not enable actions such as segregation of duties.

An opportunity for the organization to rationalize controls can be to strengthen the planning and control systems and to set up a more sophisticated IT environment.

A threat is the position of power within the organization as it is located with the owner/president of the organization which might not be willing to give up his power or part of it. When control rationalization drives an organization to a point in which big organizational changes need to be executed the owner/president could be reluctant and thereby blocking necessary changes.

Based on the SWOT analyses a scenario can be set up for the organizational change to take place based on the design parameters.

These kinds of organizations have an opportunity to grow by formalizing their communication and setting up a more elaborate planning and control system. In addition by increasing the role of regulated systems the role of IT can be improved as regulated systems are driven by the use of IT (note that the changes are formulated using the design parameters). However, looking at the environmental factors it should be taken into account that the organization is acting in a dynamic and competitive environment and that the power is located with the owner/president of the organization. This will make it difficult to achieve big changes on short notice as the organizational culture and market environment will not enable the change. (Note that the implications of the changes are described in terms of 'environmental factors' and functioning).

In this case moving forward a decision should be made on whether the threats can be overcome.

### 4.4. Summary

Our research question for this chapter ‘How can the organizational characteristics contribute in determining the potential for IT based control rationalization?’ can now be answered.
Using the organizational configuration approach of Mintzberg in combination with SWOT analyses, a company has a structured approach to define the characteristics of their company. Two out of the three dimensions used to characterize the company: functioning parameters and environmental parameters (external factors) can not, or hardly, be influenced by the organization and therefore are taken into account as preconditions for IT based control rationalization. The third dimension, design parameters can be influenced and therefore changed if required for IT based control rationalization.

As we have noted in the process of rationalization the organization perspective has to be combined with the internal control and IT perspective.
5. **IT Perspective**

In this chapter we will analyze how IT has an influence on IT based control rationalization. With IT we are meaning the organization of IT within a company, how it is organized, managed and controlled. The analyses will lead to key indicators which determine the potential for IT based control rationalization from this perspective. First, we will explain how application controls are related to the IT environment and the general computer controls. Next, we will introduce Cobit as a framework to use for the analysis. We identify key indicators per relevant area of the Cobit framework.

5.1. **Introduction**

In current business environments, the financial reporting processes are often driven by IT systems. Such systems, whether ERP or otherwise, are mostly deeply integrated with initiating, authorizing, recording, processing and reporting of financial transactions. Therefore the IT systems are unavoidable linked to the overall financial reporting process and makes internal control of the IT environment as important as the internal control of the financial reporting.

The PCAOB Auditing Standard No. 2 discusses also the relationship of IT and internal control over financial reporting but also emphasizes the importance of identifying IT controls and testing their design and operational effectiveness. In particular, it states:

"Controls should be tested, including controls over relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include [among others]: Controls, including information technology general controls, on which other controls are dependent" \(^{25}\).

IT systems are automating business processes. In doing so, these systems could also replace manual control activities with automated or IT dependent control activities. With widespread reliance on automated and IT dependent controls, general computer controls are required to support reliable functioning of application controls. The controls commonly include controls over the IT environment, computer operations, access to programs and data, program development, and program changes. For further definitions refer to the Appendix I.

Due to this dependence on general computer controls when using application controls (and thus using IT based control rationalization), we analyze the IT perspective. However it could be that the general computer controls are not the only dependencies in relation to IT based control rationalization. To identify also other dependencies we will use the Cobit framework.

5.2. **Cobit as a starting point**

Our aim is to illustrate all relationships between application controls and IT components which influence the ability of the IT organization to efficiently and effectively support correct functioning of the application controls. This part of the chapter will give an indication of the role of the GCC’s in the control rationalization process.

To do so we will use The Control Objectives for Information and related Technology or in short Cobit which is one of the most well known and used frameworks used by managers to align IT control requirements with the business risks. The IT Governance Institute (ITGI)\(^ {26}\) describes Cobit as a framework and supporting toolset that allow managers to bridge the gap with respect to control requirements, technical issues and business risks and communicate that level of control to stakeholders\(^ {27}\). The Cobit framework supports:

- making a link to the business requirements;
- organizing IT activities into a generally accepted process model;
- identifying the major IT resources to be leveraged;
- defining the management control objectives to be considered.

---


\(^{26}\) ITGI is a research think tank that exists to be the leading reference on IT-enabled business systems governance for the global business community. ITGI aims to benefit enterprises by assisting enterprise leaders in their responsibility to make IT successful in supporting the enterprise’s mission and goals.

\(^{27}\) COBIT 4.0 – IT Governance Institute, page 9
We will use Cobit as follows. The Cobit framework focuses on 5 key areas (refer to figure 10). Per area the framework shows which control objectives are primarily and secondarily linked to this area. The control objectives help an organization to obtain the goals defined for those areas. Furthermore, Cobit makes a distinction between high important, medium important and low important controls. Our analysis links the control objectives per area together with the importance, resulting in the key objectives per area.

To determine what is relevant for IT based control rationalization per area we performed the research with a different focus in comparison to the normal use of Cobit. Below we listed what the 5 areas are about and what focus we will have by analyzing the key objectives.

1. **Strategic alignment** focuses on ensuring the linkage of business and IT plans on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.
   With our focus, we will use this area to identify possible factors which have to do with the alignment between business and IT. The alignment is required for IT based control rationalization as this increases the awareness of both parties of opportunities for automated controls.

2. **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
   This area will be used to identify possible factors in regards to the perceived value within the company of the IT environment and services of the IT organizations. The perceived value could impact the acceptance of an increase of automated controls.

3. **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.
   This area will be used to identify the effectiveness of the IT organizations. Resource management could give insights in the costs of IT and their related automated controls.

4. **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise’s appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.
   Risk management will be used to get an insight how GCC controls and the level of internal control within the IT organization influence the functioning of application controls

5. **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.
   This area will be used to identify the efficiency of the IT organizations. Performance measurement could give insights in the costs and speed of implementation of automated controls.

In the next paragraphs we show the results of our analyses per key area with the focus points described above. This will result in key indicators from an IT perspective for IT based control rationalization.
5.3. **Strategic alignment**

When mapping the Cobit control objectives that are primary and secondary related to the Strategic Alignment focus area, it results in the following table (in order of importance):

<table>
<thead>
<tr>
<th>Cobit process</th>
<th>Control Objective</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary focus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO1</td>
<td>Define a Strategic IT Plan</td>
<td>H</td>
</tr>
<tr>
<td>PO9</td>
<td>Assess and Manage IT Risks</td>
<td>H</td>
</tr>
<tr>
<td>PO10</td>
<td>Manage Projects</td>
<td>H</td>
</tr>
<tr>
<td>ME3</td>
<td>Ensure Regulatory Compliance</td>
<td>H</td>
</tr>
<tr>
<td>ME4</td>
<td>Provide IT Governance</td>
<td>H</td>
</tr>
<tr>
<td>PO6</td>
<td>Communicate Management Aims and Direction</td>
<td>M</td>
</tr>
<tr>
<td>PO8</td>
<td>Manage Quality</td>
<td>M</td>
</tr>
<tr>
<td>AI1</td>
<td>Identify Automated Solutions</td>
<td>M</td>
</tr>
<tr>
<td>AI2</td>
<td>Acquire and Maintain Application Software</td>
<td>M</td>
</tr>
<tr>
<td>DS1</td>
<td>Define and Manage Service Levels</td>
<td>M</td>
</tr>
<tr>
<td>PO2</td>
<td>Define the Information Architecture</td>
<td>L</td>
</tr>
<tr>
<td>PO7</td>
<td>Manage IT Human Resources</td>
<td>L</td>
</tr>
<tr>
<td>Secondary focus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO3</td>
<td>Determine Technological Direction</td>
<td>M</td>
</tr>
<tr>
<td>PO5</td>
<td>Manage the IT Investment</td>
<td>M</td>
</tr>
<tr>
<td>AI7</td>
<td>Install and Accredit Solutions and Changes</td>
<td>M</td>
</tr>
<tr>
<td>DS4</td>
<td>Ensure Continuous Service</td>
<td>M</td>
</tr>
<tr>
<td>PO4</td>
<td>Define the IT Processes, Organization and Relationships</td>
<td>L</td>
</tr>
<tr>
<td>AI4</td>
<td>Enable Operation and Use</td>
<td>L</td>
</tr>
<tr>
<td>DS3</td>
<td>Manage Performance and Capacity</td>
<td>L</td>
</tr>
<tr>
<td>DS7</td>
<td>Educate and Train Users</td>
<td>L</td>
</tr>
<tr>
<td>DS8</td>
<td>Manage Service Desk and Incidents</td>
<td>L</td>
</tr>
</tbody>
</table>

The most important control objectives all relate to strategic and tactical level. Examples are: defining a strategic IT plan, managing projects, defining an information architecture and providing IT governance. The strategic alignment area will be used by us to identify possible factors which have to do with the alignment between business and IT and awareness of both parties to use the systems to increase automated controls.

Looking at the detailed control objectives, we conclude a lot of objectives prescribe alignment between business and the IT organization. The value management objective as part of the strategic plan clearly describes the required alignment: "Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programs that have solid business cases. Recognize that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds... ...Establish fair, transparent, repeatable and comparable evaluation of business cases including financial worth, the risk of not delivering a capability and the risk of not realizing the expected benefits"\(^{28}\). The business alignment is even recognized in a detailed control objective of the strategic plan: "Educate executives on current technology capabilities and future directions, the opportunities that IT provides, and what the business has to do to capitalize on those opportunities. Make sure the business direction to which IT is aligned is understood. The business and IT strategies should be integrated, clearly linking enterprise goals and IT goals and recognizing opportunities as well as current capability limitations, and broadly communicated. Identify where the business (strategy) is critically dependent on IT and mediate between imperatives of the business and the technology, so agreed priorities can be established"\(^{29}\).

Furthermore Cobit prescribes an IT portfolio management which requires the assistance of the business: "Actively manage with the business the portfolio of IT-enabled investment programs required to achieve specific strategic business objectives by identifying, defining, evaluating,

---

\(^{28}\) Cobit 4.0, page 30
\(^{29}\) Cobit 4.0, page 30
prioritizing, selecting, initiating, managing and controlling programs."\textsuperscript{30} Also when the IT organization is responsible for the project management, they should "obtain commitment and participation from the affected stakeholders (including the business) in the definition and execution of the project within the context of the overall IT-enabled investment program"\textsuperscript{31}.

Based on our analysis of the objectives we determined which of these relate to alignment between business and IT. Based on these objectives the following key indicators are extracted from Cobit which are relevant to measure the alignment between business and IT.

<table>
<thead>
<tr>
<th>Key indicators:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A Strategic IT Plan is developed in cooperation with the business, which result in business and IT strategies which are integrated, clearly linking enterprise goals and IT goals and recognizing opportunities as well as current capability limitations.</td>
</tr>
<tr>
<td>2. Awareness and understanding of business and IT objectives and direction are communicated throughout the enterprise.</td>
</tr>
<tr>
<td>3. A quality management system is in place focusing on customers by determining their requirements and aligning them to the IT standards and practices.</td>
</tr>
<tr>
<td>4. IT Projects include a high commitment and participation of the business including the definition, execution and closure of the projects and the overall IT-enabled investment program.</td>
</tr>
<tr>
<td>5. When new applications are required by the business a joint analysis between the IT organization and the business is conducted before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach.</td>
</tr>
<tr>
<td>6. Acquire and maintain application software is done in line with business requirements. This process covers the design of the applications and the proper inclusion of application controls and security requirements which allows organizations to properly support business operations with the correct automated applications.</td>
</tr>
<tr>
<td>7. The IT organization manage IT-enabled investment programs and other IT assets and services to ensure that they deliver the greatest possible value in supporting the enterprise’s strategy and objectives by enforcing a disciplined approach to portfolio, program and project management, insisting that the business takes ownership of all IT-enabled investments and IT ensures optimization of the costs of delivering IT capabilities and services.</td>
</tr>
</tbody>
</table>

### 5.4. Value delivery

The next focus area is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT. We will use this area to analyze which indicators there are in regards to the perceived value of the IT environment and services of the IT organization. Below is a table of all Cobit control objectives which are primary and secondary related to value delivery.

<table>
<thead>
<tr>
<th>Cobit process</th>
<th>Control Objective</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI6</td>
<td>Manage Changes</td>
<td>H</td>
</tr>
<tr>
<td>DS11</td>
<td>Manage Data</td>
<td>H</td>
</tr>
<tr>
<td>ME4</td>
<td>Provide IT Governance</td>
<td>H</td>
</tr>
<tr>
<td>PO5</td>
<td>Manage the IT Investment</td>
<td>M</td>
</tr>
<tr>
<td>AI1</td>
<td>Identify Automated Solutions</td>
<td>M</td>
</tr>
<tr>
<td>AI2c</td>
<td>Acquire and Maintain Application Software</td>
<td>M</td>
</tr>
<tr>
<td>AI7</td>
<td>Install and Accredit Solutions and Changes</td>
<td>M</td>
</tr>
<tr>
<td>DS1</td>
<td>Define and Manage Service Levels</td>
<td>M</td>
</tr>
<tr>
<td>DS4</td>
<td>Ensure Continuous Service</td>
<td>M</td>
</tr>
<tr>
<td>DS9</td>
<td>Manage the Configuration</td>
<td>M</td>
</tr>
<tr>
<td>DS10</td>
<td>Manage Problems</td>
<td>M</td>
</tr>
<tr>
<td>ME2</td>
<td>Monitor and Evaluate Internal Control</td>
<td>M</td>
</tr>
</tbody>
</table>

\textsuperscript{30} Cobit 4.0, page 30  
\textsuperscript{31} Cobit 4.0, page 68, PO10.4
The objectives related to value delivery as listed above are mostly the familiar general computer areas of an IT organization including change management, user management, Incident & problem management, performance management, etc. Most of these areas are normally in scope for Sarbanes Oxley. The value delivery is not only about being in control of the general computer areas, but is more focused on how the business perceive the value of the management of IT processes. In other words: how does the IT organization score on delivering the requested services?

**Illustration of perceived value**

In business, as in life, perception is an important basis for the trust in the IT organization and its services. For example during the month of May, system data availability and network connectivity were maintained at 100%, and the server was down only 4% of that time. IT management might think that they provided pretty respectable service during May, since two out of the three services were 100% available. But the end user who sat strumming his fingers on his desk during those hours probably has a different, and not so favorable, view of IT’s service for May.

Based on the above it is critical to have a measuring instrument for quality which is an end to end process, starting with the end user’s experience and expectations, through all the technology layers and activities, and back to the end user. This is also recognized by Cobit. The quality of IT services can be reflected in the maturity of the IT organization.

Cobit prescribes a maturity model based on the Capability Maturity Model that the Software Engineering Institute defined for the maturity of software development\[32\]. The Cobit maturity model is developed as a method to evaluate management and control over IT processes from a level of non-existent (0) to optimized (5). The levels are described below:

**0 - Non-existent.** Complete lack of any recognizable processes. The enterprise has not even recognized that there is an issue to be addressed.

**1 - Initial.** There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.

**2 - Repeatable.** Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

**3 - Defined.** Procedures have been standardized and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.

---

\[32\] COBIT, page 19
4 - Managed. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 - Optimized. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Per objective Cobit specifies the maturity levels. When selecting the most related objectives for ensuring perceived value at the business site, the following aspects are relevant:

Manage Changes: all changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. This ensures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

The different maturity stages described for the change management start a non occurrence of a controlled process (stage 0) to a recognition of change management and control but execution of changes vary and lack of consistent control and documentation (stage 1). The next stage is a change management process that is driven by intuition, however the fundamentals exist (stage 2). A defined change management process which is mostly followed is next (stage 3). When a well developed change management process is in place which is consistently followed for all changes and works effectively and efficiently an organization is mature (stage 4). The highest stage is a completely optimized change management process which is constantly in line with good practices and business (stage 5). For further details of the maturity stages refer to V.

Manage Data: Data management includes establishing effective procedures and controls to manage media and information resources, backup and recovery of data, and proper disposal of information which ensures the quality, timeliness and availability of business data (which eventually lead to satisfied business owners and high perceived value of the IT services).

The non existent stage applies when the organization do not recognize data as corporate assets. The next stage is applicable when the need for data management is recognized, however performed in an ad-hoc approach (stage 1). In the next stage the awareness of the need for accurate data management exists throughout the organization and on high level data ownership occurs (stage 2). Stage 3 applies when the need for data management within IT and across the organization is understood and accepted. Responsibility for data management is established and controls and procedures for data ownership are assigned to the responsible party who controls integrity and security (stage 3). Next stage is that data ownership and management are clearly defined, assigned and communicated within the organization. Procedures are formalized and widely known, and knowledge is shared (stage 4). When data management performed in a proactive manner and sophisticated tools are used with maximum automation of data management stage 5 applies. More details are included in V.

Provide IT Governance: IT governance is about defining organizational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives which lead to perceived value of the business.

When there is no recognition of the need of IT governance as described above an organization is staged in the lowest level. When IT governance is executed with an ad hoc approach applied on an individual or case-by-case basis on a reactive way (stage 1). When IT processes are identified for improvement based on individuals’ decisions and actions are driven by individuals stage 2 applies. Stage 3 is reached when the importance of and need for IT governance are understood by management and communicated to the organization. IT governance indicators are developed including relationships between outcome measures and performance drivers are defined. Monitoring of processes is not always performed. The next stage includes a full understanding of IT governance.

33 COBIT, page 20
issues at all levels. There is a clear understanding of who the customer is and responsibilities are defined and monitored through service level agreements. Improvement in IT processes is based on a quantitative understanding. IT governance is included in strategic and operational planning (stage 4). The most mature stage is reached when there is advanced and forward-looking understanding of IT governance issues and solutions. Processes have been refined to a level of industry best practice, based on results of continuous improvement and maturity modeling with other organizations. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise (stage 5). \(^{34}\).

Based on the objectives which relates to the perceived value within the company of the IT environment and services of the IT organization in relation to the maturity stages described, we conclude that the following key indicators are relevant.

<table>
<thead>
<tr>
<th>Key indicators:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The maturity level of the change management process based on the measurement aspects described in appendix V is satisfactory for the business owners and meet the expected level.</td>
</tr>
<tr>
<td>2. The maturity level of the manage data process based on the measurement aspects described in appendix V is satisfactory for the business owners and meet the expected level.</td>
</tr>
<tr>
<td>3. The maturity level of IT governance based on the measurement aspects described in appendix V is ensuring that IT performance is measured to ensure meeting business expectations.</td>
</tr>
</tbody>
</table>

5.5. Resource management & Performance measurement

The focus areas Resource management is about proper management of the organizations IT resources including applications, information, infrastructure and people. In regards to optimize automated controls in a control rationalization process proper management of IT which will result in effective use of the IT environment which could be an indication whether the time of implementing application controls and the costs associated with maintaining these controls will be reasonable.

The focus area performance management relates to the efficient use of IT in an organization. When the key objectives of this area are met, the chance is higher that a company has more potential for implementing and managing automated controls efficiently. In the table below the related Cobit controls are listed for both focus areas.

<table>
<thead>
<tr>
<th>Cobit process</th>
<th>Control Objective</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Primary focus</strong></td>
<td></td>
</tr>
<tr>
<td>DS11</td>
<td>Manage Data</td>
<td>H</td>
</tr>
<tr>
<td>ME4</td>
<td>Provide IT Governance</td>
<td>H</td>
</tr>
<tr>
<td>PO3</td>
<td>Determine Technological Direction</td>
<td>M</td>
</tr>
<tr>
<td>A15</td>
<td>Procure IT Resources</td>
<td>M</td>
</tr>
<tr>
<td>DS1</td>
<td>Define and Manage Service Levels</td>
<td>M</td>
</tr>
<tr>
<td>PO2</td>
<td>Define the Information Architecture</td>
<td>L</td>
</tr>
<tr>
<td>PO4</td>
<td>Define the IT Processes, organization and Relationships</td>
<td>L</td>
</tr>
<tr>
<td>PO7</td>
<td>Manage IT Human Resources</td>
<td>L</td>
</tr>
<tr>
<td>A13</td>
<td>Acquire and Maintain Technology Infrastructure</td>
<td>L</td>
</tr>
<tr>
<td>DS3</td>
<td>Manage Performance and Capacity</td>
<td>L</td>
</tr>
<tr>
<td>DS6</td>
<td>Identify and Allocate Costs</td>
<td>L</td>
</tr>
<tr>
<td>DS13</td>
<td>Manage Operations</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td><strong>Secondary focus</strong></td>
<td></td>
</tr>
<tr>
<td>PO1</td>
<td>Define a Strategic IT Plan</td>
<td>H</td>
</tr>
</tbody>
</table>

\(^{34}\) For further details of the maturity stages refer to appendix V.
When analyzing the important control areas of Cobit which primarily and secondary relate to Resource management & Performance measurement we determined that the most important control areas which relate to effectivity and efficiency in regards to managing automated controls will be manage changes (A16) and manage projects (PO10).

Manage changes include controls to effectively implement changes in accordance to business intentions. Examples are: setting up formal change management procedures to handle in a standardized manner all requests for changes to applications, procedures, processes, system and service parameters, and the underlying platforms and ensuring that all requests for change are assessed in a structured way for impacts on the operational system and its functionality. When these controls are in place and work effectively intended changes to automated controls could be (cost) effectively.

Manage projects includes establishing a program and project management framework for the management of all IT projects. Having a proper functioning project management program it ensures that when automated controls are required to be implemented, the right resources are assigned, quality assurance, proper testing and clear definition of deliverables. The program should reduce the risk of unexpected costs and project cancellations, improves involvement of business and end users and ensures the value and quality of project deliverables.

Based on these objectives we determined the following key indicators to effectiveness and efficiency of implementing automated controls.

<table>
<thead>
<tr>
<th>Key indicators:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  The IT organization have an efficient and well controlled change management process</td>
</tr>
<tr>
<td>2  A project program and project management framework for the management of all IT projects.</td>
</tr>
<tr>
<td>3  Project management include quality assurance</td>
</tr>
</tbody>
</table>

### 5.6. Risk management

The focus area Risk management includes risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.

There is a direct relation between how IT risks are addressed and managed with reliable functioning of application controls. Therefore we use this area for determining key indicators how well IT risks are managed. The Cobit objectives which are related to risk management are listed below.

<table>
<thead>
<tr>
<th>Cobit process</th>
<th>Control Objective</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO9</td>
<td>Assess and Manage IT Risks</td>
<td>H</td>
</tr>
<tr>
<td>DS5</td>
<td>Ensure Systems Security</td>
<td>H</td>
</tr>
<tr>
<td>DS11</td>
<td>Manage Data</td>
<td>H</td>
</tr>
</tbody>
</table>
The highly important control objectives which are primarily linked to risk management are related to assessing and manage IT risks, system security, managing data and meeting regulatory compliance. Sarbanes Oxley is one of the important regulations. To show that a company is SOX compliant they have to assess and manage their risks, including areas like logical access security and data management. Therefore we can conclude that Cobit’s key control objectives in relation to risk management are performed by IT management to comply with SOX.

The objective PO9 (Assess and Manage IT Risks) is described as follows: “Create and maintain a risk management framework. The framework documents a common and agreed level of IT risks, mitigation strategies and agreed-upon residual risks. Any potential impact on the goals of the organization caused by an unplanned event should be identified, analyzed and assessed. Risk mitigation strategies should be adopted to minimize residual risk to an accepted level. The result of the assessment should be understandable to the stakeholders, to enable stakeholders to align risk to an acceptable level of tolerance”\(^{35}\)

One of the detailed controls is the integration of the IT governance, risk management and control framework with the organization’s (enterprise’s) risk management framework. This includes alignment with the organization’s risk appetite and risk tolerance level. If a company wants to rely more on automated controls, they have to assess whether the general computer controls in place apply also for the systems in which you want to implement the automated controls.

Based on above, the following key indicators are identified to measure if the IT risks are sufficiently managed and controlled to ensure reliable functioning of automated controls:

<table>
<thead>
<tr>
<th>Key indicators:</th>
</tr>
</thead>
</table>
| 1. For the platforms which are used by the systems which include application controls the General computer Controls do not have deficiencies in the area of:
  - Systems Security
  - Change Management
  - Continuity Management |
| 2. Risk management of the IT environment is integrated with the organizational risk management framework and approach including a process of linking IT risks and controls to business processes. |

\(^{35}\) COBIT 4.0, page 63
5.7. Summary

Based on the five areas of Cobit we analyzed how the important objectives within these areas have an influence on IT based control rationalization with respect to the IT perspective.

Per area we determined the key indicators that give insights in regards to alignment between business and IT, acceptance of business, efficiency and effectivity and risk management. These insights contribute in determining the potential of IT based control rationalization.
6. Conclusion

To reduce the efforts and costs to comply with the Sarbanes Oxley regulation, companies can rationalize their internal control framework to increase the effectiveness of their controls. We defined control rationalization as the continuous process of designing the most effective and efficient controls, to address risks. It includes applying a top-down, risk-based approach, eliminating unnecessary controls, using of risk-based testing plans, optimizing the design of company-level and automated controls, and strategically standardizing and centralizing controls.

IT based control rationalization is about optimizing the role of IT in the internal control framework required to be compliant the Sarbanes Oxley. In other words how can the processes be more effectively controlled by using automated controls instead of manual controls? The arguments for using more automated controls are that they are less vulnerable to error or manipulation or other potential performance problems that are associated with manual controls. Furthermore the costs of automated controls are often less than manual controls as they are often easier to test than manual controls and certain application controls can be benchmarked so that the testing frequency can be rotated over a reasonable period of time.

In this thesis we analyzed how an organization can determine the potential for rationalizing controls based on IT. To do so we analyzed three perspectives: internal control, organization and IT.

6.1. Results of analysis

From an internal control perspective we looked at how organizations use internal control to manage their financial risks in their business processes with the objective to analyze how internal control contribute in determining the potential for IT based control rationalization.

We analyzed the differences of the rule based and risk based approach. As companies initially used a rule based approach to comply with SOX, the new Audit Standard promotes the use of a risk based approach.

The analysis showed that if a company uses a risk based approach it has an influence on the potential for IT based control rationalization. As the risk level of each control objective is clear, companies can focus more on the effective level of control, which means that application controls can get a more important role. E.g. if a process is overly controlled by a manual and application control, one control can be removed. In this case the application control will be preferred to keep because of the advantages with regards to costs and reliability.

Furthermore we concluded that the use of different types of controls and the mitigation of risks using these types of control in a certain sequence also has an influence on the effectiveness of IT based control rationalization. Solely transforming manual controls into automated controls will not lead to the most effective approach, as the risk is there that a company is transforming controls that are redundant or which could be more easily being transformed to another type of control.

The insights of how the organization uses a risk based approach and different types of control contribute in determining the potential for IT based control rationalization.

From an organization perspective we analyzed how the organizational characteristics can contribute in determining the potential for IT based control rationalization. We determined that the use of the organizational configuration approach of Mintzberg in combination with SWOT analyses is a structured method for a company to define the characteristics of their organization.

Two out of the three dimensions used to characterize the company: functioning parameters and environmental parameters (external factors) can not, or hardly, be influenced by the organization and therefore are taken into account as preconditions for IT based control rationalization. The third dimension, design parameters can be influenced and therefore changed if required for IT based control rationalization.

From an IT perspective we analyzed different IT areas by using Cobit with the objective to determine how IT elements contribute in determining the potential for IT based control rationalization. Based on an analysis of the control objectives per key area we concluded which key indicators can be used for determining the potential divided in the following:
Factors which relate to the alignment between business and IT. The alignment is required for IT based control rationalization as this increases the awareness of both parties of the opportunities for automated controls.

Factors with regard to the perceived value within the company of the IT environment and services of the IT organization. The perceived value could impact the acceptance of an increase of automated controls.

The effectiveness of the IT organizations which give insights in the costs of IT and their related automated controls.

The effectiveness of General Computer Controls and automated controls which has an influence on the reliable functioning of application controls.

The efficiency of the performance of IT organizations. Performance measurement could give insights in the costs and speed of implementation of automated controls.

6.2. Focus point model

Based on the analysis of the 3 perspectives, we combined the different focus points which can help companies to determine the potential of IT based control rationalization. By also taking the dependencies between the perspectives into account, a focus point model has been developed (see figure 10).

This model can be used by companies to assess the potential for IT based control rationalization. With this model, all relevant focus points from the three perspectives and their dependencies will be addressed.

The model is a basis for companies to start determining the potential for controls rationalization. It does not mean that if one focus point has a negative impact on IT based control rationalization, there are no opportunities to perform this kind of control rationalization. It is important to analyze the complete picture and judge if there is sufficient potential. For example, the characteristics of company 'A' show enough flexibility to depend more on IT systems and have the ability to manage their business processes with the related IT systems. However the IT organization within company 'A' does not support this dependence as their overall maturity is not meeting the required level. The organization cannot cost-effectively and timely support implementation and maintenance to ensure reliable functioning of automated controls. In this case, the weakness (maturity of IT organization) blocks the transformation to more IT dominant business processes and controls. The company should prioritize helping the IT organization to a mature and cost-effective way of working prior to increase system dependence in the business controls.

This model does not guide a company to exact measurements of the potential. It does serve as a handle for evaluating all focus points and the relations between those focus points. The company should question themselves, based on the focus points, if IT based control rationalization has potential and, if so, which approach is suitable.

Part of the company's evaluation should also be the financial feasibility of IT based control rationalization. In the earlier described example the focus point model taught the company that the IT maturity level needs to increase. However the costs of improving IT maturity could be substantial and eventually could counterbalance the main objective of IT based control rationalization: reduce the compliance costs.
Characteristics of the organization are input for the business and IT objectives. IT Strategic Plan fits with type of organization.

**Explore the Organization perspective**

- **Map and Characterize Organization**
  - Type of organization
  - General structures for organizations
  - Characteristics
  - Three dimensions of Mintzberg

- **Perform Rationalization SWOT Analysis**
  - Strengths & weaknesses of organization in regards to control rationalization
  - Opportunities & threats of organization in regards to control rationalizing

- **Identify focus points**
  - Specify the opportunities of the organization
  - Specify the restrictions of the organization
  - Specify if design parameters require change

**Explore the IT perspective**

- **Business and IT alignment**
  - Strategic IT Plan is developed in cooperation with the business
  - Awareness and understanding of business and IT objectives
  - A quality management system is in place
  - IT Projects include a high commitment and participation of the business
  - A joint analysis between the IT Organization and the business is conducted by new software/applications
  - Acquire and maintain application software is done in line with business requirements.
  - The IT Organization manage IT-enabled investment programmes which add value to the enterprise’s strategy

- **perceived value of IT services**
  - The maturity level of the change management process meets the required level of business owners
  - The maturity level of the management data process meets the required level of business owners
  - The maturity level of IT governance based on the meets the required level of business owners

- **effectiveness/efficiency of automated controls**
  - The IT organisation have an efficient and well controlled change management process
  - A project program and project management framework for the management of all IT projects is used.
  - Project management include quality assurance

- **Effectiveness of GCC and automated controls**
  - For the platforms used by the systems which include application controls the General computer Controls do not have deficiencies in the areas of: Systems Security, Change Management, Continuity Management
  - Risk management of the IT environment is integrated with the Organizational risk management framework
  - A process of linking IT risks and controls to business processes is in place.

**Explore the Internal Control perspective**

- **Perform Risk Assessment**
  - Business Units, accounts and Control Objectives are risk rated

- **Filter Controls**
  - A process is in place to identify the most effective controls

- **Promote Controls to Entity Wide Controls**
  - Entity Wide Controls are fully utilized

- **Leverage Automated Controls**
  - Automated controls are chosen above manual process controls

**IT environment is one of the characteristics in the SWOT analyses**

**IT organization characteristics meets overall organizational characteristics**

**Soil scenario of Internal Control Approach used as benchmark**

**Figure 10: Focus Point Model**

IT Risk Management aligned with Risk management approach

IT org. is involved in leveraging automated controls

Input for risk rating of Business units is the characteristics of organizational perspective

Identified automated controls can rely on controlled IT environment

Application controls can be implemented timely and cost effective
6.3. Reflection

The research performed by us, resulted in a focus point model. We believe this model can really help organizations to determine their potential of rationalizing controls with a prominent role of IT.

During our research we focused on 3 main perspectives: organization, IT and internal control. It could be that other perspectives also need to be taken into account to get a better picture of the potential. However we believe the selected perspectives are the main ones. Furthermore we made assumptions on how to use the Cobit model in relation to IT based control rationalization. We should learn by practice if these assumptions are valid.

The level of importance of the different focus points and their interrelations is not completely answered within this thesis. To further develop the model and the interdependence of all focus points case studies could be performed. This could be part of future research.

We are keen to use this model in the future at our clients and help them to successfully identify opportunities to rationalize controls and increase the importance of automated control activities. By this way we can help them achieving their compliance objectives on a more effective way.
Literature

Books

- PCAOB, Audit Standard 2
- Cobit 4.0 – IT Governance Institute

Articles

- Gartner, ‘Survey on Sarbanes-Oxley Compliance Practises Within IT organizations and Business’, September 14, 2006
- FEI, *Survey on Sarbanes-Oxley Section 404 Implementation*; October 2005
- Deloitte, *Lean and Balanced; how to cut costs without compromising compliance*, 2005
- Melissa Klein Aguilar, Compliance Week; *Optimizing, Rationalizing Internal Controls*;— March 7, 2006
- Financial Executive, L. Ditmar, Governance & Compliance; driving IT priorities, February 2006, page 50

Online Information Resources

Links

- www.pcaob.org  www.sec.gov
- www.itgi.org
- www.coso.org
- www.isaca.org
- www.gartner.com
- wordnet.princeton.edu/perl/webwn
- en.wikipedia.org/wiki/Organization
- sparc.airtime.co.uk/users/wysywig/gloss.htm
- http://www.sarbanes-oxley-forum.com
- www.deloitte.com
### Appendix I: TERMINOLOGY

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes Oxley (SOX)</td>
<td>The Sarbanes-Oxley Act was signed into law on 30th July 2002, and introduced highly significant legislative changes to financial practice and corporate governance regulation. It introduced stringent new rules with the stated objective: &quot;to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws&quot;. (Also known as SOX)</td>
</tr>
<tr>
<td>COSO</td>
<td>COSO refers the Committee of Sponsoring Organizations of the Treadway Commission which provides a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems. It is one of the most widely-accepted internal control frameworks for the audit of internal controls.</td>
</tr>
<tr>
<td>Cobit</td>
<td>The Control Objectives for Information and related Technology (Cobit) is a set of best practices (framework) for information (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992.</td>
</tr>
<tr>
<td>PCAOB</td>
<td>The PCAOB is a regulatory body created by the Sarbanes-Oxley Act of 2002, which regulates audits of SEC registrants. Operating under the US Securities and Exchange Commission, the PCAOB has the authority for registration, inspection, and discipline of firms auditing SEC registrants, and sets standards for public company audits.</td>
</tr>
<tr>
<td>SEC</td>
<td>The federal agency created by the Securities Exchange Act of 1934 to administer that act and the Securities Act of 1933. The statutes administered by the SEC are designed to promote full public disclosure and protect the investing public against fraudulent and manipulative practices in the securities markets.</td>
</tr>
<tr>
<td>General Computer Control (General IT Control)</td>
<td>To support the business processes, IT provides IT services, usually in a shared service to many business processes, as many of the development and operational IT processes are provided to the whole enterprise, and much of the IT infrastructure is provided as a common service (e.g., networks, databases, operating systems and storage). The controls applied to all IT service activities are known as General Computer Controls (also known as General IT Controls).</td>
</tr>
<tr>
<td>IT Organization</td>
<td>The functional groups within an entity, typically reporting to the entity's CIO, that are responsible for designing, implementing, operating, managing and governing the entity's IT environment(s) and information systems.</td>
</tr>
<tr>
<td>Control Activity</td>
<td>Control activities are the policies, procedures and practices that are put into place so that business objectives are achieved and risk mitigation strategies are carried out.</td>
</tr>
<tr>
<td>Automated control (Application control)</td>
<td>Controls that are embedded within software programs to prevent or detect unauthorized transactions. When configured appropriately, or used in combination with other manual controls, application controls support the completeness, accuracy, authorization and existence of processing transactions. (also known as application control)</td>
</tr>
<tr>
<td>IT dependent control</td>
<td>An activity that depends on both manual and automated activities</td>
</tr>
<tr>
<td>Manual Control</td>
<td>Controls performed manually by natural persons, commonly as</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Control</td>
<td>part of a procedure or work instruction, subject to the inherent risk of human error. (Also known as User Control)</td>
</tr>
<tr>
<td>Entity Level Control</td>
<td>Controls that are associated with the control environment, centralized processing, period end financial reporting, and monitoring results of operations. Entity Level Controls may reside at the entity-level and at the process-level and may include all five COSO components. Company Level Controls and Entity Level Controls are synonymous with each other.</td>
</tr>
<tr>
<td>Entity Wide Control</td>
<td>In case a control is applicable for the entire organization and not only a specific part of the organization it is called an Entity Wide Control.</td>
</tr>
<tr>
<td>Process Level Control</td>
<td>Controls that are effective in achieving process-level control objectives are Process Level Controls.</td>
</tr>
</tbody>
</table>
Appendix II: The COSO layers explained

In this appendix we shortly introduce the COSO layers as we will use these in a further explanation of the types of control used to comply with SOX.


- **Control Environment**
  - The Control Environment is the control consciousness of an organization; it is the environment in which people conduct business activities and fulfill their control obligations.
  - An effective control environment exists when employees understand their responsibilities, authority, and are committed to acting ethically.
  - Management influences an organization’s control environment through setting the standard through actions and effectively communicating written polices and procedures, a code of ethics, and standards of conduct – “tone at the top”.
  - The control environment includes both intangible and tangible elements:
    - Integrity and ethical values
    - Commitment to competence
    - Governance and organization structure
    - Management philosophy and operating style
    - Assignment of authority and responsibility
    - Human resource policies and practices
Risk Assessment

- Risk Assessment starts with identifying risks associated with business objectives linked through all levels of the organization.

- Entity-wide
  - The cornerstone for effective control, entity-wide objectives provide guidance on what the entity wishes to achieve
  - Should be consistent with budget, strategic and business plans

- Activity-level
  - Align with entity-wide objectives but differ in that they relate directly to goal setting with specific targets and deadlines
  - Provides guidance for management focus

- Risk assessment requires evaluation of external and internal factors and the impact on operations, financial reporting, and compliance.

Control activities

- Control Activities are policies and procedures that help to ensure that actions identified to manage risks are executed and timely.

- The control activities should be embedded within the operations of the business and used to manage risks to reasonable levels. Focuses on Prevention, Detection, Correction.

- Types of control activities:
  - Approvals, authorizations and verifications (e.g. delegation of authority)
  - Direct functional or activity management (e.g. reconciliations)
  - Review of performance indicators (e.g. KPI’s, metrics)
  - Security of assets (e.g. physical controls)
  - Segregation of duties (e.g. custody - authority - recording)
  - Information systems controls (e.g. security access)
Monitoring

- The purpose of Monitoring is to determine whether internal control is adequately designed, executed, effective and adaptive.

- Internal control performance should be assessed over time through ongoing monitoring of operations and separate periodic evaluations.

- Scope and frequency of monitoring activities depend on significance of risks being controlled and importance of controls in reducing risks.

- Monitoring activities should be built into normal, recurring operating activities of an organization.

- Deficiencies found should have defined escalation path for reporting and follow-up and accountability for corrective action.

Information & Communication

- Information and Communication requires that relevant external and internal information be identified, captured, processed and communicated throughout the organization in a timely manner.

- Provided through various formal and informal means.
  - Verbal communication (e.g. meetings, feedback)
  - Written communication (e.g. policies, procedures, job descriptions)
  - Demonstrated through actions (e.g. management sets example)

- The integrity of information quality is imperative for making business decisions.
  - Requires internal control mechanisms to provide reasonable assurance that information is:
    - appropriate;
    - current;
    - timely;
    - accurate and
    - accessible.
**Appendix III: Structures according to Mintzberg**

* Source: Mintzberg 2001, Page 300, 301
Appendix IV: Dimensions in Structures in Five

In this appendix the dimensions of ‘Structures in Five’ will be illustrated. First of all an overview will be given of all the elements including a short definition. In this overview an impact will be given as well as to what this inclines for organizational change.

Secondly an overview will be given of the five dominant organizational structures as identified by Mintzberg. This overview will include indicators of what the individual elements look like in these organizations.

Elements in the ‘Structures in Five’

<table>
<thead>
<tr>
<th>Primary coordination mechanism</th>
<th>Explanation</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Central part of the organization</td>
<td>Which part of the organization is the central focus point in the process of setting up policies, strategies and taking decisions? This can be any of the five central parts out of which organizations consist in the view of Mintzberg: Strategic Apex (central top), Operating Core (level at which primary processes take place), Middle line (part of the organization in which middle management is located), Technostructure (advisory staff functions in which elements such as R&amp;D are located) and Support Staff (traditional staff functions such as HR, finance etc. etc.)</td>
<td>Gives the first indication of what the driving part of the organization is. When initiating actions within the organization this part is the starting point of the change process.</td>
</tr>
</tbody>
</table>

Design parameters

<table>
<thead>
<tr>
<th>Design parameters</th>
<th>Explanation</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Specialization of tasks</td>
<td>Degree of horizontal (what the employee does for his work) and vertical (how the employee executes his work) specialization.</td>
<td>The design parameters are the only elements which can directly be changed within an organization. They influence other aspects within the organization such as overall coordination and the functioning.</td>
</tr>
<tr>
<td>3 Training and indoctrination</td>
<td>The competency and specialization necessary to have to be able to get into specific functions. Partly determined by Training and indoctrination.</td>
<td>When setting up changes in the design parameters the overall impact should be taken into account.</td>
</tr>
<tr>
<td>4 Formalization of behavior</td>
<td>The extend to which the organization determines employee behavior and their freedom to determine their own actions. There are three basic methods to formalize behavior: by position, by work and by rules.</td>
<td></td>
</tr>
<tr>
<td>5 Grouping of units</td>
<td>The starting point for splitting up working units. This can vary from functional to market oriented.</td>
<td></td>
</tr>
<tr>
<td>6 Unit size</td>
<td>The size of units as in employees and extend of work involved compared to the other units</td>
<td></td>
</tr>
<tr>
<td>7 Planning and Control systems</td>
<td>The goal of planning is to determine, specify and set standards for the desired future output. The goal of control is to determine whether these goals have been reached.</td>
<td></td>
</tr>
<tr>
<td>8 Connections</td>
<td>Means to stimulate contact between individuals. Ordinarily these are part of the formal structure (e.g. meeting agenda, reporting etc. etc.)</td>
<td></td>
</tr>
<tr>
<td>9 Decentralization</td>
<td>The extend of vertical and horizontal decentralization</td>
<td></td>
</tr>
</tbody>
</table>

Functioning

<table>
<thead>
<tr>
<th>Functioning</th>
<th>Explanation</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Strategic apex</td>
<td>Central top</td>
<td>The functioning of the organization provides an insight into the implications of the design parameter settings and the impact of the organizational culture. In itself this can not directly be changed. However, changing the</td>
</tr>
<tr>
<td>11 Operating core</td>
<td>Level at which primary processes take place</td>
<td></td>
</tr>
<tr>
<td>12 Middle line</td>
<td>Part of the organization in which middle management is located</td>
<td></td>
</tr>
<tr>
<td>13 Technostructure</td>
<td>Advisory staff functions in which elements such as R&amp;D are located</td>
<td></td>
</tr>
<tr>
<td>14 Support staff</td>
<td>Traditional staff functions such as HR, finance etc. etc.</td>
<td></td>
</tr>
<tr>
<td>15 Balance of power</td>
<td>How are the five organizational elements balanced? This can be done either via formal rule sets or informally</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>16 Influence regulated system</strong></td>
<td>Are tools and guidelines dominant in the communication between the organizational elements? E.g. is there a central workflow tool which determines the communication or is communication primarily based on the informal chats at the 'coffee machine'? See also 'Importance of informal communication'</td>
<td>design parameters will ultimately impact the way the organization functions.</td>
</tr>
<tr>
<td><strong>17 Importance of informal communication</strong></td>
<td>Next to the regulated system informal communication ad's to the total of internal coordination. This is mainly determined by the culture within organizations.</td>
<td></td>
</tr>
<tr>
<td><strong>18 Workunits</strong></td>
<td>Work units can be the determining factor within organizations. However, alternatively individuals or ad-hoc coalitions can be of influence.</td>
<td></td>
</tr>
<tr>
<td><strong>19 Decision making</strong></td>
<td>'Decision making' relates to way and the lines via which decisions are made. This can be top down or bottom up. In addition decision making can take place following the formal standards or informally</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Environmental parameters</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>20 Age and size</strong></td>
<td>Age and size of the organization are depending on the market and competitors. Age and size determine the extend to which</td>
</tr>
<tr>
<td><strong>21 Technical system</strong></td>
<td>How is the base technical structure within organizations set up? This can vary from a centralized technical system in which a central department is in charge to a situation in which everything, technically and on the point of governance are decentralized completely.</td>
</tr>
<tr>
<td><strong>22 Environment</strong></td>
<td>Is the environment stable or highly competitive? Is innovation of high importance? These are typical questions for the environment aspect.</td>
</tr>
<tr>
<td><strong>23 Power</strong></td>
<td>Power relates to the companies position in relation to the competition. E.g. Microsoft has a powerful position within the system software market because of the dominant use of Microsoft operating systems and the fact that the source codes are not public.</td>
</tr>
</tbody>
</table>
## The five typical organizational structures in detail

<table>
<thead>
<tr>
<th>Design parameters</th>
<th>Simple structure</th>
<th>Machine bureaucracy</th>
<th>Professional bureaucracy</th>
<th>Divisionalized form</th>
<th>Adhocracy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary coordination mechanism</strong></td>
<td>Direct supervision</td>
<td>Standardization of work processes</td>
<td>Standardization of skills</td>
<td>Standardization of outputs</td>
<td>Mutual adjustment</td>
</tr>
<tr>
<td><strong>Central part of the organization</strong></td>
<td>Strategic apex</td>
<td>Technostructure</td>
<td>Operating core</td>
<td>Middle line</td>
<td>Support staff (together with the operating core in the operational adhocracy)</td>
</tr>
<tr>
<td><strong>Design parameters</strong></td>
<td><strong>Specialization of tasks</strong></td>
<td><strong>Training and indoctrination</strong></td>
<td><strong>Formalization of behavior</strong></td>
<td><strong>Grouping of units</strong></td>
<td><strong>Unit size</strong></td>
</tr>
<tr>
<td></td>
<td>Little</td>
<td>Much horizontal and vertical specialization</td>
<td>Much horizontal specialization</td>
<td>Some horizontal and vertical specialization (between divisions and headquarters)</td>
<td>Much horizontal specialization</td>
</tr>
<tr>
<td></td>
<td>Little training and indoctrination</td>
<td>Little training and indoctrination</td>
<td>Much training and indoctrination (by division managers)</td>
<td>Some training and indoctrination</td>
<td>Much training</td>
</tr>
<tr>
<td></td>
<td>Little formalization, organic</td>
<td>Much formalization, bureaucratic</td>
<td>Little formalization, bureaucratic</td>
<td>Much formalization (within divisions), bureaucratic</td>
<td>Little formalization, organic</td>
</tr>
<tr>
<td></td>
<td>Ordinarily functional</td>
<td>Ordinarily functional</td>
<td>Functional and market oriented</td>
<td>Market oriented</td>
<td>Functional and market oriented</td>
</tr>
<tr>
<td></td>
<td>Big</td>
<td>Big at the base, small elsewhere</td>
<td>Big at the base, small elsewhere</td>
<td>Big (at the top)</td>
<td>Small</td>
</tr>
<tr>
<td></td>
<td>Little planning and control</td>
<td>Action planning</td>
<td>Little planning and control</td>
<td>A lot of performance control</td>
<td>Limited performance planning</td>
</tr>
<tr>
<td></td>
<td>Few connections</td>
<td>Few connections</td>
<td>Connections in management</td>
<td>Few connections</td>
<td>Much connections</td>
</tr>
<tr>
<td></td>
<td>Centralized</td>
<td>Limited horizontal decentralization</td>
<td>Horizontal and vertical decentralization</td>
<td>Limited vertical decentralization</td>
<td>Selective decentralization</td>
</tr>
<tr>
<td><strong>Functioning</strong></td>
<td>Strategic apex</td>
<td>All managerial tasks</td>
<td>Fine tuning, co-ordination of function, conflict handling.</td>
<td>Strategic portfolio, performance control</td>
<td>External contacts, conflict handling, work load balancing.</td>
</tr>
<tr>
<td></td>
<td>Operating core</td>
<td>Informal with few authorizations.</td>
<td>Routine, formalized work with few authorizations.</td>
<td>Tendency towards formalization by divisionalizing.</td>
<td>Disconnected or combined with management of informal project work.</td>
</tr>
<tr>
<td></td>
<td>Middle line</td>
<td>Insignificant</td>
<td>Extensive and differentiated.</td>
<td>Formalization of division strategy, management of execution.</td>
<td>Extensive but mixed with support staff, involved in projects.</td>
</tr>
<tr>
<td></td>
<td>Technostructure</td>
<td>None</td>
<td>Extensive with regard to formalization of work.</td>
<td>Little</td>
<td>Extended on headquarters for performance control, Little</td>
</tr>
<tr>
<td></td>
<td>Support staff</td>
<td>Little</td>
<td>Often extensive to decrease uncertainty.</td>
<td>Extensive to support professionals.</td>
<td>Division between headquarters and divisions. Very extensive but mixed with project work.</td>
</tr>
<tr>
<td></td>
<td>Balance of power</td>
<td>Significant from top</td>
<td>Significant throughout</td>
<td>Significant throughout</td>
<td>Insignificant</td>
</tr>
<tr>
<td></td>
<td>Influence regulated system</td>
<td>Insignificant</td>
<td>Significant throughout</td>
<td>Significant throughout</td>
<td>Insignificant</td>
</tr>
<tr>
<td></td>
<td>Important of informal communication</td>
<td>Significant</td>
<td>Insufficient at board level</td>
<td>Some between headquarters and divisions</td>
<td>Significant throughout</td>
</tr>
<tr>
<td></td>
<td>Workunits</td>
<td>None</td>
<td>Insignificant, especially on lower levels</td>
<td>Some at board level</td>
<td>Insignificant</td>
</tr>
<tr>
<td></td>
<td>Decision making</td>
<td>Top-down</td>
<td>Top-down</td>
<td>Bottom-up</td>
<td>Differentiated between headquarters and divisions</td>
</tr>
</tbody>
</table>

### Environmental parameters

| Age and size | Typically young and small | Typically old and big, not advanced. |Varies | Typically old and very big | Typically young |
| Technical system | Simple, not regulating. | Regulating but not automated, not advanced. | Not regulated nor advanced. | Appropriate for division structure otherwise typical machine bureaucracy. | Very advanced, often automated |
| Environment | Simple and dynamic, sometimes hostile. | Simple and stable | Complex and stable | Relatively simple and stable; divers markets (mainly products and services) | Complex and dynamic; sometimes turbulent |
| Power | Power at the executive; often external power, not dependent on trends. | Technocratic and sometimes external power, not dependent on trends. | Power at professional; dependent on trends | Power at middle line; dependent on trends | Power at expert; very dependent on trends. |

*Italic indicates the most important design parameters.*
Appendix V: Maturity Levels according to Cobit 4.0

AI6 Manage Changes 36

Management of the process of Manage changes that satisfies the business requirement for IT of responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework is:

0 Non-existent
When there is no defined change management process and changes can be made with virtually no control. There is no awareness that change can be disruptive for IT and business operations, and no awareness of the benefits of good change management.

1 Initial/Ad Hoc
When it is recognized that changes should be managed and controlled. Practices vary and it is likely that unauthorized changes take place. There is poor or non-existent documentation of change, and configuration documentation is incomplete and unreliable. Errors are likely to occur together with interruptions to the production environment caused by poor change management.

2 Repeatable but Intuitive
When there is an informal change management process in place and most changes follow this approach; however, it is unstructured rudimentary and prone to error. Configuration documentation accuracy is inconsistent and only limited planning and impact assessment takes place prior to a change.

3 Defined Process
When there is a defined formal change management process in place, including categorization, prioritization, emergency procedures, change authorization and release management, and compliance is emerging. Workarounds take place and processes are often bypassed. Errors may still occur and unauthorized changes occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalized, to support planned rollouts of new applications and technologies.

4 Managed and Measurable
When the change management process is well developed and consistently followed for all changes and management is confident that there are minimal exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimize the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked. Configuration documentation is generally accurate. IT change management planning and implementation are becoming more integrated with changes in the business processes, to ensure that training, organizational changes and business continuity issues are addressed. There is increased co-ordination between IT change management and business process redesign. There is a consistent process for monitoring the quality and performance of the change management process.

5 Optimized
When the change management process is regularly reviewed and updated to stay in line with good practices. The review process reflects the outcome of monitoring. Configuration information is computer-based and provides version control. Tracking of changes is sophisticated and includes tools to detect unauthorized and unlicensed software. IT change management is integrated with business change management to ensure that IT is an enabler in increasing productivity and creating new business opportunities for the organization.

DS11 Manage Data 37

Management of the process of Manage data that satisfies the business requirement for IT of optimizing the use of information and ensuring information is available as required is:

36 COBIT 4.0 page 96
37 COBIT 4.0, page 143
When data are not recognized as corporate resources and assets. There is no assigned data ownership or individual accountability for data management. Data quality and security are poor or non-existent.

1 Initial/Ad Hoc
When the organization recognizes a need for accurate data management. There is an ad hoc approach for specifying security requirements for data management, but no formal communications procedures are in place. No specific training on data management takes place. Responsibility for data management is not clear. Backup/restoration procedures and disposal arrangements are in place.

2 Repeatable but Intuitive
When the awareness of the need for accurate data management exists throughout the organization. Data ownership at a high level begins to occur. Security requirements for data management are documented by key individuals. Some monitoring within IT is performed on data management key activities (backup, restoration, and disposal). Responsibilities for data management are informally assigned for key IT staff.

3 Defined Process
When the need for data management within IT and across the organization is understood and accepted. Responsibility for data management is established. Data ownership is assigned to the responsible party who controls integrity and security. Data ownership is assigned, and integrity and security are controlled by the responsible party. Data management procedures are formalized within IT and some tools for backup/restoration and disposal of equipment are used. Some monitoring over data management is in place. Basic performance metrics are defined. Training for data management staff is emerging.

4 Managed and Measurable when
The need for data management is understood and required actions are accepted within the organization. Responsibility for data ownership and management are clearly defined, assigned and communicated within the organization. Procedures are formalized and widely known, and knowledge is shared. Usage of current tools is emerging. Goal and performance indicators are agreed to with customers and monitored through a well-defined process. Formal training for data management staff is in place.

5 Optimized
When the need for data management and the understanding of all required actions is understood and accepted within the organization. Future needs and requirements are explored in a proactive manner. The responsibilities for data ownership and data management are clearly established, widely known across the organization and updated on a timely basis. Procedures are formalized and widely known, and knowledge sharing is standard practice. Sophisticated tools are used with maximum automation of data management. Goal and performance indicators are agreed to with customers, linked to business objectives and consistently monitored using a well-defined process. Opportunities for improvement are constantly explored. Training for data management staff is institutionalized.

**ME4 Provide IT Governance**

Management of the process of Provide IT governance that satisfies the business requirement for IT of integrating IT governance with corporate governance objectives and complying with laws and regulations is:

0 Non-existent
When there is a complete lack of any recognizable IT governance process. The organization has not even recognized that there is an issue to be addressed; hence, there is no communication about the issue.

1 Initial/Ad Hoc
When there is recognition that IT governance issues exist and need to be addressed. There are ad hoc approaches applied on an individual or case-by-case basis. Management’s approach is reactive and there is only sporadic, inconsistent communication on issues and approaches to address them.

---

38 COBIT 4.0, page 170
Management has only an approximate indication of how IT contributes to business performance. Management only reactively responds to an incident that has caused some loss or embarrassment to the organization.

2 Repeatable but Intuitive
When there is awareness of IT governance issues. IT governance activities and performance indicators, which include IT planning, delivery and monitoring processes, are under development. Selected IT processes are identified for improvement based on individuals’ decisions. Management has identified basic IT governance measurements and assessment methods and techniques; however, the process has not been adopted across the organization. Communication on governance standards and responsibilities is left to the individual. Individuals drive the governance processes within various IT projects and processes. The processes, tools and metrics to measure IT governance are limited and may not be used to their full capacity due to a lack of expertise in their functionality.

3 Defined Process
When the importance of and need for IT governance are understood by management and communicated to the organization. A baseline set of IT governance indicators is developed where linkages between outcome measures and performance drivers are defined and documented. Procedures have been standardized and documented. Management has communicated standardized procedures and training is established. Tools have been identified to assist with overseeing IT governance. Dashboards have been defined as part of the IT balanced business scorecard. It is, however, left to the individual to get training, follow the standards and apply them. Processes may be monitored, but deviations, while mostly being acted upon by individual initiative, would unlikely be detected by management.

4 Managed and Measurable
When there is full understanding of IT governance issues at all levels. There is a clear understanding of who the customer is and responsibilities are defined and monitored through service level agreements. Responsibilities are clear and process ownership is established. IT processes and IT governance are aligned with and integrated into the business and the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management has defined tolerances under which processes must operate. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. IT governance has been integrated into strategic and operational planning and monitoring processes. Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprise wide improvements. Overall accountability of key process performance is clear and management is rewarded based on key performance measures.

5 Optimized
When there is advanced and forward-looking understanding of IT governance issues and solutions. Training and communication are supported by leading-edge concepts and techniques. Processes have been refined to a level of industry best practice, based on results of continuous improvement and maturity modeling with other organizations. The implementation of IT policies has led to an organization, people and processes that are quick to adapt and fully support IT governance requirements. All problems and deviations are root cause analyzed and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimized manner to automate the workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organization and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise. IT governance activities are integrated with the enterprise governance process.