An IT control framework for compliance with the Sarbanes-Oxley Act section 409

The impact of the Sarbanes-Oxley Act section 409 on IT control

Master Thesis Informatics & Economics

Poké Chen
December 2005

Faculty of Economics
Erasmus University Rotterdam
The Netherlands

Supervisor:

Dr. ir. Jan van den Berg

Acknowledgement

During the period when I was writing this thesis, it was (probably) the most difficult time of my life. I will never forget this period in my life. The strength of hope gave me the power to finish this thesis. Hope will give people the power to go on with their lives and strive for their goals. I would like to thank Jan van den Berg for his suggestions and guidance. Thanks should also be given to the experts who have been interviewed for this thesis. Finally, I would also like to thank my parents and brother for their support in my life and the possibility to study.

Contents

Chapter 1

Introduction

1.0 Introduction

In this chapter we will discuss the set-up of our research. We begin with an outline of the problem situation. Furthermore we will formulate the objective of our study, the research question, the used methodology and finally the layout of our research.

1.1 Problem situation

The introduction of the Sarbanes-Oxley Act has brought many enforced changes in organizations for which this is applicable. Within this Act, it mainly catches on the changes in the corporate governance. To comply with all the requirements of this Act, there is certainly a support needed from IT related on many areas. Although it is a true fact that the IT control is not much explicitly mentioned in the Sarbanes-Oxley Act, but indirectly this Act has a few essential requirements for IT control.

There are no instruments or best practices adduced within the Sarbanes-Oxley Act to comply with the requirements for IT control. Organizations often have to look elsewhere to find instruments to organize their IT control in order to be compliant with the Act.

Various researchers [Damianides, 2005] [Wyban, 2004] have already look at this problem and there are already a few standards adduced which can be helpful. The standards COSO and COBIT are examples of this. As appears from different researches [Chopskie, 2005] [McNally, 2005] and the business community, the requirements of the Sarbanes-Oxley Act on IT control can be met by existing standards.

From earlier researches [Gouffran, 2005] [Kaarst-Brown, 2005] it is appeared that the sections 302, 404 and 409 of the Sarbanes-Oxley Act have a direct impact on the IT control of an organization. Section 302 demands that the financial reporting of the organization must be reliable. For section 404, it requires a good internal control within the organization. It can be mentioned that a lot of literature has been written about these two sections. Furthermore,

there are also enough standards, which can be used for the compliance with the sections 302 and 404 [McCollum, 2004].

At this moment there are still not much literature written about section 409, which demands on real-time information, which has material changes in the financial condition or operations of the organization. The section 409 has probably a deeper impact on the organization than the sections 302 and 404. Before the introduction of the Sarbanes-Oxley Act, the requirements of sections 302 and 404 were already obliged; organizations had to carry for the reliability of their financial reporting and to guarantee the internal controls. By the introduction of the Sarbanes-Oxley Act, organizations have to prove that they are compliance with the requirements of the Act.

Section 409 of the Act contains requirements, which can be new for some organizations [Hofmann, 2003] [Kral, 2004]. The supply of real-time information can be a problem for many companies. Real-time information requires, for example, that the IT infrastructure of the organization has to be well organized. Hereby we can conclude that section 409 definitely has requirements for IT control. People often think that these requirements are for the IT area but there are also requirements for the organizational area. By using nowadays systems, organizations can possibly deliver real-time information. However to supply real-time information organizations have to use the systems on a certain way, whereby correct procedures are needed. This is where the organizational aspect comes from. It is interesting to do a research on what the impact the section 409 has on the IT control, whereby the organizational aspect also has an important influence.

With this thesis, I want to describe the impact of section 409 of the Sarbanes-Oxley Act on the IT control. After the impact of section 409 is described, it will be obvious which requirements this section demands on the IT control of an organization. Furthermore, we will look into the standards, which can be used for the compliance with these requirements. We will use these standards to develop a framework for the compliance with new requirements of section 409. This framework consists of IT controls on strategic and tactical level. The requirements and framework will be tested by interviewing with experts. The results will be discussed and as last, the conclusions of the research will be followed.

1.2 Research objective

The research objective is to describe the impact of section 409 of the Sarbanes-Oxley Act on IT control and to develop a framework on strategic and tactical level that is useful for the compliance with the new requirements of the section 409.

1.3 Research question

The research question can be defined as follows:

“Which requirements does the section 409 of the Sarbanes-Oxley Act have on IT control and how organizations can meet the new requirements on strategic and tactical level?”

In order to be able to give an answer to the research question, it will be founded by the following sub questions:

1. What is the Sarbanes-Oxley Act and what is the goal of this Act?
    a. What is the meaning of the Sarbanes-Oxley Act?
    b. What is the impact of the Sarbanes-Oxley Act on corporate governance of the organization?

2. What is the impact of section 409 of the Sarbanes-Oxley Act as a consequence of this on IT control?
    a. What are the requirements of the Sarbanes-Oxley on IT control?
    b. What are the requirements of section 409 on IT control?
    c. Which information has to be available according to section 409 and within which term must this information be available?

3. How will the framework be developed?
    a. Which useful standards can be used for the framework?

4. How can we meet the new requirements of section 409 on IT control?
    a. What are strategic and tactical levels?
    b. How will the framework look like?

5. What are the requirements of section 409 on IT control and how effective is the framework in practice?
    a. Which requirements does the section 409 have on IT control according to experts and how do experts think about of this framework?
    b. How can the framework be supplemented?

1.4 Methodology

Trough a literature study, better know as the secondary data, we will make an inventory of what the Sarbanes-Oxley Act is and what the goal of this Act is and what the impact of section 409 of the Sarbanes-Oxley Act on IT control is, the sub questions 1a up to and including 2c will be hereby answered.

Also via a literature study, we will investigate which standards can be used for the framework for compliance with the new requirements of section 409. Further, the framework will be developed with relevant parts of the standards on strategic and tactical level, whereby an answer will be given on the sub questions 3a up to and including 4b.

By having interviews, better know as the primary data, with experts we will make an inventory of how effective the framework is in practice. The requirements of section 409 on IT control will also be tested by these interviews. We will also look how completely the framework is for the compliance with section 409 of the Sarbanes-Oxley Act. The framework could possibly be supplemented with recommendations of the experts. Hereby the sub questions 5a and 5b will be answered. We would like to present the structure of this thesis in the following figure.

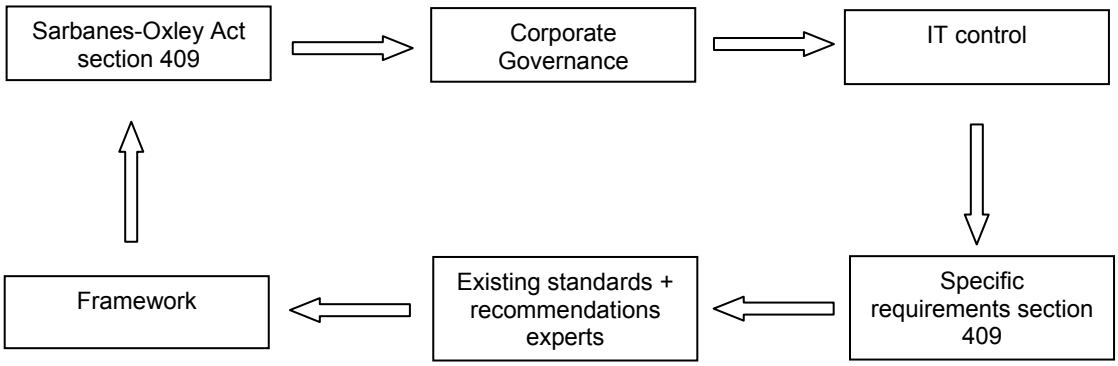


Figure 1: Thesis structure

1.5 Research layout

To keep the whole structure clear each sub question(s) will be divided in separate chapters. Furthermore each chapter starts with an introduction in which the research will be explained. Besides that, each sub question(s) will be followed by a conclusion.

This results in the following chapter layout:

Chapter 1: Introduction

Chapter 2: The Sarbanes-Oxley Act *(sub questions 1a and 1b)*

Chapter 3: Impact of section 409 *(sub questions 2a, 2b and 2c)*

Chapter 4: Standards *(sub questions 3a)*

Chapter 5: Theoretical framework *(sub questions 4a and 4b)*

Chapter 6: Test *(sub questions 5a + 5b)*

Chapter 7: Conclusions and further research

Chapter 2

The Sarbanes-Oxley Act

2.0 Introduction

In this chapter an introduction of the Sarbanes-Oxley Act will be given. We will see how the Act is developed and what it is all about. Since the Act is about better corporate governance the impact of the Sarbanes-Oxley Act on the corporate governance will be discussed afterwards.

2.1 The Sarbanes-Oxley Act

In this paragraph we will give some general information about the Sarbanes-Oxley Act [SEC, 2002]. To understand the Sarbanes-Oxley Act completely there is insight needed into the motive of the framing of this Act. This will be given in the first subparagraph. In the following subparagraphs we will look to the goal of the Sarbanes-Oxley Act. After that, the content of the Sarbanes-Oxley Act will be shortly given. Then we will see to whom the Act is relevant and it will be clear that the Sarbanes-Oxley Act is a specific reaction of the scandal of Enron.

2.1.1 The inducement of the Sarbanes-Oxley Act

One of the most direct inducements for the introduction of the Sarbanes-Oxley Act is the Enron scandal. At the end of the year 2001, Enron stunned Wall Street by announcing that it had a $ 618 million net loss for the third quarter and would reduce shareholder equity by $ 1.2 billion. The financial situation of Enron was not as propitious as represented to the investors. Enron has committed a financial accounting fraud, fictitious profits were reported and losses at subsidiary companies were not reported on time. There were also practices like off-balance sheet financing, which have been used by Enron, and not everything was reported in the bookkeeping [Brickey, 2003].

At the beginning, it was widely assumed that the Enron scandal was an anomaly. But soon it became clear that this was anything but an isolated case of financial accounting fraud at a major corporation. Enron's was the largest bankruptcy in American financial history. Since

Enron it has been soon eclipsed by WorldCom, who's less sophisticated accounting fraud led to a larger restatement of earnings, a larger bankruptcy filing, and equally far-reaching civil and criminal investigations. Federal and state regulators have since initiated fraud investigations involving dozens of corporations, including Adelphia, Health South, McKesson, Tyco, and Qwest [Brickey, 2003].

All these scandals have heavily affected the trust of the investors in issues like financial statements, integrity of corporate managers and accountants. The lack of trust of investors is definitely not positive for the political economy and the American government did a research to find a way to rectify this trust [Brickey, 2003].

2.1.2 The goal of the Sarbanes-Oxley Act

To rectify the trust of the investors, people looked at the causes of the scandals. The roots of the problem included: [Tavis, 2003]

- The lack of independence of auditors providing higher margin consulting services to audit;
- Either a lack of understanding or independence by corporate directors (or both);
- The fact that GAAP (Generally Accepted Accounting Principles) reporting has not kept pace with increasingly complex financial strategies used by corporations, such as asset securitization or other off balance sheet financing arrangements and derivative-oriented risk management techniques. For example, under the current system derivatives with the same economic exposure may be accounted for differently;
- Excessive use of stock options as a form of management compensation. The pay-off for option holders and equity holders is not the same. Option holders have unlimited upside potential if stock prices rise, but have very limited downside risk. Their "free" options simply expire worthless. This rewards unwarranted risk taking and discourages dividend payments. Further, if the options are issued "out of the money" they do not have to be treated as expenses on the income statement;
- Investor and sell side analyst emphasis on beating short-term earnings expectations which led to considerable pressure on managers to manipulate earnings, in some cases committing outright fraud. Many firms present investors with pro forma "Operating Earnings" (referred by cynics as "earnings before bad stuff").

The American government found out that rules were necessary for the independence of managers and auditors. As a consequence the American Congress has introduced the Sarbanes-Oxley Act 2002, which is designed by the congressmen Paul Sarbanes and

Michael Oxley, in an incredibly short period of time (6 weeks to be precisely) [Herwaarden, 2003]. On 30 July 2002 the President Bush has signed the Sarbanes-Oxley Act into law, "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws" [NetSec, 2004].

The goals of the Sarbanes-Oxley Act are to improve the financial overview, to make the auditor more independent, to demand more of transparency of corporate financial issues, to prevent conflict of interest by analysts and require a more comprehensive responsibility of the corporate officials. By the introduction of the Sarbanes-Oxley Act people have more possibilities to prosecute fraud and give higher punishments [Brickey, 2003].

2.1.3 Content of the Act

A lot of the causes which were mentioned in the previous paragraph are related with the so-called "corporate governance problem". The Sarbanes-Oxley Act tries by using rules, which will force a better corporate governance, to have the interests of the investors at heart. This way people will rectify hopes that the integrity at companies will be guaranteed and the trust of the investors.

The Act consists eleven titles. Each title contains one to nine sections. The titles and sections of the Act are different in interest and the impact on organizations for which they are relevance. The next sections are often seen as the most important parts of the Sarbanes-Oxley Act: [NetSec, 2004]

- Makes the CEO and CFO explicitly responsible for the integrity of the financial reports (see section 302, Appendix A);
- Establishing, evaluating and monitoring the effectiveness of internal control over financial reporting for a correct and transparency of the information (see section 404, Appendix A); [ISACA, 2005] [NetSec, 2004]
- The obligations of almost real-time delivery of important information (see section 409, Appendix A);
- To set up the Public Company Accounting Oversight Board (PCAOB) for control of the auditors and the possibilities for accountancy companies to substantially enclose the non-audit work [Travis, 2003].

2.1.4 Relevance of the Act

The Sarbanes-Oxley Act compliance is controlled and enforced by the U.S. Securities and Exchange Commission (SEC). As part of the Act, the Public Company Accounting Oversight Board was created to oversee public company auditors in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audits. In everyday terms, the PCAOB provides more specific guidelines for compliance with the Sarbanes-Oxley Act as well as regulate the previously unregulated accounting firms. According to many people in the industry, this was long overdue [NetSec, 2004].

All publicly traded corporations that fall under the jurisdiction of the SEC are subject to Sarbanes-Oxley Act requirements. Those are the firms which are quoted at the Stock Exchange of America. However, private firms interested in going public, or those that may be the target of acquisition or merger by a public firm will also implicitly fall under the Sarbanes-Oxley Act mandate. They need to prepare themselves to be compliant with the Act. Besides recently many other countries have developed their own version of the Sarbanes-Oxley Act [NetSec, 2004].

2.1.5 The Sarbanes-Oxley Act as a specific reaction on Enron

However people agreed that actions must been taken to prevent other accounting scandals there were also much criticism of the Sarbanes-Oxley Act which was signed in 2002. If people read the Sarbanes-Oxley Act well then it is clear that the Act is written as a reaction of the failure of Enron. Some of the Act's provisions are clearly helpful, while some are overly Enron-specific and could be expected to have only modest impact (like the prohibition of insider trades during pension blackouts). There are also important areas where it is silent, most notably with respect to the expensing of stock options [Travis, 2003].

The Sarbanes-Oxley Act was enacted in a flurry of congressional activity in the run-up to the midterm congressional election campaigns, after the spectacular failures of once highly regarded firms (e. g. Enron). As a consequence of this the Sarbanes-Oxley Act can be seen as a special emergency legislation before the midterm congressional election campaigns. By that, a few measures are inadequately worked-out. As a result some goals of the Sarbanes-Oxley Act are not good feasible [Romano, 2004].

Probably political issues had influence on the Act. Many of the substantive corporate governance provisions in the Sarbanes-Oxley Act are not in fact regulatory innovations devised by Congress to cope with deficiencies in the business environment in which Enron

failed. Rather corporate governance entrepreneurs may more accurately characterize them as recycled ideas advocated for quite some time. There are also measures in the Act whereof before was clear that by taking these measures hardly having any or none results [Romano, 2004].

The goal of this thesis is not to give an opinion about the quality and effectiveness of the Sarbanes-Oxley Act. For the research we use the unabridged Sarbanes-Oxley Act, which is signed by President George W. Bush in 2002.

2.2 Impact of Sarbanes-Oxley Act on corporate governance

Now it is clear what the inducement and the goal of the Sarbanes-Oxley Act is and for which organizations the Act is relevant. In this paragraph the impact of the Act on corporate governance of organizations will be discussed. To determine this it is necessary to get a clear understanding of what corporate governance is.

2.2.1 Corporate governance

In subparagraph 2.1.3 is written that many of the cases, which probably had important influences on the accounting scandals, had a link with the so-called "corporate governance problem". A corporate governance problem in an organization occurs when the situation is satisfied with two conditions. Firstly, there must be an agency problem in the organization. Secondly, the transaction costs are so high that this problem cannot be solved by contracts. An agency problem occurs when there is a conflict of interest between the participants in the organization. The participants could be owners, managers, workers and consumers, better known as stakeholders [Hart, 1995].

In practice only the conflict between the owners and the management of the organization will be inspected. This occurs when an investor wants the organization managed in a different way. This means that the investor is not satisfied about how the current manager runs the organization. When the property is spread in the organization and the owners have a conflict in interests then the problem will been strengthened. This will hamper the formation of a common front of owners opposite to the management [Becht, 2003].

To determine the impact of the Sarbanes-Oxley Act on corporate governance, we use the definition of corporate governance mentioned below, which is formulated by "Commissie Peters" in 1997: [Commissie Corporate Governance, 1997]

"Corporate governance is a system of manners for the partnership and direct interested parties involved with the firm – particularly directors, commissioners and capital procurer – containing a few rules for good management and good control and rules for the division of tasks, responsibility and authorities which achieve an balanced influence between the involved parties of the firm."

2.2.2 The Sarbanes-Oxley Act and corporate governance

The Sarbanes-Oxley Act focuses mainly on the interests of the investors (or owners) from the stated above definition. The American government wants to achieve better corporate governance by executing the measures of the Act and to prevent other (huge) accounting scandals. The Act is introduced in 2002 and has changed on a few points in the way to handle with corporate governance in practice.

2.2.2.1 The role of gatekeepers in corporate governance

In the first place the auditors, lawyers and analysts are active by corporate governance and the direct concerned parties mentioned by the definition. Mitchell [2003] called these three parties the gatekeepers of the corporate systems, because they have the task to protect the gates, which are designed by legislation and financial systems to keep the organizations fair. The tradition role of the gatekeepers was to evaluate the organizations from outside and their speciality.

Auditors and lawyers of the organizations receive a financial compensation for their duties and analysts can get benefits by manipulating news service, this happens for example when they want to keep the organizations satisfied, which provide valuable not-public information. A danger can occur when the gatekeepers in the first place not handle in advantage of the public interests. Of course every gatekeeper must comply with the legislation of his speciality, but the extent in which this legislation is to join the public and personal interests varies. Especially by the accountants, an occupational group that was self-regulating for a great part before the Act, there was the danger that they will be affect by the pressure of (paying) clients [Mitchell, 2003].

2.2.2.2 Rules amplified and drowned up by law

This brings us by the second important consequence of the Sarbanes-Oxley Act, namely the rules must be complied by the gatekeepers and concerned parties is now drowned up by the law. Besides, the Act forms an important supplement on those rules.

By binding the functions of the gatekeepers direct with the traditional corporate governance concept, the Act forces organizations to see these gatekeepers as an essential part of the corporate governance process. In the coming subparagraph this will be explained and the influence of the Act on an (other) important player in the corporate governance process will be given; the management of an organization.

A. Auditors

By obliging of an audit committee (title 2) for every organization the Act involves the auditor by the corporate governance of the organization. The audit committee has to monitor the independently of the auditor, to avoid conflicts in interests and to introduce Corporate Responsibility for financial reports (title 3), by which the auditor is bind with internal business of the organizations.

The Sarbanes-Oxley Act strengthens the relation between the auditor and the organization. The Act requires that there must be at least one independent financial expert in the audit committee. This expert is responsible for the financial matters of the organizations and will work closely with the accountants. Since the identity of this expert is public the investors can though speak to financial experts on the financial reports. This will motivate the financial expert to give faithful financial reports. The assistance of the auditor is hereby very useful [Mitchell, 2003].

Besides the Act demands that the auditors may not do non-audit services, which auditors execute for the organizations. In section 201 of the Sarbanes-Oxley Act a list of non-audits are given which may not be done by "registered public accounting firm" if they also execute the audit for the organization [Romano, 2004].

The Sarbanes-Oxley Act also demands a few new things on the internal control. The managers (see D. Managers) will clarify these demands. In section 404 of the Act is written that as well as both the management and the accountant must research objectively if the entire internal financial control has functioned appropriate. Before the introduction of the Act this research was not obligated and the auditor and the client were free to do the research subjectively [Renes, 2004].

B. Lawyers

The next category of gatekeeper brought by the Act within the corporate governance system is the lawyer, and the Act potentially changes the lawyer's role radically. The Sarbanes-Oxley Act makes the lawyer, in a meaningful way, a coordinate constituent of the corporate governance process. Section 307 of the Act requires the Commission to issue rules setting forth the duties of lawyers in this regard, and the rules that it contemplates will create a whistle blowing role for lawyers or, to put the matter perhaps a bit more modestly, a monitoring role for lawyers that requires them to police corporate misconduct. This provision does so by requiring lawyers to report various kinds of malfeasance to the corporation's general counsel or CEO and, failing satisfactory action by the reporter; lawyers must report this evidence to the audit committee of the board or an independent board.

As a consequence of this measure people can expect a reserved ness of the lawyers if they have to give advice in situations when organizations possible have handled illegal. By the Act the lawyers have to adopt a critical attitude [Mitchell, 2003].

C. Analysts

Now we come to a group that has traditionally been completely beyond the Pale of corporate governance - securities analysts. Analysts have an important role by making the markets efficiently. Ideally is the information, which is given by the analysts, complete and reliable so that the investors only have to do little or none research at all. This makes the investors possible to keep a varied effect portfolio. In practice the markets are not very efficiently, because investors can not rely on the reliability of the information which is provided by the analysts.

The Sarbanes-Oxley Act can, mainly by title 5, play an important role to improve the objectivity of analysts and the efficiency of the markets. For example the Act demands that there must be rules to protect the analysts against of reprisals the employers as a consequence of the analyst's pronunciation. On the other side this title obliges that the analysts must report the possibility of conflict of interest, for example when they have a share in firms about which they do pronunciation. Besides, the Act tries to improve the quality of the analyses by giving penalties to the analysts who did not do a solid research in concerned organizations [Mitchell, 2003].

D. Managers

According to Mitchell [2003], the focus on the short term is the most important cause of the accounting scandals in 2002. The investment strategies were especially based on analyses by the prices of stocks instead of a solid research in the real value of the firm. He also state that the focus on the short term is very destructive for investments, because the managers will be tempt to manage on short term by which accounting profits is central. A consequence of this, the long term objectives, which are focused on enlarging the value of the firm, will be in danger.

The Sarbanes-Oxley Act does not direct meet the above problem, but there are regulations for this in section 401, which induce managers to focus on the long term. The Act demands that every year or quarter report must add a report of transactions, which are not mentioned in de bookkeeping, and relations with non-consolidated firms that have potentially have a material issue. Hereby the emphasize lays on financial transactions which are not mentioned in the bookkeeping, because the lack of information about this played an important role in the Enron scandal. The CEO and CFO must guarantee for this explanation.

Besides, the Act attaches great value to the conception cash flow. Compared to the bookkeeping profit conceptions, is cash flow namely much less sensitive for fraud. Finally the cash flow determines the value of a share because cash flow represents money, which the investors will receive their investments. All these rules carry for the potential focus on short term will be hampered and that the focus on long term will be certified by the CEO and CFO. This will be represented to the shareholders [Mitchell, 2003].

In section 402 is written that the organization is forbidden to provide loan to a manager or top executive with the intention for their private use and the loan is not offered against conform the market conditions [Kintraco, 2004].

Since the reliability of financial reports is dependent for a great part of the internal control, should this have enough attention from the concerned managers (especially CEO and CFO). For this reason the Sarbanes-Oxley Act demands explicitly that the management is responsible for the internal control. As a consequence of section 302 of the Act the financial year and quarter reports must have signed explanation from the CEO and CFO for correctness of the information and the internal control of the systems, which produce this information (it was used to be "trust me" and know it has to be "prove me") [Instituut der bedrijfsrevisoren, 2005]. With this, the CEO and CFO are responsible for the reliability and effectiveness of the internal controls. This has leaded to the fact that the CEO and CFO have a personal interest in correct internal controls.

Section 404 requires that the internal control report must be a part of the year report. The management of a firm must explain that the internal control is correctly designed and implemented. The internal financial control also must have functioned accurate [Renes, 2004]. Besides, the report must have a review of the effectiveness of the internal control and processes [Kaarst-Brown, 2005].

The fact that the management is responsible for the internal control will lead to the main point of the corporate governance and will move from the board of directors to a lower level, namely the managers of the organization [Mitchell, 2003].

2.2.3 Evaluation of the whole Act

In previous subparagraph the Sarbanes-Oxley Act is viewed from the perspective of corporate governance. Hereby we discussed a great part of the titles of the Act. The titles 2, 3 (especially sections 302 en 307), 4 (especially sections 401, 402 and 404) and 5 are discussed. The most important titles of the Act are hereby mentioned. For the completeness we will handle the other titles short and discuss their impact on the corporate governance.

Title 1: PCAOB

In paragraph 2.2.2.2 is mentioned that the auditors must be independent and that the non-audit work must be enclosed. The control on the auditors is done by the PCAOB. The exact role and tasks are defined in this title. This title supports the requirements from title 2.

Title 6: Commission Resources and Authority

This title is about the role of SEC and has no impact on the corporate governance.

Title 7: Studies and Reports

In this title a few areas are mentioned upon which further research will be done to prevent accounting scandals and other fraud in the future. This Title has also no direct impact on corporate governance.

Title 8: Corporate and Criminal Fraud Accountability

The demands of this title are that it is forbidden to change, delete or create a document that could hamper a research in the future by the government. Important audit documents must be kept for minimal 5 years. This title also requires that the so-called whistle-blowers must

be protected. There are even punishments for securities-fraud. This title is practical basic important for audit ability, which will not directly improve corporate governance. A few instruments are giving to assail the offenders.

Title 9: White-collar Crime Penalty Enhancements

Punishments are mentioned in this title for committing fraud, like "mail and wire fraud" and pension fraud. Furthermore the CEO and CFO are obliged to give an explanation in the periodical financial statements about the financial condition of the organization are coped with law. It is punishable when the CEO and CFO give a wrong explanation. This is a supplement of section 302 and it is clear that this will strengthen the effect of this section on corporate governance.

Title 10: Corporate Tax Returns

The CEO must sign the corporate tax return. This is specific working out of the responsibility, which is defined in title 3.

Title 11: Corporate Fraud and Accountability

In this title the punishments are described for messing up with the files and documents and reprisals against informants. These measures has an indirect effect on the protecting of the integrity and available of information. This has also an indirect effect on corporate governance. The U. S. Sentencing Commission has the mandate to judge and fit the measures for certain offences. The SEC has the authority to freeze extraordinary compensations provided by organizations during a research. As a consequence of this title the Commission has the right to forbid persons to have the function of officer or director if they are not suited for these functions. From the corporate governance point of view this will probably lead to a better management.

2.3 Conclusion

In this chapter are the Sarbanes-Oxley Act and its influence on the corporate governance described. This chapter has given an answer to the following research questions:

- What is the meaning of the Sarbanes-Oxley Act?
- What is the impact of the Sarbanes-Oxley Act on corporate governance of the organization?

We have seen that Sarbanes-Oxley Act is arising from several accounting scandals. The Sarbanes-Oxley Act is draft to get the trust back by the investors after these accounting scandals. With this Act the American government wants to realise a better and more transparent financial reports, independently auditors and analysts and corporate directors who are personally responsible. We can conclude that the Sarbanes-Oxley Act tries to achieve better corporate governance. The Sarbanes-Oxley Act also wants that it must be demonstrable that the internal control measures are effective (from "trust me" to "prove me").

The Sarbanes-Oxley Act can been seen as a mechanism to bring the interests of the owners and management together. For this purpose the Act involved the accountants, lawyers, advisers (the so-called gatekeepers) active with the corporate governance process. By the introduction of the Sarbanes-Oxley Act are the rules, which must be compliant by the parties who are involved with this process, extended and determined by law. This has several consequences for the organizations. The main goal of the Act is to deliver reliable financial information by organizations.

Chapter 3

Impact of section 409

3.0 Introduction

In the previous chapter it is described what the Sarbanes-Oxley Act is and that the Sarbanes-Oxley Act is about better corporate governance. This has subsequently influence on the IT control. In this chapter we will discuss the demands of the Act on IT control. We will see that a few sections of the Act have direct influence on IT. These are the sections 302, 404 and 409. The content of these sections and the requirements of section 409 will be given.

3.1 Demands from Sarbanes-Oxley Act on IT control

Until so far we know what Sarbanes-Oxley Act is and what the impact of this Act on corporate governance of an organization is. To comply with the requirements of the Act is the support of IT on many areas necessary. The IT control is not explicitly mentioned in the Sarbanes-Oxley Act, but indirectly the Act demands a few essential requirements on the IT control. IT is necessary and very handy for compliance with requirements of the Act for better corporate governance. The Act provides almost only requirements from the corporate governance and let the implementation, herewith is the IT almost involved, of it to the concerned organization.

Therefore we will now look to which requirements the Sarbanes-Oxley Act demands from the IT control of organizations. The term "IT control" will be first defined, after that we will look to the direct influence of the Sarbanes-Oxley Act on IT control.

3.1.1 IT control

The supply of information supports an organization with the realisation of their goals. By using information technology it gives an organization the possibility to produce products more efficiently, effectively, and be innovative and to control the processes better. The IT

function in the organization gets more interest from the management. The expectations of the organization about the quality of the supply of information, functionality, user-friendliness and speed of the delivery of new systems are strongly increased. Beside the questions of the speed of changes of information and communication technology and the speed of changes of the structures of organizations ask an adequate control of the IT risks. The great dependently of the information systems for critical business processes ask IT control processes that are conscientiously attuned to the organization.

IT is becoming a more integral part of the strategy of an organization. The quality of the automated supply of information is a critical success factor for supporting and realisation of the internal control of business processes and giving external accountability about it. IT control goes about manage, control, executing, give accountability and the control on the supply of information within an organization [De Kennisgroep IT-Governance, 2004]. It concerns the following points:

- Decision-making and internal responsibility about IT;
- Corporate standards concerning IT;
- Manifestation of the IT organization;
- The IT processes;
- The IT changing projects;
- The IT infrastructure which is used by the systems.

3.1.2 Direct influence on IT

The supply of information plays an important role by the introduction of the Sarbanes-Oxley Act. The goal of this Act is to create transparency and reliability. The Act carries for the reliability of financial information. This information is composed from information systems within organizations. Hereby is a good organization of the supply of information important.

The Sarbanes-Oxley Act has three sections, which have direct influence on the IT of an organization. These three sections are: 302, 404 and 409. By regulation of these three sections there is no longer IT isolation of the board of directors (CEO and CFO). By taking the CEO, CFO, accounting management and internal and external auditors in the information chain, the Sarbanes-Oxley Act has a much more influence on IT within organizations. In the end the Act carries for the binding of IT Islands. This has a great consequence for the culture of organizations [Gouffran, 2005]. The content of these sections will be shortly discussed on the next page [Kaarst-Brown, 2005]. In Appendix A is the full content of these sections given.

Section 302, "Corporate Responsibility for financial reports"

As already mentioned before, section 302 demands that the board of directors are responsible for the financial reports. The board of directors must sign the financial information for the organization. This must be done for all the financial reports, as well as both quarter and annual reports. The CEO and CFO (or equivalents) are responsible for the regularity and accuracy of the elements in the financial reports, continual controls and communication with the auditors and the audit committee.

Section 404, "Management Assessment of internal controls"

Section 404 provides that the managing director must do the judgment of internal controls. The members of the board of directors are responsible for the set up and maintenance of the procedures for internal controls. Besides, the managing directors are obliged to deliver an icr (internal control report) yearly.

The internal control report contains information about the condition of the responsibility of the management for the settlement and maintenance of an adequate internal control structure and procedures for financial reports. The internal control report also contains information about the judgement of the management of the effectiveness of the internal control structure and procedures for financial controls. The intention of this section is to prevent fraud and to prove that there is an adequate control.

Section 409, "Real Time Issuer Disclosures"

Section 409 demands real-time supplying of information. A firm must almost supply real-time information (within 48 hours) to the shareholders or other interested parties, when this (changed) information has material influence on the financial performances and specifically the determination of the value of the organization.

3.2 Section 409

Section 409 of the Sarbanes-Oxley Act and guidance subsequently issued by the SEC require companies to report information about material changes in operations and financial position within 48 hours. The goal of this section is to protect investors from delayed reporting of material events and as a consequence the increasing of their losses. As with the executive's accountability for internal controls, the responsibility to comply with this section cannot be transferred to third parties. This can occur in situation when they outsource their

IT systems. The executives are still personally and legally responsible for this. In this thesis we will not take the situation of outsourcing into count.

While a compliance deadline for this section has not been set yet, many sources [Boccasam, 2005] [Zimmermann, 2005] suggest that this section might require information technology efforts on the magnitude of the Y2K projects of a few years back. It is thought that most companies would have difficulty complying with this section with their in-house systems. Section 409 consists of only two paragraphs but has potential ramifications that go far beyond sections 302 and 404 [Cannon, 2005].

Section 409 requires that the information that has to be reported to the interested parties must be on "rapid and current basis" and "in plain English". To comply with this, organizations could use trend and qualitative information and graphic presentation. This makes the information even better understandable for the interested parties.

3.2.1 Meaning of "material"

The ambiguity of the Act is a complicated factor. It is for example unclear what the legislator exactly means with "material", while this is important in accounting and auditing. There are a few examples of material events that could possibly be put under section 409, but it is desirable that the legislator gives more guidelines for this. When the deadline for section 409 is approaching it is necessary that the legislator gives more precisely information about which events fall under material events.

It is clear that material events could be internal as well as external. An example of internal material event is cost overruns on IT projects or other major capital expenditures. An example of a material event that may fall under the external material event is the loss of a major sales' contract to a competitor [Hoffman, 2003]. We see that material event is about serious great changes in the financial condition and operations of the organizations. In some situation material events will be determined by the accountant. They have the knowledge of which events will have great affect on the financial condition or operations of the organization. In this thesis we will only look to the information that will cause great changes in the financial condition or operations of the organization.

3.2.2 Definition of "information"

The definitions “data” and “information” are frequently used as a synonym for each other. Between the two definitions there is definitely a difference. The definitions and the difference of these two are given below [Overbeek, 2000] [The Telecom Glossary 2000].

The definition of “data”: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.

The definition of “information”: The meaning that a human assigns to data by means of the known conventions used in their representation.

We can conclude that information is subjective. Dependent on the person who has worked up or interpret the data, different information can be arisen from these data. The value of this information can thereby be varied in time. The relation between data and information can be compared to the relation between a raw material and a final product. Data can be worked up into information.

3.2.3 Requirements of section 409

The IT infrastructure of the organization must be in the condition to deliver financial reports within 48 hours. This means that organizations must know if the most important financial systems are in the condition to supply information on the right moment. If it is necessary the organization has to fit the existing systems or scrap the existing systems and buy special software. This can require changes to business process and the implementation of new systems [Chan, 2004]. The time-sensitive aspect of this regulation will likely put significant pressure on existing data infrastructures, requiring deeper system integration and more intelligent analytics tools. IT systems, as they support business operations and financial management, play a significant role in the detection and management of material events. Proactive use of IT, and tools like analysis methods, enables earlier detection and mitigation of material events [Damianides, 2004].

Section 409 is possibly the heaviest requirement of the Sarbanes-Oxley Act on IT. The requirement of real-time supply of information may imply that many organizations have to drastically change their IT infrastructure on short term. This will be a difficult task for organizations if they use batch processing of information. Many organizations utilize multiple legacy systems that are clumsily interfaced to each other. Many of these systems utilize batch processing and operate on different systems. A batch system that is designed to

operate on a weekly transaction cycle is not much help in the face of a 2-day reporting requirement. In fact, it is not unusual for the legacy systems of an organization to be in sync with each other only at the monthly period end. This situation can exist where information systems are wholly in-house. Often this is for some firms impossible to process all the information real-time. Add to this to comply with the other sections of the Sarbanes-Oxley Act it is already taking up a great deal of time. Further it is costly, so that there is less time and money left for the compliance with section 409 [Cannon, 2005] [Hoffman, 2003].

Looking at the reliability of real-time supply of information it is important that the internal control of the organization is in proper order. Good control of operational processes is necessary herewith. Security measures are an important part of the internal control, under which are also included back-ups. The requirements, which are demand from the security of the IT infrastructure, are dependent of the desirable security level and the vulnerability of the IT infrastructure (or parts from it) to specific threats. People can comply with the security requirements by using a set of security measures. Because the real-time information often is aggregated with high speed and descend from different locations in the organizations, these measures must have a large range. In the end the information must be aggregated in such a way that everybody receive the information on time and can judge the accurateness of the information [Wyban, 2004]. The integrity of the real-time information must be guaranteed and besides it must be possible to judge this information afterwards. In the first place only authorised persons may look to this information so that the information is confidential. This all implies that information must be: [www.wikipedia.org]

- *Confidentiality (C)*: ensuring that information is accessible only to those authorized to have access;
- *Integrity (I)*: comprises the personal inner sense of "wholeness" deriving from honesty and consistent uprightness of character;
- *Availability (A)*: the degree to which a system, subsystem, or equipment is operable and in a committable state at the start of a mission, when the mission is called for at an unknown, i.e., a random, time;
- *Accountability*: constrains the extent to which elected representatives and other office-holders can wilfully deviate from their theoretical responsibilities.

The aspects C, I and A combined represents the reliability of the information [Overbeek, 2000]. To keep the real-time information reliable, it is important that the internal control of the organization is accurate as well. The financial reporting processes are nowadays heavenly dependent on IT systems. These financial reporting processes are also linked with other (important) supporting processes. The financial processes and these linked supporting processes must be in control. If it comes to section 409 then it is obvious that the controls of

IT processes must be well organized. This thesis will only take the requirement of effective IT processes of internal control into count. For complying with effective internal control totally people can look to section 404. Section 404 of the Sarbanes-Oxley Act requires that the internal control must be well organized. Organizations, which already comply with section 404, are also compliance with a part of section 409. This part is the requirement of good internal control of operational processes. Besides, in practice section 404 goes together with section 302, because these two sections have a relation with each other. This is not where this thesis is focusing on and will not be discussed. In Appendix A more information can be found about sections 302 and 404.

We see that important information has to be available internal within time, but this information must also be communicated to the interested parties, like the investors. Thereby the Internet can play an important role. It takes for example a short time to deliver information via a website and interested parties can get the information easily and directly [Wyban, 2004].

If we now make a link between the requirements that are given, we can conclude that there are four subjects, which are important for the compliance with section 409. These four subjects are:

- *Application controls*: information must be protected so that it is accurate all the times and available;
- *Processes*: within the organization the IT processes must be correct, efficient and effective to deliver the information on time. Hereby must be focused on the business processes;
- *IT infrastructure*: IT infrastructure must be well organized to deliver the information on time;
- *Systems*: IT systems (including batch-processing systems) have to be integrated so that the information can be easily and quickly produced. These systems must also have the possibility to deliver the information on time.

Actually the requirement “systems” belongs to the requirement “IT infrastructure”. We have split it from this requirement because the framework which will be presented in chapter 5 will not have IT controls for the requirement “systems”. This will be explained in chapter 5. The requirements, which are discussed up here, are for the summary put in the table on the next page. The first row is the subject of the IT control mentioned and the second row are the requirements of it described.

Subject	*Requirements*
Application controls	*To protect the information.*
Processes	*Ensuring correct, efficient and effective IT processes for the delivery of information.*
IT infrastructure	*In condition to deliver information within 48 hours.*
Systems	*Integrated and in condition to produce information within 48 hours.*

Table 1: Requirements of section 409 on IT control

3.3 Conclusion

We have seen what the impact is of section 409 of the Sarbanes-Oxley Act on IT control. An answer has been given to the following research questions:

- What are the requirements of the Sarbanes-Oxley Act on IT control?
- What are the requirements of section 409 on IT control?
- Which information has to be available according to section 409 and within which term must this information be available?

IT is an essential factor upon which the Act has an impact. There are a few sections from the Sarbanes-Oxley Act that have influence on IT control within an organization. The sections that have direct influences on IT are 302, 404 and 409. A short content of these sections are given in this chapter. An explanation of section 409 is given and also the essential requirements of section 409 on IT control are described and presented in a table. The requirements of section 409 of the Sarbanes-Oxley Act on IT control are: “application controls”, “processes”, “IT infrastructure” and “systems”. We have seen that (changed) information, which has a material influence on the financial performances and the determination of the specific value of the organization, has to be supplied within 48 hours. Material can be internal as well as external.

Chapter 4

Standards

4.0 Introduction

In this chapter we will discuss several existing standards, which we can use for setting up a framework for compliance with section 409. First the standards will be given, followed by a comparison between the standards.

4.1 Standards

The standards COBIT, ITIL and ISO 17799 will be described in this paragraph. We have chosen for these three standards because they are frequently used for managing issues related to IT control in practice. A short introduction and the content will be given of these standards. The PCAOB has recommended organizations to use the internal control framework COSO for complying with the Sarbanes-Oxley Act. Therefore the standard COSO will be first described. This standard will not be used for the framework for compliance with section 409, because COSO does not define IT controls specifically.

4.1.1 COSO

COSO (The COSO Committee of Sponsoring Organizations of the Treadway Commission) was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. An independent private sector initiative studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. This model has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control. The COSO framework contains a structured and comprehensive set of instructions for framing and implementing of internal controls.

The COSO model defines internal control as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance of the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting;
- Compliance with applicable laws and regulations.”

The first category addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs.

While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time. Internal control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. Although the components apply to all entities, small and mid-size companies may implement them differently than large ones. Its controls may be less formal and less structured, yet a small company can still have effective internal control. In an “effective” internal control system, the following five components work to support the achievement of an entity’s mission, strategies and related business objectives.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of

relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Information and Communication

Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

Monitoring

Internal control systems need to be monitored, a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

The above can be presented in a cube. The cube that is given below is the well-know COSO cube.

Figure 2: COSO cube

There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. These components work to establish the foundation for sound internal control within the company through directed leadership, shared values and a culture that emphasizes accountability for control. The various risks facing the company are identified and assessed routinely at all levels and within all functions in the organization. Control activities and other mechanisms are proactively designed to address and mitigate the significant risks. Information critical to identifying risks and meeting business objectives is communicated through established channels up, down and across the company. The entire system of internal control is monitored continuously and problems are addressed timely [COSO, 1992] [Protiviti, 2005].

4.1.2 COBIT

The Control Objectives for Information and related Technology (COBIT) is a framework for information (IT) management risks created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI). It was developed by the ITGI and the Information Systems Audit and Control Foundation (ISACF) in 1992 when the control objectives relevant to information technology were first identified. Control Objectives for Information and related Technology provides managers, auditors, and IT users with a set of

generally accepted information technology control objectives to assist them in maximizing the benefits derived through the use of information technology and developing the appropriate IT governance and control in a company. COBIT has 34 high level objectives that cover 318 control objectives categorized in four domains.

The COBIT mission is “to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors”. Managers, auditors, and users benefit from the development of COBIT because it helps them understand their IT systems and decide about the level of security and control that is necessary to protect their companies’ assets through the development of an IT governance model.

COBIT provides benefits to managers, IT users, and auditors. Managers benefit from COBIT because it provides them with a foundation upon which IT related decisions and investments can be based. Decision making is more effective because COBIT aids management in defining a strategic IT plan, defining the information architecture, acquiring the necessary IT hardware and software to execute an IT strategy, ensuring continuous service, and monitoring the performance of the IT system. IT users benefit from COBIT because of the assurance provided to them if the applications that aid in the gathering, processing, and reporting of information complies with COBIT since it implies controls and security are in place to govern the processes. COBIT benefits auditors because it helps them identify IT control issues within a company’s IT infrastructure. It also helps them corroborate their audit findings. COBIT covers the following domains.

Planning and Organization

The Planning and Organization domain covers the use of technology and how it can be best used in a company to help achieve the company’s goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT.

Acquisition and Implementation

The Acquisition and Implementation domain addresses the company’s strategy in identifying its IT requirements, acquiring the technology, and implementing it within the company’s current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components.

Delivery and Support

The Delivery and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as, the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training.

Monitoring

The Monitoring domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors.

By each of the 34 IT processes COBIT has a few management instruments to execute these processes. A few of these are:

- Control objectives for each IT process. Each of the 34 processes has a few, total 318, detailed control objectives;
- Compare the Key Goal Indicators (KGIs), the norms, with Key Performance Indicators (KPIs), the results. A list of Critical Success Factors (CSFs) for each IT process;
- Maturity levels model for comparing and supporting of decision making of capacity improvements;
- Audit guidelines, like guidelines for interviews, information and tests that can be taken.

To realise the goals of the organization the information for steering the organization and business processes must be compliant with the seven quality criteria: effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability. The IT governance model is focused on the realisation of the goals of the organization with the contribution of the supported IT processes. In Appendix B is a figure presented which gives insight in the mutual relationship between the organization goals and the supply of information from COBIT domains and the associated IT processes, quality criteria and IT resources [Capgemini, 2005] [ITGI 1, 2000] [Wikipedia 1, 2005].

4.1.3 ITIL

The recommendations of ITIL were developed in the late 1980's by the Central Computer and Telecommunications Agency (CCTA), which merged into the OGC in April, 2001 and disappeared as a distinct organization. The CCTA created ITIL in response to the growing dependence on information technology to meet business needs and goals.

The Information Technology Infrastructure Library (ITIL) is a customizable standard of best practices that promote quality-computing services in the information technology sector. ITIL addresses the organizational structure and skill requirements for an IT organization by presenting a comprehensive set of management procedures with which an organization can manage its IT operations. These procedures are supplier independent and apply to all aspects of IT infrastructure; ITIL provides the basis for improvement of the use and effect of an operationally deployed IT infrastructure and service management. ITIL is the de-facto global standard in the area of service management. The introduction of service management makes it necessary to focus less on functions and components and more on an approach guided by the business process. The service management is concerned with delivering and supporting IT services that are appropriate to the business requirements of the organizations. In many enterprises, this requires a cultural change. This important point must always be taken into account when implementing service management.

ITIL is defined by a collection of books that describe guidelines for different aspects of best-practice data center management. Taken as a whole, ITIL presents a comprehensive view of the field. The subjects of the individual books are referred to as sets; currently there are eight. The sets are further divided into disciplines, each of which is focused on a specific subject. The service management set is the main discipline of ITIL which is split into two sections, service support and service delivery. The service support discipline ensures that the customer has access to the appropriate services to support the business functions. This section consists of the following processes:

Service Desk

The service desk is the central point of contact between the customer and the IT area in all matters concerning IT services. This includes help desk functions as well as coordination of change requests, service level management, configuration management and all other service management processes of ITIL. The service desk is not a process but a function within the service organization. In its special role as a first point of contact with the customer, the service desk is of great importance, all the more so since it embodies the image and the quality of service of the IT organization.

Configuration Management

Configuration Management is a process that tracks all of the individual Configuration Items (CI) in a system. The CIs show the interconnection of the individual elements in the IT infrastructure. A system may be as simple as a single server, or as complex as the entire IT department. The objective of configuration management is to provide up-to-date secure information via the configuration elements in use, thus ensuring direct interlinking with all other disciplines of IT service management.

Incident Management

The first goal of the incident management process is to restore a normal service operation as quickly as possible and minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA).

Problem Management

The goal of Problem management is to minimize the adverse impact of Incidents and Problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. A `Problem' is an unknown underlying cause of one or more incidents, and a `Known error' is a problem that is successfully diagnosed and for which a Work-around has been identified.

Release Management

Release Management is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper software and hardware control ensure the availability of licensed, tested, and version certified software and hardware, which will function correctly and respectively with the available hardware. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management. This guarantees that all software can be conceptually optimized to meet the demands of the business processes.

Change Management

The goal of the change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize

the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organization.

The second section service delivery looks at what service the business requires of the provider in order to provide adequate support to the business users. This section has the following processes:

Service Level Management

Service Level Management provides for continual identification, monitoring and review of the levels of IT services specified in the Service Level Agreements (SLAs). The process involves assessing the impact of change upon service quality and SLAs. The service level management process is in close relation with the operational processes to control their activities.

Financial Management

Financial management is responsible for the identification, calculation, monitoring and onward allocation of costs for the customer's contracted IT services. Financial management provides the basis for information on economical control, finance planning and cost accounting.

Capacity Management

Capacity Management supports the optimum and cost effective provision of IT services by helping organizations match their IT resources to the business demands. Capacity management ensures that the resources necessary to meet the agreed customer requirements are provided economically.

Availability Management

Availability Management allows organizations to sustain the IT service availability in order to support the business at a justifiable cost. Using availability management, ensure the availability of IT services as specified by the customer.

IT Continuity Management

The objective of IT continuity management is to safeguard the performance of services in any eventuality based on planning and implementation of preventive measures. IT Continuity

Management helps to ensure the availability and rapid restoration of IT services in the event of a disaster.

Security Management

The goal of security management is to protect the data and infrastructures. Security is a moving target and almost invariably difficult to plan and calculate because changes often originate from the outside in particular when understanding a necessary technical innovation. However, the integrity as well as protection of customer and business data and of IT resources is crucial to the very survival of an enterprise. Corporate management must therefore determine and document the security policy of the enterprise or the business sectors to be secured, set objectives and specify commitments for IT security.

According to Overbeek [2000] the service support discipline is at operational level, so this discipline will not be used for the framework. Another set of ITIL; the business perspective can be used for the framework for compliance with section 409. The business perspective covers a range of issues concerned with understanding and improving IT service provision, as a part of the entire business requirement for high IS quality management. These issues are:

- *Business Continuity Management:* describes the responsibilities and opportunities available to the business manager to improve what is, in most organizations one of the key contributing services to business efficiency and effectiveness;
- *Surviving Change*: IT infrastructure changes can impact the manner in which business is conducted or the continuity of business operations. It is important that business managers take notice of these changes and ensure that steps are taken to safeguard the business from adverse side effects:
- *Transformation of business practice through radical change*: helps to control IT and to integrate it with the business;
- *Partnerships and outsourcing*: helps to handle the partnerships with other parties and outsourcing of IT (parts).

The ICT Infrastructure Management set of ITIL can also be helpful for the framework for compliance with section 409. ICT infrastructure management is concerned with the flow of work from the definition of the business requirements through to the deployment and delivery of the final ICT business solutions. The ICT infrastructure management processes proceed along the following lifecycle:

- *Design and planning*: providing overall guidelines for the development and installation of an ICT infrastructure management structure that satisfies the needs of all aspects of the business;
- *Deployment*: implementation and rolling out of the ICT infrastructure management as designed and planned;
- *Operations*: daily housekeeping and maintenance of the ICT infrastructure management structure;
- *Technical support*: structuring and underpinning other processes to guarantee the services delivered by ICT infrastructure management.

In Appendix C the relationships between the above sections and processes are presented in a figure. In this Appendix, the standard of ITIL is also presented in a figure with all sections [ITIL 1, 2000] [ITIL 2, 2001] [ITIL 3, 2004] [ITIL 4, 2001] [The Information Management Company, 2005] [Wikipedia 2, 2005] [www.itil.org].

4.1.4 ISO 17799

In 1995 the British Standards Institution developed British Standard BS 7799, which should provide recommendations on how to design an Information Security Management System (ISMS). The success of this standard was great so it is now internationally accepted and published as ISO 17799.

ISO 17799 is an information security standard published in December 2000 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) in 2000 entitled Information technology - Code of practice for information security management. ISO 17799 provides best practice recommendations on information security management for the use by those who are responsible for initiating, implementing or maintaining information security management systems.

ISO 17799 is high level, broad in scope, and conceptual in nature. This approach allows it to be applied across multiple types of enterprises and applications. It has also made the standard controversial among those who believe standards should be more precise. In spite of this controversy, ISO 17799 is the only “standard” that devoted information security management in a field that generally governed by “Guidelines” and “Best Practices.”

ISO 17799 contains ten main sections. Within each section, information security control objectives (in total 36) are specified and a range of controls (in total 127) are outlined which are generally regarded as best practice means of achieving those objectives. Specific controls are not mandated since each organization is expected to undertake a structured

information security risk assessment process. It has to determine its requirements before selecting controls that are appropriate to its particular circumstances. Further it is practically impossible to list all conceivable controls in a general purpose standard. The ten sections are:

Security Policy

The objectives of this section are to provide management direction and support for information security.

Security Organization

The organization of security means principles and procedures to manage information security. These also include security of third party access and outsourced information processing.

Asset Classification and Control

The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

Personnel Security

It is the objective of personnel security to reduce the risks of human error, theft, fraud or misuse of facilities.

Physical and environmental security

Secure areas prevent unauthorised access, damage, and interference to business premises and protect against loss, damage, compromise of assets and interruption to business activities.

Communications and Operations Management

The objectives of this section are: to ensure the correct and secure operation of information processing facilities; to minimize the risk of systems failures; to protect the integrity of software and information; to maintain the integrity and availability of information processing and communication; to ensure the safeguarding of information in networks and the protection of the supporting infrastructure; to prevent damage to assets and interruptions to business

activities; to prevent loss, modification or misuse of information exchanged between organizations.

Access Control

Access control determines access to information systems. Unauthorised user access, computer access, access to information shall be prevented Network services shall be protected. Further some focus is put on mobile computing and teleworking.

Systems Development and Maintenance

The objectives of this section are: to ensure security is built into operational systems; to prevent loss, modification or misuse of user data in application systems; to protect the confidentiality, authenticity and integrity of information; to ensure IT projects and support activities are conducted in a secure manner; to maintain the security of application system software and data.

Business Continuity Management

The objectives of this section are to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

Compliance with Legal Requirements

The objectives of this section are: to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements; to ensure compliance of systems with organizational security policies and standards; to maximize the effectiveness of and to minimize interference to/from the system audit process [Carlson, 2001] [ISO 17799, 2000] [Wikipedia 3, 2005].

4.2 Comparison between the standards

If we look to the standards, which are described in the previous paragraph, we can conclude that there is a link between those standards. It is described before that the Sarbanes-Oxley Act wants to achieve better corporate governance within organizations. By using an effective internal control organizations can realise better corporate governance. The COSO framework is the framework that is frequently used for internal control. Hence the PCAOB has recommend organizations to use the COSO framework to comply with the requirements of the Sarbanes-Oxley Act.

COSO does not focus deeply on IT control. Therefore the COBIT framework was developed. COBIT is often seen as the IT variant of COSO. The COSO framework will not be used for the framework for compliance with section 409. For complying with the requirements on IT control, it is recommended to use the COBIT framework. By using the COBIT framework organizations can realise the effective of IT governance.

Look at the concept of a control framework; a framework is a collection of controls to highlight what needs to be done at various levels of the organizations. It is an outline that tells “what” but not “how”, because that level of detail is something what has to be filled in. Each organization differs from each other and so are their controls. For example, all the groups need to change the management but how it is implemented will depend on the enterprise. The point is that organizations will need to tune their policies, procedures and work instructions. Not only do they need to meet the spirit of the controls but they also need to be feasible in the context of their organization.

COBIT is an overall control framework for IT and the standards ITIL and ISO 17799 are best practices. It is obvious that the COBIT framework does not contain detailed tasks and instructions about what to do. This is precisely where ITIL and ISO 17799 come into play. They can fill in the blanks about how to structure processes. The COBIT framework contains almost IT control objectives and the standards ITIL and ISO 17799 contain IT control measures. The standards ITIL and ISO 17799 can be seen as complementary for the COBIT framework. In the table below are the strong and weak points mentioned for each standard. For each standard it is also described when it can be used.

Standard	*Strong*	***Weak***	***Use***
COBIT	*Provides IT controls and IT metrics.*	*Does not define how and not strong in security.*	*To be used as the delivery mechanism, where it describes what.*
ITIL	*Provides IT processes.*	*Not strong in security and system development.*	*To be used as the delivery mechanism, where is describes how.*
ISO 17799	*Provides security controls.*	*Does not define how.*	*To be used for improve security processes and controls.*

Table 2: Comparison between the standards

We see that the standards do not compete to each other and there is not really overlapping. In fact they are mutually complementary. The following tables contain references to a high level mapping of which processes, as defined in COBIT as high level control objectives, are addressed by the respective standard. The legend of the tables is represented next to these tables [ITGI 2, 2004] [Overbeek, 2000] [Spafford, 2004] [Wallhoff, 2005].

COBIT Processes Addressed*

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	+	+	+	+	+	+	+	+	+	+	+	\	\
AI	+	+	+	+	+	+	\	\	\	\	\	\	\
DS	+	+	+	+	+	+	+	+	+	+	+	+	+
M	+	+	+	+	\	\	\	\	\	\	\	\	\

(+) Addressed
(-) Not or rarely addressed

Table 3: Mapping between COBIT and COBIT

COBIT Processes Addressed

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	-	+	+	+	-	-	-	-	+	-	\	\
AI	+	+	+	+	+	+	\	\	\	\	\	\	\
DS	+	+	+	+	+	+	-	+	+	+	+	+	+
M	-	-	-	-	\	\	\	\	\	\	\	\	\

(+) Addressed
(-) Not or rarely addressed

Table 4: Mapping between COBIT and ITIL

COBIT Processes Addressed

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	+	+	+	-	+	+	+	+	-	-	\	\
AI	-	+	+	+	+	+	\	\	\	\	\	\	\
DS	-	+	+	+	+	-	+	+	+	+	+	+	+
M	+	+	-	-	\	\	\	\	\	\	\	\	\

(+) Addressed
(-) Not or rarely addressed

Table 5: Mapping between COBIT and ISO 17799

*Note: this chart are not a comparison, this is COBIT itself.

The framework for compliance with section 409 at strategic level will be based on the elements, the IT controls, from the standards that are useful for the framework. By looking to the requirements and the associated IT controls, we will look to standard COBIT first, because COBIT contains high level IT control objectives. These are at strategic level. If an IT control of COBIT can be complemented by an IT control of ITIL or ISO 17799 then this IT control of ITIL or ISO 17799 will be used, this will be at tactical level. This IT control of ITIL or ISO 17799 is usually a specific IT control. This IT control will be mapped to the IT control of the COBIT framework [ITGI 2, 2004] [ITGI 4, 2005] [Overbeek, 2000].

4.3 Conclusion

With describing of the useful standards COBIT, ITIL and ISO 17799, an answer has been given to the following research question:

- Which useful standards can be used for the framework?

COSO is recommended by the PCAOB for the use as the internal control framework for complying with the Sarbanes-Oxley Act. This framework does not define IT controls. COBIT is an overall control framework for IT. It describes what must be done on the field of IT control. COBIT describes this on a high level and describes not how to meet these IT control objectives. The standards ITIL and ISO 17799 can be used for filling up the blanks about how to meet the IT control objectives. ITIL contains measures to structure IT processes and ISO 17799 contains measures to organize security. ITIL and ISO 17799 can be seen as a complementary for the COBIT framework. The framework for compliance with section 409 at strategic level will be structured by relevant IT controls of COBIT and where it is necessary it will be complemented by IT controls of ITIL and ISO 17799 at tactical level.

Chapter 5

Theoretical framework

5.0 Introduction

The standards are described in the previous chapter. Now we can set up the IT control framework for complying with section 409 of the Sarbanes-Oxley Act. First we will give more information about the specific requirements of section 409; the framework will consist only IT controls for new specific requirements of section 409. After the new specific requirements are described the framework will be presented. Because the framework contains IT controls of COBIT, ITIL and ISO 17799 at strategic and tactical level, the definition of the strategic and tactical level will be described.

5.1 Specific requirements of section 409

In paragraph 3.2.3 the requirements of section 409 of the Sarbanes-Oxley Act are summed up. If we look closer to these requirements we can make a difference between the requirements.

Section 409 of the Act does not only contain new requirements but also requirements that already existed before the introduction of the Sarbanes-Oxley Act. So the requirement “application controls” is already an important topic in the information security field. Measures like "user registration" and "user identification and authentication" are always needed and thus are not new. The requirement "systems" sounds like as a new requirement. However in the world of today there are very well build software systems like ERP (Enterprise resource planning) systems. These ERP systems have integrated modules. All the modules in an ERP suite have a common set of data that is stored in a central database. With these modules an organization can easily combine the business processes together in the system. Many organizations are using these ERP systems [Janstal, 1999].

It is notable that the requirements “processes” and “IT architecture” are not really mentioned as important requirements before the introduction of the Sarbanes-Oxley Act. Well organised of business processes will lead to better IT processes, this is a part of internal control. To

deliver real-time information the IT processes must be effective; otherwise it is impossible to deliver real-time information. Another necessary issue is the IT architecture. The IT architecture must be structured in a way that the information can be delivered on time.

The IT control framework will be based on the requirements of “processes” and “IT architecture”, because these two really require new demands. We will look to what is needed to have good processes and an IT infrastructure.

5.2 Strategic and tactical levels

The framework consist IT controls that are at strategic level. This implies that these controls are strategic controls. These controls focus on the planning, organizing and directing processes that contribute to the achievement of the long-term mission and goals of the organization. The framework also consist IT controls, which are at tactical level, these controls will be placed under the strategic level. Tactical controls focus on the planning, organizing and directing processes that contribute to the achievement of the short-term objectives and organization the activities that will lead to successful achieving of the strategic mission and goals. The strategic and tactical level is presented in a figure down here [Overbeek, 2000] [www.wikipedia.org].

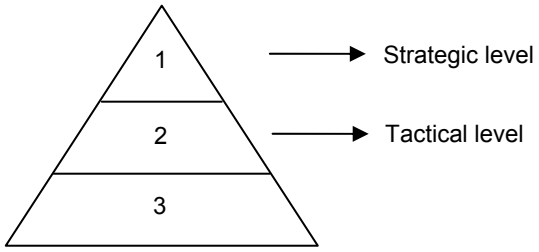


Figure 3: Levels or an organization

5.3 IT control framework for compliance with section 409

The IT control framework for compliance with section 409 will be presented in this paragraph. For each of the requirements, controls will be defined which are useful for complying with these requirements. First we will look to which control objectives of COBIT, at strategic level, can be used for the framework and then we look to which parts of the standards ITIL and ISO 17799, at tactical level, can be used to complementary the IT

controls of COBIT. The IT Governance Institute has released a document that maps the IT controls of the standards ITIL and ISO 17799, the lower level, to the IT controls of the COBIT framework, the higher level. For the set up of the framework this document and other documents of the IT Governance Institute has been used [ITGI 1, 2000] [ITGI 2, 2004] [ITGI 3, 2004] [ITGI 4, 2005].

In the first row of the IT control framework the identity is given of the concerning IT controls. The second row represents the IT control name. The IT control objective is described in the third row. In the last row the reference, to one of the official standards, of the IT control is presented.

5.3.1 Processes

To ensure that the processes are correct, organizations need IT controls that will help them establish the processes. These IT controls are for planning, executing, monitoring and reporting of the processes [ITGI 1, 2000] [ITGI 2, 2004] [ITGI 3, 2004] [ITGI 4, 2005].

ID	IT control name	IT control objective	Reference
P1	*IT as Part of the Organization's Long- and Short-Range Plan*	*Senior management is responsible for developing and implementing long- and short-range plans that fulfils the organization's mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organization's long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organization.*	*COBIT PO1.1*
P1.1	The Approach to Business Alignment	*The strategic plan must be clear. The plan that underpins the organization's strategy must be clearly understood so that IS can be influenced and guided to work within such policies.*	ITIL Business Perspective 4
P2	*Communication of IT Plans*	*Management should ensure that IT long- and short-range plans are communicated to business process owners and other relevant parties across the organization.*	*COBIT PO1.6*
P3	*Monitoring and Evaluating of IT Plans*	*Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long- and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.*	*COBIT PO1.7*
P4	*Review of Organizational Achievements*	*A framework should be in place for reviewing the organizational structure to continuously meet objectives and changing circumstances.*	*COBIT PO4.3*

P5	*Positive Information Control Environment*	*In order to provide guidance for proper behaviour, remove temptation for unethical behaviour and provide discipline, where appropriate, management should create a framework and an awareness programme fostering a positive control environment throughout the entire organization. This should address the integrity, ethical values and competence of the people, management philosophy, operating style and accountability. Specific attention is to be given to IT aspects, including security and business continuity planning.*	*COBIT PO6.1*
P6	*Management's Responsibility for Policies*	*Management should assume full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives. Regular reviews of policies for appropriateness should be carried out. The complexity of the written policies and procedures should always be commensurate with the organization size and management style.*	*COBIT PO6.2*
P7	*Communication of Organization Policies*	*Management should ensure that organizational policies are clearly communicated, understood and accepted by all levels in the organization. The communication process should be supported by an effective plan that uses a diversified set of communication means.*	*COBIT PO6.3*
P8	*Policy Implementation Resources*	*Management should plan for appropriate resources for policy implementation and for ensuring compliance, so that they are built into and are an integral part of operations. Management should also monitor the timeliness of the policy implementation.*	*COBIT PO6.4*
P9	*Maintenance of Policies*	*Policies should be adjusted regularly to accommodate changing conditions. Policies should be re-evaluated, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness, and amended as necessary. Management should provide a framework and process for the periodic review and approval of standards, policies, directives and procedures.*	*COBIT PO6.5*
P10	*Compliance with Policies, Procedures and Standards*	*Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the policies and procedures are being followed. Compliance procedures for ethical, security and internal control standards should be set by top management and promoted by example.*	*COBIT PO6.6*
P11	*Security and Internal Control Framework Policy*	*Management should assume full responsibility for developing and maintaining a framework policy which establishes the organization's overall approach to security and internal control to establish and improve the protection of IT resources and integrity of IT systems. The policy should comply with overall business objectives and be aimed at minimisation of risks through preventive measures, timely identification of irregularities, limitation of losses and timely*	*COBIT PO6.8*

		restoration. Measures should be based on cost/benefit analyses and should be prioritised. In addition, management should ensure that this high-level security and internal control policy specifies the purpose and objectives, the management structure, the scope within the organization, the definition and assignment of responsibilities for implementation at all levels, and the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies. Criteria for periodic re-evaluation of the framework should be defined to support responsiveness to changing organizational, environmental and technical requirements.	
P12	*External Requirements Review*	*The organization should establish and maintain procedures for external requirements review and for the coordination of these activities. Continuous research should determine the applicable external requirements for the organization. Legal, government or other external requirements related to IT practices and controls should be reviewed. Management should also assess the impact of any external relationships on the organization's overall information needs, including determination of the extent to which IT strategies need to conform with or support the requirements of any related third-parties.*	*COBIT PO8.1*
P13	*Electronic Commerce*	*Management should ensure that formal contracts are in place establishing agreement between trading partners on communication processes and on standards for transaction message security and data storage. When trading on the Internet, management should enforce adequate controls to ensure compliance with local laws and customs on a world-wide basis.*	*COBIT PO8.5*
P13.1	Electronic commerce security	*Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and on-line transactions across public networks such as the Internet. Electronic commerce is vulnerable to a number of network threats which may result in fraudulent activity, contract dispute and disclosure or modification of information. Controls should be applied to protect electronic commerce from such threats. Security considerations for electronic commerce should include the following:* *a) Authentication. What level of confidence should the customer and trader require in each others claimed identity?* *b) Authorization. Who is authorized to set prices, issue or sign key trading documents? How does the trading partner know this?* *c) Contract and tendering processes. What are the requirements for confidentiality, integrity and proof of despatch and receipt of key documents and the non-repudiation of contracts?* *d) Pricing information. What level of trust can be put in the integrity of the advertised price list and the confidentiality of sensitive discount arrangements?* *e) Order transactions. How is the confidentiality and integrity of order, payment and delivery address details, and confirmation of receipt, provided?* *f) Vetting. What degree of vetting is appropriate to check payment information supplied by the*	ISO 17799 8.7.3

		customer? *g) Settlement. What is the most appropriate form of payment to guard against fraud?* *h) Ordering. What protection is required to maintain the confidentiality and integrity of order information, and to avoid the loss or duplication of transactions?* *i) Liability. Who carries the risk for any fraudulent transactions?* *Many of the above considerations can be addressed by the application of cryptographic techniques, taking into account compliance with legal requirements. Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization. Other agreements with information service and value added network providers may be necessary. Public trading systems should publicize their terms of business to customers.* *Consideration should be given to the resilience to attack of the host used for electronic commerce, and the security implications of any network interconnection required for its implementation*	
P14	*Coordination and Communication*	*Management should establish a process for ensuring close coordination and communication between customers of the IT function and system implementers. This process should entail structured methods using the system development life cycle methodology to ensure the provision of quality IT solutions which meet the business demands. Management should promote an organization which is characterised by close cooperation and communication throughout the system development life cycle.*	*COBIT PO11.8*
P15	*Performance Procedures*	*Procedures should be put in place to ensure that the manner of and responsibilities for performance governing relations (e.g., non-disclosure agreements) between all the involved parties are established, coordinated, maintained and communicated to all affected departments.*	*COBIT DS1.3*
P16	*Monitoring and Reporting*	*Management should appoint a service level manager who is responsible for monitoring and reporting on the achievement of the specified service performance criteria and all problems encountered during processing. The monitoring statistics should be analysed on a timely basis. Appropriate corrective action should be taken and failures should be investigated.*	*COBIT DS1.4*
P17	*Availability and Performance Requirements*	*The management process should ensure that business needs are identified regarding availability and performance of information services and converted into availability terms and requirements.*	*COBIT DS3.1*
P17.1	Determing Availability requirements	*Determing the availability requirements of the business. Analyses are needed for the desired availability level.*	ITIL Availability Management 8.5.1
P17.2	Business Capacity Management	*Ensure that the business requirements for IT services are considered and understood, and that sufficient capacity to support the services is*	ITIL Capacity Management 6.2.1

		planned and implemented in an appropriate timescale.	
P17.3	Capacity planning	*Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections should take account of new business and system requirements and current and projected trends in the organization's information processing.* *Mainframe computers require particular attention, because of the much greater cost and lead time for procurement of new capacity. Managers of mainframe services should monitor the utilization of key system resources, including processors, main storage, file storage, printers and other output devices, and communications systems. They should identify trends in usage, particularly in relation to business applications or management information system tools.* *Managers should use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services, and plan appropriate remedial action.*	ISO 17799 8.2.1
P18	*Monitoring and Reporting*	*Management should implement a process to ensure that the performance of IT resources is continuously monitored and exceptions are reported in a timely and comprehensive manner.*	*COBIT DS3.3*
P18.1	Monitoring	*Monitors should be specific to particular parts of IT. This is needed to ensure the optimal use of the resources, to achieve the agreed service level and that business volumes are expected.*	ITIL Capacity Management 6.3.1
P18.2	Availability measurement and reporting	*The output of the Availability Management process is the measurement and reporting of IT Availability.*	ITIL Availability Management 8.7
P19	*Emergency Processing Priorities*	*Emergency processing priorities should be established, documented and approved by appropriate program and IT management.*	*COBIT DS10.5*
P19.1	Aspects of business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.	ISO 17799 11.1
P20	*Source Document Data Collection*	*The organization's procedures should ensure that all authorised source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry.*	*COBIT DS11.3*
P21	*Data Processing Integrity*	*The organization should establish procedures for the processing of data that ensure separation of duties is maintained and that work performed is routinely verified. The procedures should ensure adequate update controls such as run-to-run control totals and master file update controls are in place.*	*COBIT DS11.9*
P22	*Data Processing Validation and*	*The organization should establish procedures to ensure that data processing validation,*	*COBIT DS11.10*

	Editing	*authentication and editing are performed as close to the point of origination as possible. When using Artificial Intelligence systems, these systems should be placed in an interactive control framework with human operators to ensure that vital decisions are approved.*	
P23	*Processing Operations Procedures and Instructions Manual*	*IT management should establish and document standard procedures for IT operations (including network operations). All IT solutions and platforms in place should be operated using these procedures, which should be reviewed periodically to ensure effectiveness and adherence.*	*COBIT DS13.1*
P23.1	Documented Operating procedures	*The operating procedures identified by the security policy should be documented and maintained. Operating procedures should be treated as formal documents and changes authorized by management.* *The procedures should specify the instructions for the detailed execution of each job including:* *a) Processing and handling of information;* *b) Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;* *c) Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;* *d) Support contacts in the event of unexpected operational or technical difficulties;* *e) Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs;* *f) System restart and recovery procedures for use in the event of system failure.* *Documented procedures should also be prepared for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.*	ISO 17799 8.1.1
P24	*Collecting Monitoring Data*	*For the IT and internal control processes, management should ensure relevant performance indicators (e.g., benchmarks) from both internal and external sources are being defined, and that data is being collected for the creation of management information reports and exception reports regarding these indicators. Controls should also be aimed at validating the propriety and integrity of both organizational and individual performance measures and indicators.*	*COBIT M1.1*
P24	*Management Reporting*	*Management reports should be provided for senior management's review of the organization's progress toward identified goals. Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Upon review, appropriate management action should be initiated and controlled.*	*COBIT M1.4*
P25	*Internal Control Monitoring*	*Management should monitor the effectiveness of internal controls in the normal course of operations*	*COBIT M2.1*

		through management and supervisory activities, comparisons, reconciliations and other routine actions. Deviations should evoke analysis and corrective action. In addition, deviations should be communicated to the individual responsible for the function and also at least one level of management above that individual. Serious deviations should be reported to senior management.	
P25.1	Compliance with legal requirements	*To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.*	ISO 17799 12.1

Table 6: IT controls for complying with requirements of "processes"

5.3.2 IT infrastructure

To establish a well organized IT infrastructure, IT controls are needed to set up the infrastructure for IT in the organization. Also IT controls are useful for designing of the IT infrastructure [ITGI 1, 2000] [ITGI 2, 2004] [ITGI 3, 2004] [ITGI 4, 2005].

ID	IT Control name	IT Control objective	Reference
I1	*Information Architecture Model*	*Information should be kept consistent with needs and should be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities effectively and on a timely basis. Accordingly, the IT function should create and regularly update an information architecture model, encompassing the corporate data model and the associated information systems. The information architecture model should be kept consistent with the IT long-range plan.*	*COBIT PO2.1*
I1.1	Design and Planning	*Involves the development and maintenance of IS strategies for the deployment of infrastructure solutions to meet business needs.*	ITIL ICT Infrastructure Management
I2	*Data Classification Scheme*	*A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined.*	*COBIT PO2.3*
I3	*Technological Infrastructure Planning*	*The IT function should create and regularly update a technological infrastructure plan which is in accordance with the IT long- and short-range plans. Such a plan should encompass aspects such as systems architecture, technological direction and migration strategies.*	*COBIT PO3.1*
I4	*Technological*	*The technological infrastructure plan should be*	*COBIT PO3.3*

	Infrastructure Contingency	*assessed systematically for contingency aspects (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure).*	
I4.1	Activities in capacity management	*Specific activities must be undertaken when carrying out any of the sub-processes of capacity management.*	ITIL Capacity Management 6.3
I4.2	Availability planning	*Planning for availability must be made. Activities for planning the availability planning are needed.*	ITIL Availability Management 8.5
I4.3	Aspects of business continuity management	*To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.*	ISO 17799 11.1
I5	*Information Architecture*	*Management should ensure that attention is paid to the enterprise data model while solutions are being identified and analysed for feasibility.*	*COBIT AI1.7*
I6	*Source Data Collection Design*	*The organization's system development life cycle methodology should require that adequate mechanisms for the collection and entry of data be specified for each information system development or modification project.*	*COBIT AI2.6*
I7	*Data Classification*	*Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived or deleted. Evidence of owner approval and data disposition should be maintained. Policies should be defined to support reclassification of information, based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between organizations, addressing both security and compliance with relevant legislation.*	*COBIT DS5.8*
I7.1	Classification guidelines	*Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, and the business impacts associated with such needs, e.g. unauthorized access or damage to the information. In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected. Information and outputs from systems handling classified data should be labelled in terms of its value and sensitivity to the organization. It may also be appropriate to label information in terms of how critical it is to the organization, e.g. in terms of its integrity and availability. Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to an unnecessary additional business expense. Classification guidelines should anticipate and allow for the fact that the classification of any given item of information is not necessarily fixed for all time, and may change in accordance with some*	ISO 17799 5.2.1

	predetermined policy. Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic to use or prove impractical. Care should be taken in interpreting classification labels on documents from other organizations which may have different definitions for the same or similarly named labels. The responsibility for defining the classification of an item of information, e.g. for a document, data record, data file or diskette, and for periodically reviewing that classification, should remain with the originator or nominated owner of the information.	

Table 7: IT controls complying with requirements of "IT infrastructure"

5.4 Conclusion

By setting up the IT control framework for compliance with section 409 of the Sarbanes-Oxley Act, an answer has been given to the following research questions:

- What are strategic and tactical levels?
- How will the framework look like?

We have seen that the section 409 of the Sarbanes-Oxley Act actually contains two new specific requirements. These are the requirements “processes” and “IT infrastructure”. The framework for compliance with section 409 will focus on these two requirements. Because the framework is on strategic and tactical level, the definitions of strategic and tactical levels are described in this chapter. The framework contains IT controls from COBIT on strategic level and these IT controls are complemented by the IT controls from ITIL and ISO 17799 on tactical level. IT controls for the requirement “processes” focus on planning, executing, monitoring and reporting of the processes. IT controls for the requirement “IT infrastructure” focus on the set up and designing of the IT infrastructure

Chapter 6

Test

6.0 Introduction

This chapter gives a description of the test of the requirements of section 409 of the Sarbanes-Oxley Act and the framework for compliance with section 409 of the Sarbanes-Oxley Act. The set up of the test will be presented in the following paragraph. Thereafter the result of the test will be discussed.

6.1 Test set-up

The hypotheses for the test will be described first. This is followed by the method, which we want to use to test our hypothesis and after that, a list of professionals is given. These professionals have been interviewed for the test.

6.1.1 Hypotheses

Via interviews we will test two hypotheses. The first hypothesis is the requirements of section 409 of the Sarbanes-Oxley Act on IT control. These requirements are presented in table 1 on page 34. The requirements are “application controls”, “processes”, “IT infrastructure” and “systems”.

The second hypothesis is the framework for compliance with section 409 of the Sarbanes-Oxley Act on strategic and tactical level. This framework consist IT controls of the standards COBIT, ITIL and ISO 17799 for the requirements “processes” and “IT infrastructure”. These IT controls are given in tables 6 and 7 on pages 55-63.

6.1.2 Method

To test the requirements and framework we will use an empirical research. An empirical research is any activity that uses direct or indirect observation as its test of reality [Wikipedia 4, 2005]. For this research we will use interviews to test our requirements of section 409 and framework for compliance with section 409 on strategic and tactical level.

We have done several interviews with experts on the area of IT auditing. These experts are divided into external en internal, because internal expert could have different knowledge, experience and insight than the external expert. Internal experts are usually people who have set up the control environment within the organization and the external experts are people who will test these control environment. By splitting the experts into internal and external a completely representation can be create of the requirements and needs of the section 409 of the Sarbanes-Oxley Act.

The interviews are dividend in two parts. The first part is to test the requirements of section 409 of the Sarbanes-Oxley Act on IT control, according to the experts. This will be done by asking the following question: "*What are the requirements of the section 409 of the Sarbanes-Oxley Act on IT control according to you?*". By asking this question, the completeness and the correctness of the first hypothesis can be tested. If the expert does not mentioned all the requirements from the first hypothesis then we will put this to the expert to determine how far this is relevant to IT control according to the expert. This will be done by asking the following question: "*If you did not mentioned the requirements by question 1A, but I have these requirements in mine hypothesis then I want to put this to you. This is needed to know of how much you think these requirements are relevant*".

By means of the second part of the interview we want to know which IT controls (of the standards COBIT, ITIL and ISO 17799) can be used for the compliance with the new requirements of section 409 of the Sarbanes-Oxley Act on strategic and tactical level. This will be done by asking the following question: "*Which IT controls of the standards COBIT, ITIL and ISO 17799 can be used for the compliance with the new requirements of section 409 on strategic and tactical level according to you?*". By asking this question, the correctness and completeness of the second hypothesis can be tested. If he does not mentioned all the IT controls from our hypothesis then we will put this to the expert to determine how far this is relevant to the requirements according to the expert. This will be done by asking the question: "*If you did not mentioned the IT controls by question 2A, but I have these IT controls in mine hypothesis then I want to put this to you. This is needed to know of how much you think these IT controls are relevant for the requirements*".

6.1.3 Interview

The interviews are held with professionals who are mentioned in the table below. The first column is the name given of the person, the second column the function of this person and the last column the sort of auditor.

Name	*Function*	***Sort of auditor***
Ivan Spruit	*IT-auditor*	*External*
Sander Reerink	*IT-auditor*	*External*
Stan van Bommel	*IT-auditor*	*Internal*
Stefan Schuiling	*Manager of an auditing department*	*Internal*

Table 8: Interview

6.2 Test results

In the previous paragraph is the set up of the test described. In this paragraph we will discuss the results of the test of the hypotheses, which are also described in the previous paragraph, by having interviews with experts. First we will give the results of the two hypotheses. We will show this by giving the summation of each question. After that the total summation of the requirements of section 409 on IT control and the IT controls of the framework will be described. In Appendix D is a report of the interviews given.

6.2.1 Summation of the questions

"What are the requirements of the section 409 of the Sarbanes-Oxley Act on IT control according to you?"

The internal experts mentioned one requirement of the four requirements of the first hypothesis. This is the requirement "processes". The external experts have mentioned that you first have to know which information you need then you know how you can deliver this information. To know this there is insight in processes needed. Further, they have conveyed

that internal controls (section 404) are important for section 409. The other requirements that they have not mentioned will be tested by the next question.

"If you did not mentioned the requirements by question 1A, but I have these requirements in mine hypothesis then I want to put this to you. This is needed to know of how much you think these requirements are relevant"

The internal experts do think that all requirements of the first hypothesis are relevant for section 409, but according to them, these requirements are also requirements of section 404; the internal control. However, these requirements are important for section 409 according to them. Section 409 does not specific requires new requirements. The external experts also think that the requirements are important for compliance with section 409.

"Which IT controls of the standards COBIT, ITIL and ISO 17799 can be used for the compliance with the new requirements of section 409 on strategic and tactical level according to you?"

According to the internal experts, COBIT is a good framework to use for the compliance with the requirements. One of the experts said that section 409 does not have specific requirements on IT control, because section 404 (internal control) already demands this. The external experts also have mentioned that COBIT is a useful framework for the requirements. IT controls for section 404 are also relevant for section 409. The document "IT controls for Sarbanes-Oxley" of ISACA is helpful. This document describes which IT controls of COBIT are needed for compliance with sections 302 and 404.

"If you did not mentioned the IT controls by question 2A, but I have these IT controls in mine hypothesis then I want to put this to you. This is needed to know of how much you think these IT controls are relevant for the requirements"

The internal experts think that the document "IT controls for Sarbanes-Oxley" of ISACA is useful for the compliance with section 409. IT controls for internal control and IT infrastructure are relevant for this section. The document "Aligning COBIT, ITIL and ISO 17799 for Business Benefits" of ISACA is useful document for mapping ITIL and ISO 17799 to the COBIT framework. The external experts have mentioned that the documents "IT control for Sarbanes-Oxley" and "Aligning COBIT, ITIL and ISO 17799 for Business Benefits" are helpful by selecting IT controls for the requirements.

6.2.2 Requirements of section 409 on IT control

The internal experts have the opinion that the section 409 of the Sarbanes-Oxley Act does not have really new requirements on IT control. Section 404 of the Act demands organization to organize their internal control well. Implicitly the requirements “application controls”, “processes”, “IT infrastructure” and “systems” are requirements of section 404 of the Sarbanes-Oxley Act. This has the consequence that the application controls, processes, IT infrastructure and systems need to be well established. For the compliance with section 409 these requirements are certainly necessary. Section 404 is the most important section of the Sarbanes-Oxley Act. Many sections of the Act have a relation with this section.

The external experts mentioned that the section 409 has certain requirements with respect to IT control. The requirements “application controls”, “processes”, “IT infrastructure” and “systems” are required to be compliance with section 409. “Application controls” and “processes” are also requirements of the internal control, the requirement of section 404 of the Act. The requirement “application controls” can be combined with the requirement “processes” and the requirement “systems” with the requirement “IT infrastructure”. We see that we have two main requirements: “processes” and “IT infrastructure”. The experts also think that the internal controls, the requirement of section 404, are important for most sections of the Act.

6.2.3 Framework for compliance with section 409

The experts have the opinion that the framework with the IT controls is useful for the compliance with the section 409. All these IT controls will contribute to have correct processes and well organized IT infrastructure. To comply with the section 409 of the Sarbanes-Oxley Act organizations have to focus on the internal processes which need to be effective and efficient. IT controls are needed for planning, executing, monitoring and reporting of the processes. The IT controls of the framework ensure that the processes will be effective and efficient. The IT controls for the IT infrastructure in the framework will lead to an effective and efficient IT infrastructure. IT controls are therefore needed for setting up and designing of the IT infrastructure.

We just described that the requirements of section 409 are also relevant for section 404. The experts marked that the document “IT control for Sarbanes-Oxley” is very helpful by choosing relevant IT controls for section 409. This document describes which IT controls of COBIT are needed for compliance with sections 302 and 404 of the Sarbanes-Oxley Act. An IT control framework with the IT controls for sections 404 and 409 could be very useful in practice.

COBIT is appropriate for designing an IT control framework at strategic (or maybe tactical) level. For a lower level like the tactical level are the standards ITIL and ISO 17799 better useful. These standards have specific practices for some controls. For choosing IT controls of ITIL and ISO 17799 for COBIT on tactical level, the documents “Cobit Mapping” and “Aligning COBIT, ITIL and ISO 17799 for Business Benefits” are very useful.

6.3 Conclusion

By testing the hypotheses, described in this chapter, an answer has been given to the following research questions:

- Which requirements does the section 409 have for IT control according to experts and how do experts think of this framework?
- How can the framework be supplemented?

This chapter has described which hypotheses will be tested by interviewing experts. The four formulated requirements of section 409 of the Sarbanes-Oxley Act and the framework for compliance with the requirements “processes” and “IT infrastructure” on strategic and tactical level have been tested. The method of the test has been described and we have seen who have been interviewed for this test.

We have seen that the experts have the opinion that the first hypothesis, with the respect to the requirements of section 409 on IT control, is right. The experts think that the section 409 has the requirements “application controls”, “processes”, “IT infrastructure” and “systems” on IT control. A requirement, which also could be relevant for section 409, is internal control. Section 404 demands that the internal controls of an organization have to be well organized. Section 404 could be seen as a requirement for section 409.

The framework for compliance with section 409 on strategic and tactical level is useful for requirements “processes” and “IT infrastructure”. This framework has relevant IT controls for these requirements on strategic and tactical level. The framework could be expanded with IT controls for internal control. The whole IT control framework is presented in Appendix E.

Chapter 7

Conclusions and future research

7.0 Conclusions

The goal of this thesis was to do a research about the impact of section 409 of the Sarbanes-Oxley Act on IT control and to develop a framework on strategic and tactical level for compliance with the new requirements of section 409. With the describing of the requirements of section 409 on IT control we have outline what the impact is. By a literature study we have found that the section 409 have four requirements, these are:

- *Application controls*: to protect the information;
- *Processes*: ensuring correct, efficient and effective IT processes for the delivery of information;
- *IT infrastructure*: in condition to deliver information within 48 hours;
- *Systems*: integrated and in condition to produce information within 48 hours.

Via interviews with experts we have tested these requirements. All of the experts think that these aspects are needed for the compliance with section 409, but these requirements are not (all) specific for section 409. Some of these requirements are already demand by section 404, the section that requires for internal controls. For the totally compliance of section 409 organizations have also look to section 404. If organizations have to meet the requirements of section 404, then to be compliance with section 409 will generally not take much more time and energy. Section 404 has influence on the requirements of section 409. By describing the requirements of the section 409 on IT control, we have not looked to all aspects like the change management aspect. By having a well organized internal control this aspect is already included. The change management aspect and few other aspects are indirectly relevant for section 409. By describing the requirements of section 409 it is wise to look to section 404 too. For example in the literature section 302 will be seen with section 404, because these two sections have a relation with each other. Section 409 has to be seen with section 404 too. This will give organizations a totally clear representation of which requirements the sections have on IT control.

Trough a literature study an IT control framework for section 409 of the Sarbanes-Oxley Act on strategic and tactical level has been developed for the requirements “processes” and “IT infrastructure”. The experts mentioned that the COBIT framework has IT controls on a high level. These controls can be used for the strategic level. The standards ITIL and ISO 17799 have IT controls on a lower level. These IT controls can be used for the tactical level. The IT controls of these two standards can be mapped to the COBIT framework. We can conclude that we have chosen a right structure for the IT control framework for section 409 on strategic and tactical level.

The experts think that the IT control framework has relevant IT controls for the requirements “processes” and “IT infrastructure” on strategic and tactical level. By setting up the framework for section 409 the documents “Cobit Mapping”, “IT controls for Sarbanes-Oxley” and “Aligning COBIT, ITIL and ISO 17799 for Business Benefits” of the IT Governance Institute are used.

The presented IT control framework for the requirements of section 409 is not complete. It does not have IT controls for the requirements “applications controls” and “systems”. We have done this conscious, because we only wanted to focus on the new requirements. For a more useful IT control framework for compliance with the section 409 IT controls must be defined for all requirements of this section. Thereby IT controls for internal control are also needed.

An important point about section 409 is the content of this section. People can interpret this section in many ways. That is the reason that (some) experts gave different answers by some questions. The interpretation of this section must be the same for all the people.

7.1 Future research

With this thesis, an exploring research has been done for the requirements of section 409 of the Sarbanes-Oxley Act on IT control. A further research can be done for a total insight in the requirements of the sections 404 and 409. The section 409 does directly require correct internal control. Therefore, section 404 of the Act is necessary for section 409.

The IT control framework for compliance with the requirements “processes” and “IT infrastructure” of section 409 on strategic and tactical level, which is presented in this thesis, has to be tested by test cases (in practice). A further research on this can be done. Besides, the IT control framework is not complete for compliance with all the requirements of section 409 on IT control. A further research can be done for setting up a new IT control framework or supplement the IT control framework in this thesis, which is useful for the compliance with

all requirements of the section 409 on IT control. Besides researching IT controls for the other two requirements of section 409, a research can be done for selecting the (remaining) IT controls for the internal control. To select IT controls on lower level like tactical and operational level the document “Aligning COBIT, ITIL and ISO 17799 for Business Benefits” of ISACA can be used.

A technique that can be useful for helping with the compliance with section 409 is XBRL. This simple technique collects data and represents the data easy and fast. A further research on the use of this technique with section 409 is interesting.

References

Becht, M., Bolton, P. en Röell, A., Corporate Governance and Control, Handbook of the Economics of Finance, Elsevier, 2003

Boccasam, P. V., *The impact of Sarbens-Oxley on Enterprise applications: It's a dilemma of heroic proportions*, http://www.s-ox.com/features/article.cfm?articleID=212, visited June 2005

Brickey, K. F., *From Enron to Worldcom and beyond: life and crime after Sarbanes-Oxley*, Washington University in St. Louis, School of law, 1 June 2003

Cannon, D. M. , Growe, G. A., *How Does Sarbanes-Oxley Affect Outsourcing?*, Wiley Periodicals Inc., March/April 2005

Capgemini, *CobiT Framework*, http://academy.capgemini.nl/Content.aspx?menuid=135, visited September 2005

Carlson, T., *Information Security Management: Understanding ISO 17799*, INS, October 2001

Chan, S. & Lepeak, S., *IT and Sarbanes Oxley,* CMA MANAGEMENT 3, 4 June/July 2004

Chopskie, E., *Sarbanes-Oxley and the IT organization: A survival guide for year two*, Evolve Wisely, January 2005

Commissie Corporate Governance, *Aanbevelingen inzake Corporate Governance in Nederland*, 25 June 1997

COSO, Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control - Integrated Framework*, 1992

Damianides, M., *How Does SOX Change IT?*, The Journal of Corporate Accounting & Finance, September/October 2004

Damianides, M., *Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance*, Information System Management, winter 2005

Gouffran, P., *Geld moet transparant rollen - Sarbanes-Oxley aansporing tot verbetering informatiesystemen*, http://www.computable.nl/artikels/archief4/d49hb4mi.htm, visited June 2005

Hart, O., *Corporate Governance: Some Theory and Implications*, The Economic Journal, 105 (May), 678-689

Herwaarden, P., Boer, M., Visser, C.A., *Van financial reporting control naar organisatiebrede control en risicomanagement: Hoe 'Sarbanes-Oxley' kan leiden tot goed ondernemingsmanagement,* AIV control, October 2003

Hoffman,T *Rapid-reporting mandate adds to compliance woes: Companies need systems overhauls to meet Sarbanes-Oxley's 'material events' requirement*, 14 juli 2003, http://computerworld.com/governmenttopics/government/policy/story/0,10801,83004,00.html, visited June 2005

Instituut der bedrijfsrevisoren, *Corporate Governanceen de toegevoegde waarde van de bedrijfsrevisor*, Periodieke berichten nr. 2/2003, http://www.ibr-ire.be/ned/periodiekeberichten/berichten003204.aspx, visited June 2005

ISACA, http://www.isaca.org/AMTemplate.cfm?Section=Sarbanes-Oxley2&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11239, Sarbanes-Oxley FAQ's, visited June 2005

ISO17799, *Information technology — Code of practice for information security management*, British Standards Institution, 2000

ITGI 1, *Cobit Control Objectives 3rd Edition*, IT Governance Institute, 2000

ITGI 2, *Cobit Mapping: Overview of International IT Guidance*, IT Governance Institute, 2004

ITGI 3, *IT Controls for Sarbanes-Oxley*, IT Governance Institute, 2004

ITGI 4, *Aligning COBIT, ITIL and ISO 17799 for Business Benefits,* IT Governance Institute, 2005

ITIL 1, *Service Support*, British Office of Government Commerce, 2000

ITIL 2, *Service Delivery*, British Office of Government Commerce, 2001

ITIL 3, *Business Perspective*, British Office of Government Commerce, 2004

ITIL 4, *ICT Infrastructure Management*, British Office of Government Commerce, 2001

Janstal, S., *Enterprise Resource Planning: Integrating Applications and Business Processes across the Enterprise*, Computer Technology Research Corporation, April 1999

Kaarst-Brown, M. L., Kelly, S., *IT Governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT Function?*, Proceedings of the 38th Hawaii International Conference on System Sciences – 2005

De Kennisgroep IT-Governance, *IT-Governance Een verkenning,* NOREA, June 2004

Kintraco Management Consultants, *Sarbanes Oxley: Samenvatting op hoofdlijnen van de Sarbanes Oxley Act (Bron: NRC 29 juli 2002)*, http://www.kintraco.nl/sarbanes%20oxley%20act%20samenvatting.htm, visited June 2005

Kral, R., *Technology Implications of Sarbanes-Oxley,* January 2004

McCollum, T., *Sarbanes-Oxley: The IT Dimension*, Computers & Auditing, February 2004

McNally, J. S., *Another hurdle on the road to compliance: Assessing company-level controls*, Pennsylvania CPA Journal, Winter 2005

Mitchell, L. E., *The Sarbanes-Oxley Act and the Reinvention of Corporate Governance?*, Villanova University School of Law's Law Review Symposium Uitgave, *Lessons from Enron, How did Corporate and Securities Law Fail?,* Volume 48, nummer 4, 2003

NetSec, *SOX & security*, NetSec Security brief, November 2004

Overbeek, P., Roos Lindgreen, E., Spruit, M., *Informatiebeveiliging onder controle*, Pearson Education, 2000

Protiviti, *COSO Description*, http://www.knowledgeleader.com/iafreewebsite.nsf/content/COSOFrameworkDescription!OpenDocument, visited September 2005

Renes, R. M., *Zonder interne beheersing geen corporate governance,* Accounting nr, 9, September 2004

Romano, R., *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance,* Yale Law School, Yale International Center for Finance

SEC, *Sarbanes-Oxley Act 2002*, U.S. Securities and Exchange Commission, 2002

Spafford, G., *Control Framework Misconceptions*, http://itmanagement.earthweb.com/netsys/article.php/3439901, 2004, visited October 2005

The Information Management Company, *ICT Infrastructure Management – ICT Infrastructure Management Publications*, http://itil.tso.co.uk/ict_infrastructure_management.html, visited October 2005

The Telecom Glossary 2000, *The American National Standard for Telecommunications*, http://www.atis.org/tg2k, visited September 2005

Travis, R. J., *Overview of the Sarbanes-Oxley Act of 2002,* Briefing note Chartwell consulting, April 2003

Wallhoff, J., *How ITIL can be combined with ISO 17799 and COBIT*, Scillani Information, April 2005

Wikipedia 1, *COBIT*, http://en.wikipedia.org/wiki/COBIT#COBIT_and_ISO.2FIEC_17799:2000, visited September 2005

Wikipedia 2, *Information Technology Infrastructure Library*, http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library#Process_theory, visited October 2005

Wikipedia 3, *ISO/IEC 17799*, http://en.wikipedia.org/wiki/ISO/IEC_17799, visited October 2005

Wikipedia 4, *Emperical research*, http://en.wikipedia.org/wiki/Empirical_research, visited October 2005

Wyban, S., *Sarbanes-Oxley Compliance meets technology*, Computer Technology Review, September 2004

Zimmermann, J., Sarbanes-*Oxley compliance: It's not over yet for public traded companies*, http://techrepublic.com.com/5100-6298_11-5035056.html, visited June 2005

Other websites:

www.isaca.org
www.coso.org
www.itgi.org
www.itil.org
www.wikipedia.org

Appendix A: Sections 302, 404 and 409

SECTIE 302. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS.

(a) REGULATIONS REQUIRED- The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that--

(1) the signing officer has reviewed the report;
(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;
(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;|(4) the signing officers--

(A) are responsible for establishing and maintaining internal controls;
(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;
(C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and
(D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)--

(A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and
(B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

(b) FOREIGN REINCORPORATIONS HAVE NO EFFECT- Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having

engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.
(c) DEADLINE- The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act.

SECTIE 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED- The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall--

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

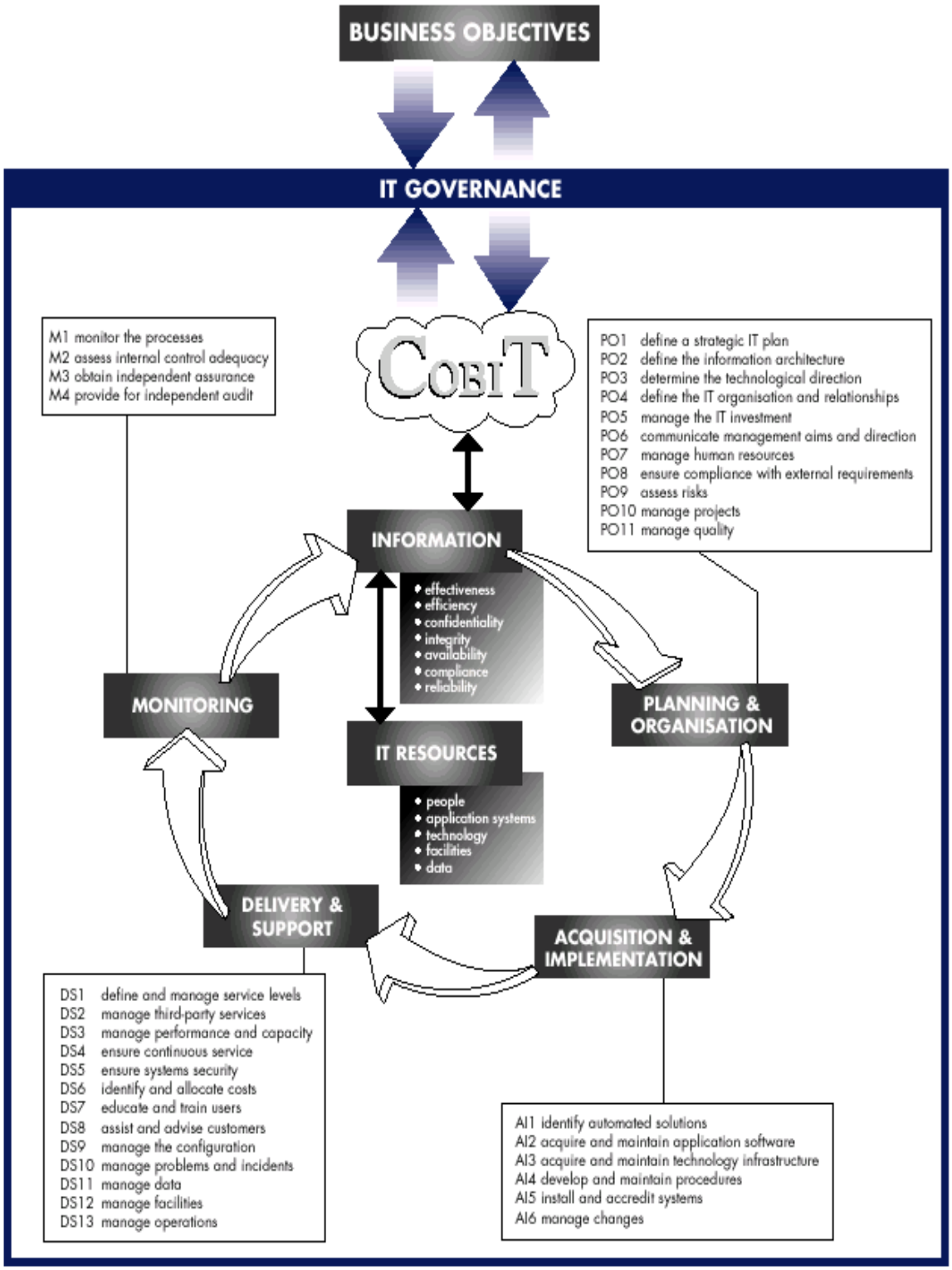
(b) INTERNAL CONTROL EVALUATION AND REPORTING- With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

SECTIE 409. REAL TIME ISSUER DISCLOSURES.

Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m), as amended by this Act, is amended by adding at the end the following:

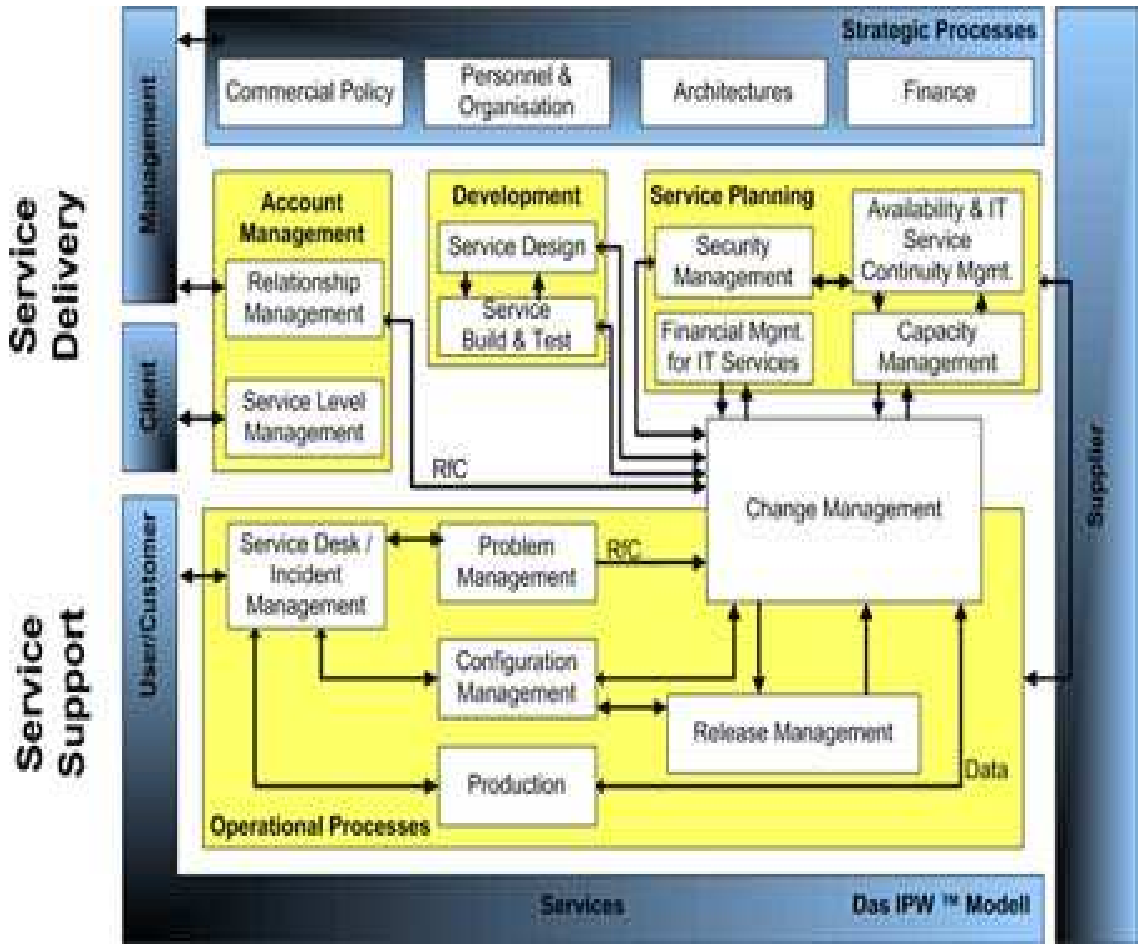
(l) REAL TIME ISSUER DISCLOSURES- Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest.'.

Appendix B: COBIT

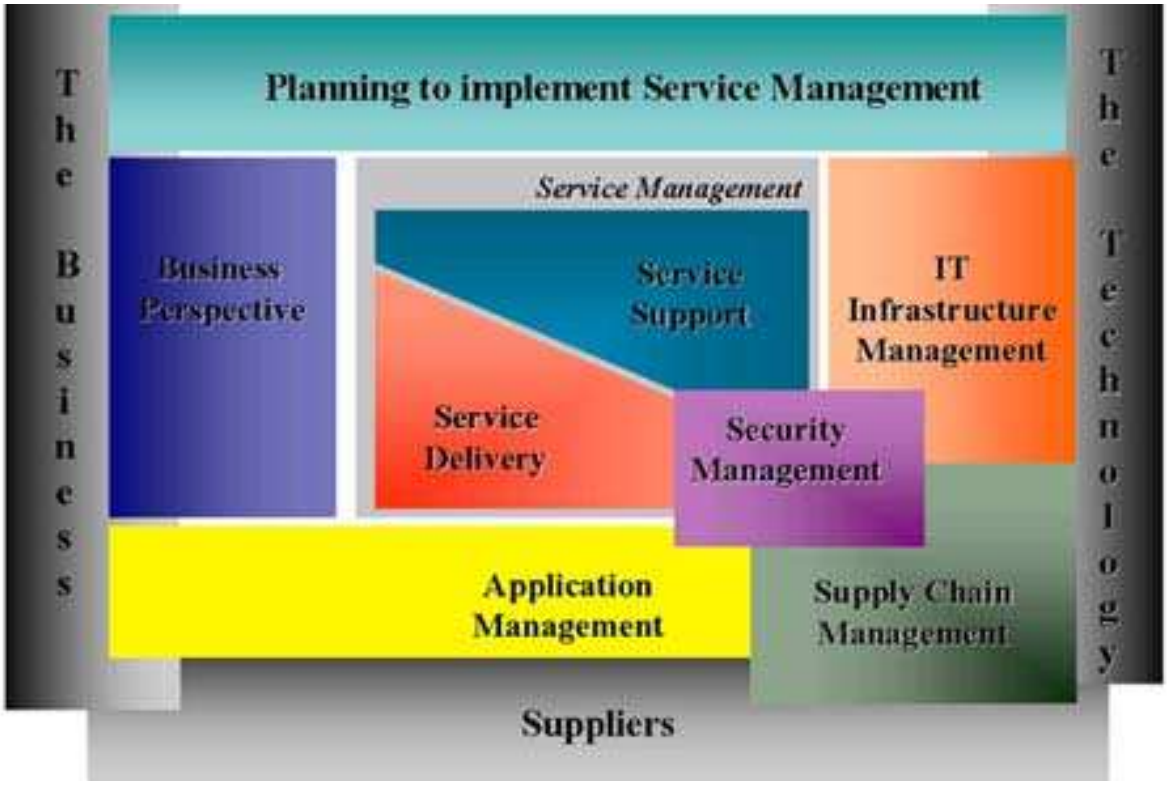


Appendix C: ITIL

Relationship between the sections and processes



ITIL standard



Appendix D: Interviews

Sander Reerink, 8 November 2005

1A. What are the requirements of the section 409 of the Sarbanes-Oxley Act on IT control according to you?

This is a difficult question. I think that it is important to know when the information is material. If you know this then you can think about of how you can supply this information. You also have to look to how you want to create the information in a report. The information, which is material, has to be decided with the accountant, because they know when information is material. Besides the law has not described what material exactly is, so that is a little bit difficult. I think that many people will interpret this section on a different way. It is also important that everybody knows what this section really demands.

1B. If you did not mentioned the requirements by question 1A, but I have these requirements in mine hypothesis then I want to put this to you. This is needed to know of how much you think these requirements are relevant.

Application controls, this is relevant. The information has to reliable and it is necessary that the information must to be protected for example changes by unauthorized persons. Application controls are a part of internal control. When your internal control and processes are correct then your application controls are probably also correct.

Processes, if the processes and procedures have to be right then this needed. The information is generated from the processes within the organization, so this is important to section 409. The procedures have to be correct to produce and supply the information. This is also relevant.

IT infrastructure, if we look to the availability and the sort of information then the organization of your IT in your organization is very important.

Systems, relevant systems and techniques like artificial intelligence can be used to retrieve the information on time. Websites can be used to deliver this information. This requirement can be seen as a part of the IT infrastructure.

2A. Which IT controls of the standards COBIT, ITIL and ISO 17799 can be used for the compliance with the new requirements of section 409 on strategic and tactical level according to you?

This is another difficult question. I think that a lot IT controls which are needed for the compliance with section 404 are also needed for the requirements of section 409. Therefore, IT controls for internal control are needed. So IT controls for planning, performance, availability and procedures are useful for example. The standard COBIT is very helpful.

2B. If you did not mentioned the IT controls by question 2A, but I have these IT controls in mine hypothesis then I want to put this to you. This is needed to know of how much you think these IT controls are relevant for the requirements.

IT controls for IT infrastructure are relevant. Especially if they describe how you must organize your information architecture and about how you must design your data model and systems. I think that these are the most important IT controls. An important technique can be used to help organization with the compliance with the section 409. This is XBRL, with this technique you can easily manage your data and to share data with other parties.

Further, I think that the IT controls of standards ITIL and ISO 17799 can be mapped to the COBIT framework (for a lower level).

Stefan Schuiling, 9 November 2005

1A. What are the requirements of the section 409 of the Sarbanes-Oxley Act on IT control according to you?

I think that there are no requirements of the section 409 on IT control. Section 409 just only has consequences for the disclosures of information concerning material changes in the financial condition of the organization. Indirectly this has no requirements for the IT control.

1B. If you did not mentioned the requirements by question 1A, but I have these requirements in mine hypothesis then I want to put this to you. This is needed to know of how much you think these requirements are relevant.

Application controls, needed but this can be seen as a part of the internal controls.

Processes, are important and certainly needed. Section 404 of the Sarbanes-Oxley Act demands organization that the internal controls have to be correct. If the internal control is correct then the processes within the organization are well organized. This has the consequence that the IT processes are also well organized.

IT infrastructure, for an organization this is certainly an important issue but for section 409 this has no influence. I agree that the IT infrastructure of the organization has to be correct but section 409 does not demand this. Section 409 only requires that the information have to be communicated to the interested parties. Section 404 already requires that the IT infrastructure (part of the internal controls) have to be correct.

Systems, in situation where Internet is used, I think that almost every company does, for the supply of information then systems has to be in condition to realize this. Nevertheless, I think section 404 already requires this. Many requirements of section 409 are the same for section 409. In fact, section 409 does not has many requirements, only that the information has to be communicated to the interested parties and this must be happen on time.

2A. Which IT controls of the standards COBIT, ITIL and ISO 17799 can be used for the compliance with the new requirements of section 409 on strategic and tactical level according to you?

I think that there are not IT controls which are useful for the requirements of section 409.

2B. If you did not mentioned the IT controls by question 2A, but I have these IT controls in mine hypothesis then I want to put this to you. This is needed to know of how much you think these IT controls are relevant for the requirements.

If we look to the internal controls, then these controls are enough for the compliance with section 409. The only extra demand of this section, comparing to section 404, is that the information has to be communicated to the interested parties on time. IT controls for internal controls are needed. IT controls are thereby needed for organizing your IT infrastructure. The document of ISAC, “IT control objectives for the Sarbanes-Oxley”, is a useful document that can be used for the compliance with section 302 and 404 of the Sarbanes-Oxley Act. The COBIT framework focuses on a higher abstract level. For mapping the standards ITIL and ISO 17799 (on a lower level) the document “Aligning COBIT, ITIL and ISO 17799 for Business Benefits” can be used.

Ivan Spruit, 17 November 2005

1A. What are the requirements of the section 409 of the Sarbanes-Oxley Act on IT control according to you?

I think that the section 409 of the Sarbanes-Oxley Act requires the organization to look to availability management, continuity management, change management and capacity management. I work a lot with section 404 of the Sarbanes-Oxley Act that requires the internal controls to be correct. This is a very important section of the Sarbanes-Oxley Act. Moreover, I think that al lot of requirements of section 404, like availability management and continuity management, are also important for section 409.

1B. If you did not mentioned the requirements by question 1A, but I have these requirements in mine hypothesis then I want to put this to you. This is needed to know of how much you think these requirements are relevant.

Application controls, these are important. For correct internal control, these controls have to be right.

Processes, definitely important. Organizations have to think how they have to structure their processes.

IT infrastructure, this is relevant. This means that organization has to think about how they have to organize their IT.

Systems, systems are used for generate information. So this is needed for recording and supplying of your information.

Many people interpret the content of sections 404 and 409 different. The scope determination of the sections is very important by organization. Some IT controls are relevant for some organizations and for some organizations not. In comparison with section 404, I do think that the section 409 demands that the information has to be communicated to the investors within a short time.

2A. Which IT controls of the standards COBIT, ITIL and ISO 17799 can be used for the compliance with the new requirements of section 409 on strategic and tactical level according to you?

I think that IT controls for capacity management, planning, continuity management and availability management are specific needed for section 409. Many IT controls for section 404 are also relevant for section 409. The IT controls, which are mentioned in the document of ISACA “IT controls for Sarbanes-Oxley” are also relevant.

2B. If you did not mentioned the IT controls by question 2A, but I have these IT controls in mine hypothesis then I want to put this to you. This is needed to know of how much you think these IT controls are relevant for the requirements.

These IT controls are relevant for section 409. If you used the documents “IT controls for Sarbanes-Oxley”, “Cobit Mapping” and “Aligning COBIT, ITIL and ISO 17799 for Business Benefits” then you probably have the right controls for section 409. COBIT consist IT controls on a higher level and ITIL and ISO 17799 can be used for filling places where COBIT is too abstract. These two standards can be mapped to the COBIT framework.

Stan van Bommel, 21 November 2005

1A. What are the requirements of the section 409 of the Sarbanes-Oxley Act on IT control according to you?

This is quiet difficult. I think that you have to conclude what it is relevant for the Act. The processes are relevant. The processes within the organization are important for this section. An important requirement is to understand your processes and to know if your processes are right. If you have that in picture then you automatically know which measures you need for these requirements.

1B. If you did not mentioned the requirements by question 1A, but I have these requirements in mine hypothesis then I want to put this to you. This is needed to know of how much you think these requirements are relevant.

Application controls, these controls are important for the protection of your information.

Processes, this is a requirement (already mentioned by question 1A). I think further that internal controls are important for the processes.

IT infrastructure, the IT infrastructure is based on the business processes within the organizations. To organize your infrastructure well is very essential.

Systems, you have to use right systems for your IT infrastructure and for the use of your information.

2A. Which IT controls of the standards COBIT, ITIL and ISO 17799 can be used for the compliance with the new requirements of section 409 on strategic and tactical level according to you?

The framework COBIT can be used for the compliance. Thereby are the IT controls very useful for the requirements; processes, application controls, IT infrastructure and systems.

2B. If you did not mentioned the IT controls by question 2A, but I have these IT controls in mine hypothesis then I want to put this to you. This is needed to know of how much you think these IT controls are relevant for the requirements.

I think that the standards ITIL and ISO 17799 can be used for the mapping to COBIT. COBIT describes what has to be done and ITIL and ISO 17799 can be used for how things can be done. I think that the document “Aligning COBIT, ITIL and ISO 17799 for Business Benefits” is a good document for mapping the ITIL and ISO 17799 to the COBIT framework.

Appendix E: Framework

Framework for compliance with the requirements “processes” and “IT infrastructure” of section 409 of the Sarbanes-Oxley Act

Processes			
ID	**IT control name**	**IT control objective**	**Reference**
P1	*IT as Part of the Organization’s Long- and Short-Range Plan*	*Senior management is responsible for developing and implementing long- and short-range plans that fulfils the organization’s mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organization’s long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organization.*	*COBIT PO1.1*
P1.1	The Approach to Business Alignment	*The strategic plan must be clear. The plan that underpins the organization’s strategy must be clearly understood so that IS can be influenced and guided to work within such policies.*	ITIL Business Perspective 4
P2	*Communication of IT Plans*	*Management should ensure that IT long- and short-range plans are communicated to business process owners and other relevant parties across the organization.*	*COBIT PO1.6*
P3	*Monitoring and Evaluating of IT Plans*	*Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long- and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.*	*COBIT PO1.7*
P4	*Review of Organizational Achievements*	*A framework should be in place for reviewing the organizational structure to continuously meet objectives and changing circumstances.*	*COBIT PO4.3*
P5	*Positive Information Control Environment*	*In order to provide guidance for proper behaviour, remove temptation for unethical behaviour and provide discipline, where appropriate, management should create a framework and an awareness programme fostering a positive control environment throughout the entire organization.*	*COBIT PO6.1*

		This should address the integrity, ethical values and competence of the people, management philosophy, operating style and accountability. Specific attention is to be given to IT aspects, including security and business continuity planning.	
P6	*Management's Responsibility for Policies*	*Management should assume full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives. Regular reviews of policies for appropriateness should be carried out. The complexity of the written policies and procedures should always be commensurate with the organization size and management style.*	*COBIT PO6.2*
P7	*Communication of Organization Policies*	*Management should ensure that organizational policies are clearly communicated, understood and accepted by all levels in the organization. The communication process should be supported by an effective plan that uses a diversified set of communication means.*	*COBIT PO6.3*
P8	*Policy Implementation Resources*	*Management should plan for appropriate resources for policy implementation and for ensuring compliance, so that they are built into and are an integral part of operations. Management should also monitor the timeliness of the policy implementation.*	*COBIT PO6.4*
P9	*Maintenance of Policies*	*Policies should be adjusted regularly to accommodate changing conditions. Policies should be re-evaluated, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness, and amended as necessary. Management should provide a framework and process for the periodic review and approval of standards, policies, directives and procedures.*	*COBIT PO6.5*
P10	*Compliance with Policies, Procedures and Standards*	*Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the polices and procedures are being followed. Compliance procedures for ethical, security and internal control standards should be set by top management and promoted by example.*	*COBIT PO6.6*
P11	*Security and Internal Control Framework Policy*	*Management should assume full responsibility for developing and maintaining a framework policy which establishes the organization's overall approach to security and internal control to establish and improve the protection of IT resources and integrity of IT systems. The policy should comply with overall business objectives and be aimed at minimisation of risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration. Measures should be based on cost/benefit analyses and should be prioritised. In addition, management should ensure that this high-level security and internal control policy specifies the purpose and objectives, the management structure, the scope within the organization, the definition and assignment of responsibilities for implementation at all levels, and*	*COBIT PO6.8*

		the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies. Criteria for periodic re-evaluation of the framework should be defined to support responsiveness to changing organizational, environmental and technical requirements.	
P12	*External Requirements Review*	*The organization should establish and maintain procedures for external requirements review and for the coordination of these activities. Continuous research should determine the applicable external requirements for the organization. Legal, government or other external requirements related to IT practices and controls should be reviewed. Management should also assess the impact of any external relationships on the organization's overall information needs, including determination of the extent to which IT strategies need to conform with or support the requirements of any related third-parties.*	*COBIT PO8.1*
P13	*Electronic Commerce*	*Management should ensure that formal contracts are in place establishing agreement between trading partners on communication processes and on standards for transaction message security and data storage. When trading on the Internet, management should enforce adequate controls to ensure compliance with local laws and customs on a world-wide basis.*	*COBIT PO8.5*
P13.1	Electronic commerce security	*Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and on-line transactions across public networks such as the Internet. Electronic commerce is vulnerable to a number of network threats which may result in fraudulent activity, contract dispute and disclosure or modification of information. Controls should be applied to protect electronic commerce from such threats. Security considerations for electronic commerce should include the following:* *a) Authentication. What level of confidence should the customer and trader require in each others claimed identity?* *b) Authorization. Who is authorized to set prices, issue or sign key trading documents? How does the trading partner know this?* *c) Contract and tendering processes. What are the requirements for confidentiality, integrity and proof of despatch and receipt of key documents and the non-repudiation of contracts?* *d) Pricing information. What level of trust can be put in the integrity of the advertised price list and the confidentiality of sensitive discount arrangements?* *e) Order transactions. How is the confidentiality and integrity of order, payment and delivery address details, and confirmation of receipt, provided?* *f) Vetting. What degree of vetting is appropriate to check payment information supplied by the customer?* *g) Settlement. What is the most appropriate form of payment to guard against fraud?* *h) Ordering. What protection is required to maintain the confidentiality and integrity of order information, and to avoid the loss or duplication of transactions?* *i) Liability. Who carries the risk for any fraudulent*	ISO 17799 8.7.3

		transactions? *Many of the above considerations can be addressed by the application of cryptographic techniques, taking into account compliance with legal requirements. Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization. Other agreements with information service and value added network providers may be necessary. Public trading systems should publicize their terms of business to customers.* *Consideration should be given to the resilience to attack of the host used for electronic commerce, and the security implications of any network interconnection required for its implementation*	
P14	*Coordination and Communication*	*Management should establish a process for ensuring close coordination and communication between customers of the IT function and system implementers. This process should entail structured methods using the system development life cycle methodology to ensure the provision of quality IT solutions which meet the business demands. Management should promote an organization which is characterised by close cooperation and communication throughout the system development life cycle.*	*COBIT PO11.8*
P15	*Performance Procedures*	*Procedures should be put in place to ensure that the manner of and responsibilities for performance governing relations (e.g., non-disclosure agreements) between all the involved parties are established, coordinated, maintained and communicated to all affected departments.*	*COBIT DS1.3*
P16	*Monitoring and Reporting*	*Management should appoint a service level manager who is responsible for monitoring and reporting on the achievement of the specified service performance criteria and all problems encountered during processing. The monitoring statistics should be analysed on a timely basis. Appropriate corrective action should be taken and failures should be investigated.*	*COBIT DS1.4*
P17	*Availability and Performance Requirements*	*The management process should ensure that business needs are identified regarding availability and performance of information services and converted into availability terms and requirements.*	*COBIT DS3.1*
P17.1	Determing Availability requirements	*Determing the availability requirements of the business. Analyses are needed for the desired availability level.*	ITIL Availability Management 8.5.1
P17.2	Business Capacity Management	*Ensure that the business requirements for IT services are considered and understood, and that sufficient capacity to support the services is planned and implemented in an appropriate timescale.*	ITIL Capacity Management 6.2.1
P17.3	Capacity planning	*Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections should*	ISO 17799 8.2.1

		take account of new business and system requirements and current and projected trends in the organization's information processing. *Mainframe computers require particular attention, because of the much greater cost and lead time for procurement of new capacity. Managers of mainframe services should monitor the utilization of key system resources, including processors, main storage, file storage, printers and other output devices, and communications systems. They should identify trends in usage, particularly in relation to business applications or management information system tools.* *Managers should use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services, and plan appropriate remedial action.*	
P18	*Monitoring and Reporting*	*Management should implement a process to ensure that the performance of IT resources is continuously monitored and exceptions are reported in a timely and comprehensive manner.*	*COBIT DS3.3*
P18.1	Monitoring	*Monitors should be specific to particular parts of IT. This is needed to ensure the optimal use of the resources, to achieve the agreed service level and that business volumes are expected.*	ITIL Capacity Management 6.3.1
P18.2	Availability measurement and reporting	*The output of the Availability Management process is the measurement and reporting of IT Availability.*	ITIL Availability Management 8.7
P19	*Emergency Processing Priorities*	*Emergency processing priorities should be established, documented and approved by appropriate program and IT management.*	*COBIT DS10.5*
P19.1	Aspects of business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.	ISO 17799 11.1
P20	*Source Document Data Collection*	*The organization's procedures should ensure that all authorised source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry.*	*COBIT DS11.3*
P21	*Data Processing Integrity*	*The organization should establish procedures for the processing of data that ensure separation of duties is maintained and that work performed is routinely verified. The procedures should ensure adequate update controls such as run-to-run control totals and master file update controls are in place.*	*COBIT DS11.9*
P22	*Data Processing Validation and Editing*	*The organization should establish procedures to ensure that data processing validation, authentication and editing are performed as close to the point of origination as possible. When using Artificial Intelligence systems, these systems should be placed in an interactive control framework with human operators to ensure that vital decisions are approved.*	*COBIT DS11.10*

P23	*Processing Operations Procedures and Instructions Manual*	*IT management should establish and document standard procedures for IT operations (including network operations). All IT solutions and platforms in place should be operated using these procedures, which should be reviewed periodically to ensure effectiveness and adherence.*	*COBIT DS13.1*
P23.1	Documented Operating procedures	*The operating procedures identified by the security policy should be documented and maintained. Operating procedures should be treated as formal documents and changes authorized by management.* *The procedures should specify the instructions for the detailed execution of each job including:* *a) Processing and handling of information;* *b) Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;* *c) Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;* *d) Support contacts in the event of unexpected operational or technical difficulties;* *e) Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs;* *f) System restart and recovery procedures for use in the event of system failure.* *Documented procedures should also be prepared for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.*	ISO 17799 8.1.1
P24	*Collecting Monitoring Data*	*For the IT and internal control processes, management should ensure relevant performance indicators (e.g., benchmarks) from both internal and external sources are being defined, and that data is being collected for the creation of management information reports and exception reports regarding these indicators. Controls should also be aimed at validating the propriety and integrity of both organizational and individual performance measures and indicators.*	*COBIT M1.1*
P24	*Management Reporting*	*Management reports should be provided for senior management's review of the organization's progress toward identified goals. Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Upon review, appropriate management action should be initiated and controlled.*	*COBIT M1.4*
P25	*Internal Control Monitoring*	*Management should monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, reconciliations and other routine actions. Deviations should evoke analysis and corrective action. In addition, deviations should be communicated to the individual responsible for the function and also at least one level of management above that individual. Serious deviations should be reported to senior*	*COBIT M2.1*

		management.	
P25.1	Compliance with legal requirements	*To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.*	ISO 17799 12.1
IT infrastructure			
ID	**IT Control name**	**IT Control objective**	**Reference**
I1	*Information Architecture Model*	*Information should be kept consistent with needs and should be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities effectively and on a timely basis. Accordingly, the IT function should create and regularly update an information architecture model, encompassing the corporate data model and the associated information systems. The information architecture model should be kept consistent with the IT long-range plan.*	*COBIT PO2.1*
I1.1	Design and Planning	*Involves the development and maintenance of IS strategies for the deployment of infrastructure solutions to meet business needs.*	ITIL ICT Infrastructure Management
I2	*Data Classification Scheme*	*A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined.*	*COBIT PO2.3*
I3	*Technological Infrastructure Planning*	*The IT function should create and regularly update a technological infrastructure plan which is in accordance with the IT long- and short-range plans. Such a plan should encompass aspects such as systems architecture, technological direction and migration strategies.*	*COBIT PO3.1*
I4	*Technological Infrastructure Contingency*	*The technological infrastructure plan should be assessed systematically for contingency aspects (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure).*	*COBIT PO3.3*
I4.1	Activities in capacity management	*Specific activities must be undertaken when carrying out any of the sub-processes of capacity management.*	ITIL Capacity Management 6.3
I4.2	Availability planning	*Planning for availability must be made. Activities for planning the availability planning are needed.*	ITIL Availability Management 8.5
I4.3	Aspects of business continuity management	*To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.*	ISO 17799 11.1
I5	*Information Architecture*	*Management should ensure that attention is paid to the enterprise data model while solutions are*	*COBIT AI1.7*

		being identified and analysed for feasibility.	
I6	*Source Data Collection Design*	*The organization's system development life cycle methodology should require that adequate mechanisms for the collection and entry of data be specified for each information system development or modification project.*	*COBIT AI2.6*
I7	*Data Classification*	*Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived or deleted. Evidence of owner approval and data disposition should be maintained. Policies should be defined to support reclassification of information, based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between organizations, addressing both security and compliance with relevant legislation.*	*COBIT DS5.8*
I7.1	Classification guidelines	*Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, and the business impacts associated with such needs, e.g. unauthorized access or damage to the information. In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected. Information and outputs from systems handling classified data should be labelled in terms of its value and sensitivity to the organization. It may also be appropriate to label information in terms of how critical it is to the organization, e.g. in terms of its integrity and availability. Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to an unnecessary additional business expense. Classification guidelines should anticipate and allow for the fact that the classification of any given item of information is not necessarily fixed for all time, and may change in accordance with some predetermined policy. Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic to use or prove impractical. Care should be taken in interpreting classification labels on documents from other organizations which may have different definitions for the same or similarly named labels. The responsibility for defining the classification of an item of information, e.g. for a document, data record, data file or diskette, and for periodically reviewing that classification, should remain with the originator or nominated owner of the information.*	ISO 17799 5.2.1