UNIVERSITY OF OSLO
Department of Informatics

Sarbanes - Oxley Act of 2002 vs. The 8^{th} Company Law Directive

Iman Dagnew

Network and System Administration

Oslo University College

May 19, 2008

Sarbanes - Oxley Act of 2002 vs. The 8^{th} Company Law Directive

Iman Dagnew

Network and System Administration
Oslo University College

May 19, 2008

Abstract

In 2001 and 2002 a wave of corporate and accounting scandals became known to the public. As a direct consequence of these frauds the Sarbanes - Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002, was signed in to law. The main focus of Sarbanes - Oxley compliance is to ensure the accuracy of financial reporting and the systems that support this data. The law directly affected all US public traded companies and was costing millions to comply with. These costs led the European public companies to consider unlisting from the American stock market, not knowing that a European version (The 8^{th} Company Law Directive) of the Act would come into force four years later. This project will focus on the comparison of these two laws using promise theory as a model to better see the similarities and differences and understand the relationship between the affected parties of both laws in the eyes of promises. We will finally relate the Sarbanes - Oxley to technology, more specifically policy based configuration management.

Acknowledgments

First I would like to express my gratitude to my supervisor Mark Burgess, for giving me motivation, inspiration and suggestions during this work.

I would like to thank Kyrre Begnum for the fun talks and jokes, but also for the more serious critical questions asked to make this work better.

Thanks to ISPartner for giving me the time and understanding of what compliance on low level is.

I am grateful to my fellow students for the support through the two years master's program.

Special thanks to my family and friends for supporting and encouraging me through the tough times.

Last but not least I would like to thank mum and dad; this wouldn't be possible without you!

Oslo, May 2008

Iman Dagnew

Contents

Chapter 1

Introduction

1.1 Relevant background information

In 2001 and 2002 a wave of corporate and accounting scandals became known to the public. These scandals involved big companies like Enron, WoldCom and Adelphia amongst others.

Enron was a large American energy company which at that time was the worlds' leading electricity company. Late 2001 the company filed for what was considered to be the largest bankruptcy in US history. This bankruptcy cost 4000 employees their jobs and investors their savings. Months later WorldCom and Adelphia filed for bankruptcy caused by internal corruption. Investors lost billions of dollars and their confidence was badly shaken. Something had to be done.

The direct consequence of these scandals and in attempt to restore public confidence President George W. Bush signed the Sarbanes - Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002, into law, on July 30, 2002. The Sarbanes - Oxley Act also called SOX or Sarbox is named after its authors former Senator Paul Sarbanes and former Congressman Michael Oxley.

The main focus of Sarbanes - Oxley compliance is to ensure the accuracy of financial reporting and the systems that support this data. Even though Sarbanes - Oxley Act has been given large amount of attention, quite little has focused on the role of information technology in the financial reporting process. The Act requires that CEO's of public companies certify on the accuracy of the financial report and on the quality of the internal controls established which enable the accurate financial reporting. This certification will hold the executives accountable in case of investigations.

Within the public company all the employees are affected by this Act eventhough it may seem like most of the burden is laid on the management, internal auditors and the audit committee.

As most organizations are IT driven now days the Sarbanes - Oxley affects the IT department as much as the financial department and the certifying CEO. They might not be the ones imprisoned if mistakes occur in the financial

report, but the issue of compliance will depend on the support from IT. Documentation and being able to prove who did what, when, where and how is an important part of SOX. In the eyes of compliance it means that IT need to know exactly what is going on in their system. Any change made in the system, whether it is change of permission on files or any change made to a file, has to be documented so back trail is possible in case of audits. So even when the legislation is not specifically targeted IT, it has an impact on the IT system, mainly in the area of security.

IT also need to understand how their responsibilities for the computing system, that affect the financial reporting process, affects the certifying CEO and the business at large. Sarbanes - Oxley calls for wide range of financial controls, which all employees need to understand to be able to document their effectivness. Controls are only as good as the employees. So all employees need to know how the Sarbanes - Oxley relates to their daily work.

Before the passage of Sarbanes - Oxley, in case of financial fraud management could claim they did not know or understand what was going on. Sarbanes - Oxley has put a stop to that. Management have to certify on the effectiveness of the internal controls, which means they need to know what is going on, or be subject to the penalties defined in the Act. This of course puts pressure on the management or any other certifying employee for that matter, by relying on others to attest to the accuracy of the controls.

The legislation directly affects all US public traded companies, their employees and officers in U.S. It also affects auditors and audit firms auditing public companies. Non-US public companies listed in the U.S. also had to comply with the law. The legislation has set new standards on the transparency and responsibility of companies financial reports, which means CEOs and CFOs now have to state the responibility for establishing and maintaining an adecuate internal control structure and procedures for financial reporting and certify the accuracy and completeness of an annual financial report. They will also have to report on the effectiveness of the companies' internal control system and disclose material weaknesses in the system on annually bases. Furthermore companies are required to disclose information on material changes that could affect the companies' financial condition or operations, in real-time.

In the Enron scandal one of the Big Five accounting firm, Arthur Andersen was indicted for obstruction of justice for shredding documents related to the audit of Enron in 2001. This led to the end of Arthur Andersen leaving the accounting profession to what is now called the Big Four. The scandal of Arthur Andersen affected the accounting and audit profession in great extent. After the passage of Sarbanes - Oxley accounting firms and auditors were given certain criterias on how to audit public companies. Amongst other things auditor independence is given great attention in this Act. Any auditor carrying out audit for a public company must stay independent of that public company. No person or firm could now preform any auditing for any public company without being registered with the newly established Public Company Accounting Oversight Board. PCAOB was created by the Act to, amongst other things,

approve and keep a register of all public accounting firms and ”any associated person of that firm”.

SOX was and is still costing all public companies millions of dollars to comply with. And some non-US companies have even unlisted from the American Stock market, to avoid the cost of compliance. They did this not knowing that a European version of SOX would be implemented and require the same as the American original did six years ago.

The Directive on the Statutory Audits of Annual Accounts and Consolidated Accounts, also called The 8^{th} Company Law Directive was published in the Official Journal on 9 June 2006 and came into force on 29 June 2006. The Directive must be implemented by EU Member States by 29 June 2008. The directive is an expanded version of the 8^{th} Council Directive, which was adopted April 10, 1984 and mainly addressed the requirements on the approval of statutory auditors in EU member states. The new version addresses the requirements on how audits should be performed and calls for public oversight of the accounting profession.

The directive is considered to be the European version of Sarbanes - Oxley Act and sometimes also called Euro - SOX or E - SOX, while in fact “E - SOX” is a collection of several directives:

- The European Unions Financial Services Action Plan (FSAP)
- The 4^{th} directive Annual Accounts of spesific type of companies
- The 7^{th} directive Consolidated accounts
- The 8^{th} Company Law Directive
- The Transparency Directive
- The Market Abuse Directive
- The EU Data Protection Act

We will in this paper concentrate on the 8^{th} Company Law Directive which mainly focus on statutory audit and audit committee.

All European and non-European companies listed in the European Union have to comply with the directive. This means that auditors in third countries have to register with the European national board, just like European auditors have to register with the U.S Public Company Accounting Oversight Board. Companies listed in EU are directly affected by the directive.

During 2003 the EU finance minister called for exemption for EU audit firms from registrating with the PCAOB. Three years later the new Directive

was published. The EU Internal Market Commissioner Frits Bolkestein said on Sarbanes - Oxley:

"We in the European Union were faced with a simple choice: Either we could oppose tooth-and-nail the Sarbanes-Oxley Act and add yet another fiery dispute to our post-Iraq bilateral relations, or we could try to find a constructive, cooperative way forward, jointly respecting to the maximum degree possible our different legal traditions and cultures. We decided on the latter."

1.2 Promblem description

There are many similarities between Sarbanes - Oxley and the 8^{th} Comapany Law, but there are also differences. Both have the maninly same goal; to restore investor confidence after the wave of corporate scandals and accounting frauds which became publicly known from the late 2001. All these scandals had their roots in US, so it is only understandable that the Sarbanes - Oxley was published before the the 8^{th} Company Law.

Other main similarities between Sarbanes - Oxley and 8^{th} Company Law are;

- the need for indepenent public oversight of audit firms and the financial reporting process,
- to have an audit quality assurance system to test audit files and review compliance with appropriate auditing standards,
- to frequently rotate audit partner or audit firm,
- to avoid auditor conflict of interest by defining certain prohibited non-audit services.

On the other hand there are also the differences:

- The Sarbanes - Oxley Act implementation is based on the US Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework. Such a framework does not exist in Europe which makes implementation a difficult task.
- While there is a clear definition of ”significant deficiency” and a ”material weakness” in Auditing Standard No. 2, there is no such definition in Europe.
- In US public company management have to certify on the responsibility of establishing and maintaining internal control. There is no such certification required in Europe.
- For Sarbanes - Oxley compliance it is “Comply or Die”, while for the 8^{th} Company Law it is “Comply or Explain”.

After the passage of Sarbanes - Oxley all public companies listed in US have to comply with the Act or be subject to a strict penalty system. June 2008 is the deadline for implementation of the 8^{th} Comapany Law Directive by EU Member States. This means third country auditors and audit firms have to comply with the 8^{th} Comapany Law Directive, just like non-US have to comply with the Sarbanes - Oxley Act.

The issue we are trying to address by the present work is the need for public companies, auditors and audit firms to comply with both laws. We will study both documents to get a more detailed understanding of the similarities and differences in the laws. In this process we will use promise theory as a model, to get a clearer picture of what really distinguish them from each other. We will then try to relate the Sarbanes - Oxley to technology, more specifically configuration management.

1.3 Approach

To solve our problem defined in the previous section we will start by reading both the Sarbanes - Oxley Act and the 8^{th} Comapany Law Directive. Then we will try to categorize the laws so we can easily see the topics involved, and use it to compare the laws in general manner. Then we will try to look into detail in each topic or category of both laws and compare them to each other. Finally we will try to relate these laws to technology and configuration management in specific.

1.4 Thesis outline

Chapter 2 present related work in the area

Chapter 3 contains a case study on how ISPartner solved the challenge of Sarbanes - Oxley compliance.

Chapter 4 presents both the Sarbanes - Oxley and the 8^{th} Comapany Law. First a summarization of the main parts of the laws is provided. Then the different parties affected by the laws are described.

Chapter 5 gives an overview of the laws. Words used in both laws and throughout the thesis are explained here, and a general and overviewed comparison of both laws is given.

Chapter 6 describes Promise Theory model and shows how we used it to understand the concept of promise and compliance. This chapter also relates the laws discussed in the previous chapters to technology and more specific configuration management.

Chapter 7 concludes the work with suggestions for future work.

Chapter 2

Related research

This chapter is ment to give background information on research done to relate to the problem we are trying to solve in this work.

2.1 IT - business alignment

There have been several discussions on how IT affects the business part of the company. After the passage of Sarbanes - Oxley it has been even clearer. The Act requires for management to certify on the accuracy of the financial reports, which depends on the computing system of the company. For the management to certify on the accuracy of the reports with any certainty they need to include the IT department in the work of compliance. IT needs to understand the requirements by the Act and the management and contribute to the discussion on which computing processes and resources that will affect the financial reporting process.

[1] states that companies that have taken IT-business alignment seriously and have bought enterprise-wide configuration control and infrastructure relationship mapping solutions will find complying with the legislation much faster and easier. This is because these tools can be used to help control the constantly changing infrastructure so that the resources to the regulation stay in compliance.

In [2] alignment of helper technologies with business goals is discussed in the framework of promise theory. The paper states business are human-computer systems and addresses the issue of business alignment by abstracting away the humans and computers with generalized agents that make promises. Business promises are discussed to lead to an understanding of value or potential profit, and how such promises can be thought of as driver to achieve business goals. The paper further discusses how businesses can set value on their survival, and how promise theory can be used to model these values. To talk about alignment of an IT infrastructure to a business goal, the IT system has to have an impact on the business goal. The business must rely on the IT system in some way. The IT system is therefore an intermediate in the performance of a service, by the business to a client. Promise theory claims that an

agent cannot promise something to another agent it is not directly in contact with. The problem with intermediate agents is in this paper explored using promise theory.

2.2 Compliance with directives and best practices

After the passage of Sarbanes - Oxley there have been discussions on which and how to use best practices to be in compliance. Most companies and auditors are using COBIT (Control Objectives for Information and Related Technology) as standard to deal with compliance.

[3] and [4] both discuss the fact that there is no mentioning of the IT in the Sarbanes - Oxley Act. There is no specific mentioning of what controls need to be established within an IT organization to be in compliance with SOX. [4] mentions ITIL (IT Infrastructure Library), Six Sigma and COBIT as the best practices a company can use for defining and documenting its internal control. Further it states that most auditors have adopted COBIT as a standard for their SOX compliance, mostly because the COBIT standards are platform independent. The book helps to understand and shows how COBIT can be used as best practice to solve the compliance issues.

[3] gives guidance on how to improve the efficiency and effectiveness of compliance using a risk-based approach. This guidance is given to help companies in performing an IT risk assessment for Sarbanes - Oxley. Not all controls are relevant to all companies. Each company needs to decide and prioritize which is relevant for their organization. The paper gives therefore guidance to companies on the issue of defining "relevant controls". COSO's Internal Control-Integrated Framework has become the most commonly used framework by companies complying with Sarbanes - Oxley and it is used to help companies in ensuring the effectiveness of their financial, operational, and compliance-related internal controls. This paper gives an insight into COSO and its implications for IT. Cultural and people management issues is also addressed to highlight the human factors that need to be considered when complying with Sarbanes-Oxley.

Sarbanes - Oxley implementation is based on the COSO internal framework and it is recommended that COBIT is used as best practice. In Europe there is no COSO framework which makes it a challenge for companies to comply with the 8^{th} Comapany Law there.

2.3 Configuration Management

When it comes to configuration management issues in the eyes of compliance, [5] discusses policy based management as a way of influencing management behaviour within a system. Two types of policies are discussed ;

- *Authorisation policies*, which specify what activities a manager is permitted or forbidden to a set of objects,

- *Obligation policies*, which specify what activities a manager must or must not do to a set of objects.

Obligation models are like “laws”, where rules on what you should or should not do are specified. Roles have been used to model authority and responsibility within organizations. They are used as a means of grouping policies related to particular manager position and then managers can be assigned or removed from position without having to change the policies [5].

This way of management can be used to segregate duties and responsibilities in a company. By using role based management you specify the policies to positions in a company and assign it to the people in those positions. If an employee were to change position all you have to do is remove the person from that position. By not changing the policies every time changes in the system is needed you minimize the risk of flaw in the configuration.

The main problem when it comes to Sarbanes - Oxley or any other business “rules” is in the translating the high-level SOX directives into concrete low-level issues. This is like the ”policy continuum” in John Strassner’s DEN-ng model discussed in [6, 7, 8]. DEN-ng is being designed to help solving the problem by providing facilities to translate business rules and procedures of an organization to policies that configure and control the network.

This is where the promise method helps us by simple algebra, using dependency.

Chapter 3

Case study - ISPartner

To see how a real company interpreted SOX requirements and translated these into operational issues, we approached one that has just been through a SOX compliance process.

ISPartner is a provider of information system services to land-based and off-shore industrial companies. From January 2008 IS Partner is a part of EDB Business Partner, one of the leading IT groups in the Nordic region. One of the companies ISPartner provides services for is Hydro, which is a global provider of aluminum and aluminum products, with their base in Norway.

Since Hydro is listed in the US stock exchange market it is obliged to register with and report to the Securities Exchange Commission under the US Securities Exchange Act of 1934. After the passage of Sarbanes - Oxley Act in 2002 Hydro now also have to comply with the demanding legislation.

We were lucky enough to talk to an employee at ISPartner, to help us understand more on how businesses actually solved IT compliance according to Sarbanes - Oxley.

Truls Arne Nygård has been working at ISPartner for ten years now, and was part of the time consuming and costly transition to SOX compliance. About SOX he says: ”When the legislation first came to force no one really knew what needed to be done to be considered SOX compliant. No exact instructions were given on how to solve the new requirements for financial reporting process”. He continues to explain: ”The main purpose of the Sarbanes - Oxley is to prevent any attempt of manipulation of financial data, and detect fraud. It is important to keep this focus when thinking about risk management”.

Before Sarbanes - Oxley you could secure computers without necessarily thinking about why and how security measures were taken. In the post - SOX era on the other hand it is all about risk management. ”We had to identify the risks for manipulation of financial report data and fraud and then take any measures needed to minimize those risks. Any actions taken that would affect the financial reporting process now have to be explained”.

One of the ”Big Four” audit firms Deloitte Touche Tohmatsu was employed

as ISPartners audit firm, and handled the risk management when SOX first came to force. ISPartner decided to have the risk analysis evaluated by two of the other ”Big Four” audit firms; KPMG and Ernst Young. ISPartner found soon out that the three audit firms had different requirements for what they considered SOX compliance. ”The first year we used about 20 million Norwegian kroner to comply with the new legislation. We used about one million on auditing tools, licenses, software. We had to get extra machines to only use for SOX. We also had to employ two fulltime just to handle the extra work; monitoring and control testing, caused by SOX.

ISPartner use Control Objectives for Information and related Technology (COBIT) as framework for their IT management. “When defining controls it is important not to lose focus on the purpose and describe the controls too detailed”, Nygård explains”. Security has always been an important issue in all IT departments, but after the passage of SOX, security is considered even more important. The main goal is to secure everything that have affect on the financial report. It would therefore be a waste of time to define risk for files that do not affect the financial report in anyway.

”Too much security can harm more than it help, by creating mile long log files. It is important to have a realistic goal for handling log files otherwise too much time will be wasted reading unnecessary long log files. We limit our log filing to 3-4 logs each day. ”

Overall SOX has lead to more segregation and restriction. ISPartner use Role Based Access Control to limit access to files that could affect financial reports. Some employees have access all the time, another group in the working hours, while a third group of employees do not have any access at all. ”In general SOX has lead to a more secure environment”, Nygård concluded.

Talking to someone who has actually worked with the compliance of Sarbanes - Oxley made it easier for us to start understand the role of IT in SOX compliance. We realized that a lot of effort is spent understanding what compliance really means. We try therefore to see if we can make a model that will help us to understand and translate SOX guidelines into

- actions (actual changes),
- monitoring (assessing the status quo),

so that we can make certain statements about a human - IT system with knowable level of certainty.

Chapter 4

The Act & The Directive

To motivate a model we begin by summarizing the main parts of the Act and Directive. They are both arranged into titles and chapters categorized by content which makes it easier to summarize each title and chapter. This chapter will also summarize the responsibilities of the parties to which the laws are intended for.

4.1 The Sarbanes - Oxley Act

4.1.1 Summary of the Act

The Sarbanes - Oxley Act is arranged into eleven titles with different categorizes, and every title consists of several sections. The different titles describe the requirements for financial reporting and are categorized as follows;

- TITLE I - Public Company Accounting Oversight Board (PCAOB)
  - The first title establishes the public company accounting oversight board. The Board is reponsible for the registration of accounting frims and oversight of public auditors and audit firms.
- TITLE II - Auditor Independence
  - This title establishes the standards for external auditor independence. It describes the auditor reporting requirements, what services auditors and audit firms can perform for a public company and when audit partner rotation should be carried out.
- TITLE III - Corporate Responsibility
  - This title addresses the public companies responsibility for financial reports. Executives have to take the responsibility for the accuracy of corporate financial reports. It also describes the relation between external auditors and the companies audit committee.
- TITLE IV - Enhanced Financial Disclosure

  - This title describes the improved reporting requirements for financial reports. It requires executives and auditors to certify in annually reports the effectiveness of internal controls for financial reporting. Any change in the financial state of the company has to be disclosed for the public.

- TITLE V - Analyst Conflicts of Interest
  - This title consists of only one section, and is proposed to prevent conflicts of interest.

- TITLE VI - Commission Resource and Authority
  - Title VI authorizes SEC to have available fixed amount of money to fund different requirements, like salaries and benefits, information technology and hiring of qualified professionals. This title gives the SEC authorization to censure professionals for unethical or improper behavior.

- TITLE VII - Studies and Reports
  - This title requires studies and reports to be conducted on different matters, for example,
    * Study and report regarding consolidation of public accounting firms
    * Commission study and report regarding credit rating agencies
    * Study and report on violators and violations
    * Study of investment banks

- TITLE VIII - Corporate and Criminal Fraud Accountability
  - This title is also referred to as ”Corporate and Criminal Fraud Act of 2002”. It describes the penalties for fraud by altering, destroying, concealing or falsifying financial records. The title also provides protection for whistle-blowers.

- TITLE IX - White Collar Crime and Penalty Enhancement
  - The title is also called ”White Collar Crime Penalty Enhancement Act of 2002.” This title increases the penalties for white collar crimes. In particular the title adds failure to certify corporate financial reports as a criminal offense.

- TITLE X - Corporate Tax Returns
  - This title contains only one section stating that the chief executive officer should sign the company tax return.

- TITLE XI - Corporate Fraud Accountability

– This title defines tampering with records as a criminal offense and describes the specific penalty. The title gives SEC the authority to temporarily freeze large or extraordinary payments to management or employees.

4.1.2 The Securities Exchange Commission (SEC)

The Securites Commission was created when the Securities Exchange Act of 1934 was passed, to restore investor confidence after the stock market crashed in 1929. The Commissions mission is to protect investors, maintain fair, orderly and efficient markets. The Commission is composed of 5 presidentially-appointed commissioners. One of the commissioners is appointed as Chairman of the commission by the President.

The SEC responsibilities are many [9]:

- *"Interpret federal securities laws"*
- *"Issue new rules and amend existing rules"*
- *"Oversee the inspection of securities firms, brokers, investment advisers and ratings agencies"*
- *"Oversee private regulatory organizations in the securities, accounting and auditing fields"*
- *"Coordinate U.S. securities regulation with federal, state and foreign authorities"*

Since protecting the investors is one of the Commissions mission, it requires that all investors should have access to certain basic information/facts about an investment before buying it and so long as they hold it. Public companies are therefore required to disclose important financial information to the public. This gives the investors the knowledge they need to make investment decisions.

4.1.3 Public Company Accounting Oversight Board (PCAOB)

The Public Company Accounting Oversight Board (PCAOB) is established by the first section 101 in the first title. It is a non-profit corporation intended to oversee auditors and audit firms auditing public companies [10].

The board consists of five members, appointed by the Securities and Exchange Commission (SEC). The Securities Exchange Commission appoints the members after consultation with the Chairman of the Board of Governors of the Federal Reserve System and the Secretary of the Treasury.

The Act requires certain criteria for the selection of members of the board. It is required that two of the members be or have been certified public accountants. Further it requires that all members of the board serve on full time basis.

The Act defines the term service of each Board member to be 5 years, but limits persons from serving as chairperson or a member of the Board for more than 2 terms.

In 2004 the public company accounting oversight board created Office of Internal Oversight and Performance Assurance (IOPA) to provide internal examination of the operations of the PCAOB . IOPA conducts performance reviews and real-time quality assurance of PCAOB functions and programs [10]. Currently there are 1833 registered firms with the PCAOB.

The PCAOB is funded by mandatory fees that the public companies pay, but each registered public accounting firm has to pay registration and annual fees enough to recover the costs of processing and reviewing applications and annual reports.

In general the Commission has oversight and enforcement authority over the Board. For instance, a rule of the Board has to be approved by the Commission before it can become effective. The Commission has the authority to remove from office or censure any member of the Board, if it finds that such member has [11];

- *"violated the Act, the rules of the Board or the securities law,"*
- *"abused the authority of that member,"*
- *"failed to enforce compliance with rules or professional standard by any registered public accounting firm or any associated person."*

The Board has several duties [11];

- *"keep register of public auditors and audit firms that prepare audit for companies"*
- *"establish rules for auditing, quality control, ethics, independence and other standards"*
- *"carry out inspections of registered public accounting firms"*
- *"carry out investigations and disciplinary actions concerning public accounting firms and associated persons of such firms"*
- *"perform duties the Board or the Commission sees as necessary or appropriate to uphold high professional standard, improve the quality of audit services and carry out this Act"*
- *"enforce this Act"*
- *"set the budget and manage the function of the Board and the staff of the Board"*

4.1.4 The public companies

All US publicly traded companies and non-US public companies listed in the US have to comply with the Sarbanes - Oxley Act.

The most important sections which affect the management of public companies are 302 and 404.

According to section 302 CEOs and CFOs now have to personally certify that the financial reports are accurate and complete and state the responsibility for establishing and maintaining internal control structure and procedures for financial reporting.

Section 404 of the Act requires for annual report by the management on the effectiveness of the internal control structure and procedures for financial reporting, which also have to be attested by the external accounting firm preparing the audit report for the company.

4.1.5 The audit committee

Every public traded company has an audit committee, which consists of members of the board of directors of the company. The committee should otherwise be independent. The committee is responsible for overseeing the accounting and financial reporting processes and the audits of the financial statements of the company.

Section 301 (2) of the Act states that the audit committee should be directly responsible for the appointment, compensation and oversight of the work of the registered public accounting firm employed by that company.

Each registered public accounting firm performing an audit for a company is required to report to the audit committee of the company. Section 204 of the Act defines what should be reported.

Section 302 (4) requires the audit committee establish procedures on how to handle

- *"complaints received by the company regarding accounting, internal accounting controls, or auditing matters"*
- *"the confidentiality and anonymity of employees of the company for bringing up concerns regarding questionable accounting and auditing matters."*

4.1.6 The auditors and accounting firms

All accounting firms that carry out audits for public firms must register with the Public Company Accounting Oversight Board (PCAOB). Non - US accounting firms carrying out audits for public US companies also has to register with the Board.

Auditor independence is an important issue given great attention in the Sarbanes - Oxley, so accounting firms are therefore prohibited from providing non-audit services to the companies they are carrying out audits for. The prohibited services are listed in section 201.

Accounting firms can on the other hand engage in any non-audit service that is not listed in section 201 if it is approved in advance by the audit committee of the public company.

Accounting firms are required to rotate the audit partner (the partner in charge of the audit for a company), so that an accountant does not audit the same company for more than 5 years.

An accounting firm is required to report annually to the audit committee of the company. The reporting matter is described in section 204 of the Act.

4.2 The 8^{th} Company Law Directive

4.2.1 Summary of the Directive

The Company Law Directive is arranged into twelve chapters with different categories, and every chapter consists of several articles. The twelve chapters describe the requirements for financial reporting and are categorized as follows;

- CHAPTER I - Subject matter and definitions
  - This chapter explains the different definitions used throughout the Directive.
- CHAPTER II - Approval, continuing education mutual recognition
  - This chapter describes who may approve statutory auditors and audit firms and what conditions audit firms need to satisfy
- CHAPTER III - Registration
  - This chapter gives Member States the responsibility to ensure that auditors and audit firms are entered in a public register in accordance with the requirements.
- CHAPTER IV - Professional ethics, independence, objectivity, confidentiality and professional secrecy
  - In this chapter Member States are responsible to ensure that auditors and audit firms are subject to professional ethics. Member States should also make sure that auditors and audit firms performing an audit are independent of the audited company.
- CHAPTER V - Auditing standards and audit reporting

  - Chapter V contains three articles stating that Member States should require that auditors and auditing firms perform audits in compliance with international auditing standards. Member States should ensure that certain requirements are fulfilled in case of audit of consolidated accounts. When it comes to audit reporting it is required that the person performing the audit on behalf of the audit firm signs the audit report.

- CHAPTER VI - Quality assurance
  - This chapter contains only one article defining the criteria's a system of quality assurance need to meet to review auditors and audit firms. The quality assurance system review is supported by testing selected audit files to ensure compliance with auditing standards and independence requirements.

- CHAPTER VII - Investigations and penalties
  - This chapter states that there should be effective systems of investigations and penalties to detect, correct and prevent inadequate performance of audits. It also requires that penalties imposed on auditors and audit firms be appropriately disclosed to the public.

- CHAPTER VIII - Public oversight and regulatory arrangements between member states
  - This chapter describes the principles and the responsibilities that the system of public oversight should base on when reviewing auditors and audit firms. It is also described how professional secrecy and regulatory cooperation between Member States should be performed.

- CHAPTER IX - Appointment and dismissal
  - This chapter contains two articles describing how appointment and dismissal of auditors and audit firms should be handled.

- CHAPTER X - Special provisions for the statutory audits of public-interest entities
  - In this chapter Member States are responsible to ensure that auditors and audit firms that perform audits for public-interest companies publish annual transparency reports describing the legal structure and ownership, when the last quality assurance review took place and a list of public-interest companies the audit firm has carried out audits for the preceding financial year.
  - This chapter also establishes the audit committee that each public-interest company has to have. The committees' responsibilities are also defined here. Auditors and audit firms performing audits of public-interest companies, has to annually report to the committee.

- CHAPTER XI - International aspects
  - This chapter describes the requirements for approval, registration and oversight of third country auditors and audit entities.
- CHAPTER XII - Transitional and final provisions
  - This chapter defines the changes made in two other directives (Fourth Directive: annual accounts of companies with limited liability and Seventh Directive: consolidated accounts of companies with limited liability) as a result of this directive. In this chapter Member States are made responsible for adopting and publishing provisions necessary to comply with this Directive before 29 June 2008.

4.2.2 The European Commission

The European Commission consists of 27 Commissioners, one from each Member State. The Commissioners are appointed by the Member States and the President of the Commission. The body is responsible for proposing legislation, implementing decisions and the general day-to-day running of the Union. Eventhough the Commissioners are distributed between Member States they have to act in European interest and not their Member State.

4.2.3 European Group of Auditors' Oversight Bodies (EGAOB)

The European Group of Auditors' Oversight Bodies was established in 2005 by the European Commission. It is composed of representatives from the entities responsible for public oversight of auditors and audit firms in Member States.

Only non-practitioners can be designated as members of the EGAOB. In order to ensure input from the profession, the Commission will consult on the work of the group extensively and at an early stage with market participants, consumers, the audit profession and end-users in an open and transparent manner [12].

The decision on the establishment of the group was published in the Official Journal of the European Union on 16 December 2005 [13]. In this publication the tasks of the group, the composition and the appointment of the representatives is described.

The groups' tasks are mainly to [13]:

- *"facilitate cooperation between public oversight systems of Member States and to bring about an exchange of good practice concerning the establishment and ongoing cooperation of such systems;"*
- *"contribute to the technical assessment of public oversight systems of third countries and to the international cooperation between Member States and third countries in this area;"*
- *"contribute to the technical examination of international auditing standards, including the processes for their elaboration, with a view to their adoption at the community level."*

4.2.4 The public oversight system in Member States

Each Member state has to organize a system of public oversight for auditors and audit firms based on the principles laid out in Article 32 (2-7) of the Directive.

The public oversight system consists of non-practitioners who are knowledgeable in the areas relevant to statutory audit.

Article 32 (4) lists the responsibility of the public oversight system:

- approval and registration of auditors and audit firms
- adoption of standards on professional ethics, internal quality control of audit firms and auditing
- oversight of continuing education, quality assurance and investigative and disciplinary systems

Paragraph 5 of this article gives the system of public oversight the right to carry out investigations in relation to statutory auditors and audit firms and the right to take appropriate action.

The system of public oversight is transparent, and includes the publication of annual work programs and activity reports.

This Article requires that the adequate funding of the system is secure and free from any influence by statutory auditors or audit firms.

4.2.5 The audit committee

Article 41 of the Directive states that each public - interest entity should have an audit committee, which Member State determines the composition of. It is required though that at least one member of the audit committee should be independent and have competence in accounting and/or auditing. The committees' responsibility among other things is the monitor the financial process and effectivness of the company's internal control.

4.2.6 The auditors and audit firms

All auditors and audit firms have to be approved by Member States based on Chapter II of the Directive. An audit can only be carried out by auditors and audit firms who are approved by the Member State requiring the audit. So all auditors and audit firms have to be approved in all Member States they will be carrying out statutory audits.

Audit firms can only be approved if they satisfy the conditions laid down in Article 3 (4). If the fulfillment of the conditions should change, Member States should withdraw the approval, giving the audit firms a period of time to fulfill the conditions.

Natural persons who carry out audits on behalf of an audit firm has to satisfy the conditions laid down in Article 4 and 6 to 12 of the Directive. Article 6

to 12 describes the conditions regarding educational qualifications, examination of professional competence and practical training.

Each Member State should make sure that all auditors and audit firms are entered into a public register, which has to be fully operational by 29 June 2009.

Auditors and audit firms are required to stay independent of the audited company and are prohibited from carrying out an audit if they are already providing non-audit services to the company.

Article 42 (1) requires auditors and audit firms to annually confirm in writing to the audit committee on their independence from the audited company.

The key audit partner(s) responsible for carrying out an audit has to rotate every seven years from the date of appointment and can take part in the audit of the audited company again after at least two years.

4.2.7 Quality assurance

Article 29 states that all auditors and audit firms has to be reviewed by a system of quality assurance. The quality assurance system has to consist of persons with the appropriate education and relevant experience in statutory audit and financial reporting combined with specific training on quality assurance reviews. The system is funded securely and with no influence from auditors or audit firms. The quality assurance systems task is to test selected audit files and review the compliance with appropriate auditing standards and independence requirements. The quantity and quality of the resources spent, the audit fees charged and the internal quality system of the audit firm will also be reviewed by the quality assurance system. The quality assurance review will be reported with the main conclusions of the review.

For auditors and audit firms carrying out audits of public-interest companies quality assurance reviews has to take place at least every three years, but the overall result of the quality assurance system should be published annually. The quality assurance system already exist in some EU Member States.

Chapter 5

Overview

This chapter will first give an explanation on the definitions used in both documents to better understand the meaning of the text, and then a general and overviewed comparison on the main topics of the laws is presented.

5.1 Definitions

Both documents use definitions we need to explain to understand the meaning of the text. Some definitions are similar in both documents but there are also different definitions used in the documents describing the same concept. More detailed explanation on the definitions can be found in the documents [11, 14]

- *Audit* - means a review of the financial account of any entity by an independant auditor or audit firm.
- *Statutory auditor* (EU Directive) - means a natural person approved to carry out audits.
- *Audit firm* (EU Directive) - means a legal person or any other entity that is approved to carry out audits.
- *Public accounting firm* (Sarbanes - Oxley) - means any legal entity that practice public accounting or prepare or issue audit reports.
- *Audit report* - is a document or any other record prepared by auditors or audit firms.
- *Public-interest entity* (EU Directive) - *"means entities governed by the law of a Member State whose transferable securities are admitted to trading on a regulated market of any Member State"* [14].
- *Issuer* (Sarbanes - Oxley) - means any person who issues or proposes to issue any security and that file reports with the Securities Exchange Commission.

- *Audit committee* - in the EU directive the committee is appointed by the general meeting of shareholders of the audited entity, while in Sarbanes - Oxley the committee is established by and amongst the board of directors of the audited entity. The committees' purpose is amongst others to oversee the financial reporting process of the entity.

5.2 Comparison

5.2.1 Registration of auccounting firms, auditors and audit firms

All accounting firms carrying out audits for public companies are required to register with the Public Company Accounting Oversight Board. The Board requires names of the companies the accounting firm has prepared audits for the previous year and expects to prepare audit for during the existing year. Annual fees received from companies for audit, services, other accounting services and non-audit services should also be registered with the Board. The accounting firm additionally has to submit a statement of the quality control policies of the firm for its accounting and auditing practices. The Board requires a list of all the accountants associated with the accounting firm who participate or contribute to the preparation of audit reports.

Also in Europe there need to be a registration of auditors and audit firms carrying out audit for public interest companies. Member States are responsible for keeping a register of auditors and audit firms. The registration information should be stored in electronic form and be accessible to the public. Name, address and registration number of both auditors and audit firms is some of the information the public register shall contain. Audit firms registered has to list the name and registration number of the auditors associated with the audit firm. Third - country auditors and audit firms should be registered in according to Article 45 of the Directive and it should be clearly indicated in the register as such and not as auditors and audit firms.

5.2.2 Audit committee

After the passage of the Sarbanes - Oxley Act having an audit committee has become a mandatory requirement for public companies. The Act defines the audit committee as followed:

"a committee (or equivalent body) established by and amongst the board of directors of an issuer for the purpose of overseeing the accounting and financial reporting processes of the issuer and audits of the financial statements of the issuer".

If no such committee exists the Act states that the whole Board is considered as the audit committee. The members of the audit committee should otherwise be independent from the company.

Section 301 makes sure that the independence between the external auditor and the audited company is kept by giving the audit committee responsibility of appointing out the external accounting firm. The audit committee is further responsible of overseeing the work done by the accounting firm employed by the company, whether it is audit report or related work. The registered public accounting firm should report directly to the audit committee. The committee determines the fees that should be provided to the public accounting firm for audit related work performed for the company.

Section 204 of the Act states that each public accounting firm performing audit for a company should timely report to the audit committee of the company. If there should occur any disagreements between the accounting firm and the management of a company on audit matters the audit committee should be involved. Any material written communication between the accounting firm and the management is also to be disclosed to the audit committee.

The audit committee is also responsible of having procedures on how to handle whistle blowing matters.

Also in Europe public companies are required to have audit committee. The compensation of the committee is determined individually by Member States as mentioned in the directive:

"The Member State shall determine whether audit committees are to be composed of non-executive members of the administrative body and/or members of the supervisory body of the audited entity and/or members appointed by the general meeting of shareholders of the audited entity."

At least one member has to be independent and have competence in accounting and/or auditing.

Article 41 defines the audit committees' responsibilities as followed:

- *"monitor the financial reporting process;"*
- *"monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems;"*
- *"review and monitor the independence of the auditor or audit firm, and in particular the provision of additional services to the audited entity."*

Auditor and audit firm has to report to the audit committee on "key matters" arising from the audit and especially on material weaknesses in internal controls affecting the financial reporting process.

Article 37 of the directive states that auditor or audit firm should be appointed by the general meeting of shareholders or members of the audited entity, based on a recommendation made by the audit committee.

Auditors and audit firms confirm annually to the audit committee on their independence from the audited company. Any additional services provided to the audited company should also be reported annually to the audit committee.

5.2.3 Auditing, quality control, and independence standards and rules

PCAOB is responsible for the establishment and adoption of auditing standards. The following standards and related rules has been adopted by the Board and approved by the Securities Exchange Commission [10]:

- *Auditing Standard No. 1: References in Auditors' Reports to the Standards of the Public Company Accounting Oversight Board*
- *Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements*
- *Auditing Standard No. 3: Audit Documentation*
- *Auditing Standard No. 4: Reporting on Whether a Previously Reported Material Weakness Continues to Exist*
- *Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements*
- *Interim Standards: Pre-existing standards adopted by the Board as its interim standards to be used on an initial, transitional basis.*
- *Interim Standards: Pre-existing standards adopted by the Board as its interim standards to be used on an initial, transitional basis.*
- *Rule 3100: Compliance with Auditing and Related Professional Practice Standards*
- *Rule 3101: Certain Terms Used in Auditing and Related Professional Practice Standards*
- *Rules 3501, 3502, and 3520 to 3524: Ethics and Independence Rules and Related Information Concerning Independence, Tax Services, and Contingent Fees*
- *Rule 3525: Audit Committee Pre-Approval of Non-Audit Services Related to Internal Control Over Financial Reporting*

Auditors and audit firms in Europe are required to carry out audits in compliance with international auditing standards adopted by the European Commission. Two important sets of standards have been adopted internationally. The International Accounting Standards, now called International Financial Reporting Standards (IFRS), developed by the International Accounting Standards Committee (IASC) and the auditing standards developed by the International Auditing Practices Committee (IAPC) of the International Federation of Accountants (IFAC).

5.2.4 Rotation

While Sarbanes - Oxley only requires for the rotation of lead or coordinating audit partner (the person primarily responsible for the audit) every five years, the 8^{th} Company Law requires for key audit partner rotation every seven years. In addition Member States can if they find it appropriate require for the rotation of audit firm.

Audit partner rotation has been the solution to the issue on auditor independence in both US and Europe. But the 8^{th} Company Law can also require for audit firm rotation which raises the issue on audit quality. Effective audits require deep understanding of the company, which is lost if the audit firm rotate. [15] claims that in the US, statistical evidence suggests that audit failures occurred almost three times as often when the auditor was performing the audit for the first or second year.

5.2.5 Competent authority

Sarbanes - Oxley specifies the different authorities which are required to approve, register, inspect, oversee and investigate registered accounting while the 8^{th} Company Law addresses the ”competent authority” in general. In Sarbanes - Oxley PCAOB is mostly responsible for the upper mentioned tasks, while in Europe, Member States designate these tasks to one or more competent authorities, as long as conflict of interest is avoided and the Commission is informed.

	The 8th Company Law Directive	**The Sarbanes - Oxley Act of 2002**
Approval, continuing education and mutual recognition of statutory auditors and audit firms	Public oversight systems approves auditors and audit firms if conditions laid down in Article 3(4) to 10	PCAOB approves auditor firms after reviewing application for registration with deails the Board specify in section 102(b)
Registration of statutory auditors and audit firms	Public oversight systems in Member States register auditors and audit firms with the information required in Article 16 and 17	PCAOB registers public accounting firms in accordance with section 102
Professional ethics, independence and objectivity	Auditors and audit firms are subject to principles of professional ethics. When carrying out audit they have to be independent of the audited entity(Article 22)	Audit firms are required to maintain professional ethics and independence of the audited entity
Auditing standards	Audits are required to be carried out in compliance with international auditing standards adopted by the Commission (Article 26)	Section 103 requires PCAOB to establish auditing, quality control and ethics standards and rules to be used by registered public accounting firms
Audit reporting	Audits carried out by audit firms has to be signed by the auditor carrying out the audit on behalf of the audit firm	
Quality assurance systems	Auditors and audit firms has to be subject to quality assurance systems wich meets the criterias laid down in Article 29	The PCAOB inspects auditors and audit firms to review the compliance with the Act, the rules of the Board or professional standars (Section 104)
Public oversight	Member States are responsible of oganizing a public oversight system to review auditors and audit firms. The reviews are based on principles laid down in Article 32, paragraphs 2 to 7	PCAOB oversees audit of public companies and conduct inspections and investigation of registered public accounting firms

Table 5.1: Overview of the requirements in Sarbanes - Oxley and the 8th Company Law

5.3 Summary

Both Sarbanes - Oxley and the 8^{th} Company Law require for the registration of accounting firms, auditors and audit firms performing audits for public interest companies. PCAOB is responsible for the approval and registration of accounting firms, while public oversight systems approves auditors and audit firms and make sure that they are kept in a register.

The 8^{th} Company Law Directive defines specific requirements the auditors and audit firms need to satisfy before they can be approved. These requirements are among other things the need for continuing education of auditors in order for them to maintain their theoretical knowledge, professional skills and values at a high level. The Sarbanes - Oxley does not address the educational requirements of the accounting firms in the Act.

Audit committee is a requirement for public interest companies, in both the Sarbanes - Oxley and the 8^{th} Company Law. The audit committee is responsible for the oversight of the company's financial reporting process as well as the oversight of internal and external audit work papers. The accounting firms, auditors and audit firms report directly to the company's audit committee annually. Independence between the company and accounting firm, auditor and audit firm is kept by giving the audit committee the responsibility for the appointment of the external accounting firm, auditor and audit firm.

Sarbanes - Oxley gives the public company accounting oversight board the responsibility to establish auditing, quality control, ethics, and independence standards and rules to be used by registered accounting firm performing audit of public interest companies. The Board has set up a Standing Advisory Group (SAG) to advise the Board on the establishment of auditing standards.

In US accounting firms mainly use the Generally Accepted Accounting Principles (GAAP) as a standard framework of guidelines for financial accounting. In Europe, all EU listed companies are required to use International Financial Reporting Standards (IFRS) adopted by the International Accounting Standards Committee (IASC).

Sarbanes - Oxley require for audit partner rotation every five years, while in Europe rotation of audit partner is required to occur seven years. In addition Member State can require for the rotation of audit firm if it finds it necessary.

PCAOB is established by Sarbanes - Oxley to approve, register, inspect, investigate and sanction accounting firms. In the 8^{th} Company Law there is no single entity defined, responsible of all the upper mentioned tasks. Member States designate these tasks to one or more competent authorities.

Chapter 6

A Model for Compliance

We need a model by which to compare the legal documents described so far in the foregoing chapters. There are several models one might use for documtents. e.g.

- DOM - The document object model, takes an OO view of a document as used in web browsers.
- Taxonomy - another hierarchical description of subjects
- Topic Maps - a non-hierarchical descripion of concepts and relationships with a generalized ontology, which places ”topics” or concepts as the most important entities
- Promise theory - a model of properties and constraints based on a generalized ontology of ”promises made by agents” which places individual agents as the most important entities.

Taxonomy and OO are not rich enough to capture the relationships in a general organization as they are fundamentally hierarchical, but organizations are not. In principle both Topic Maps and Promises could be used, but we choose promises because they focus on the responsible agents for compliance with policy. This results in a more practical model for implementing compliance.

6.1 Introduction to Promises

6.1.1 Concepts

Promise theory is a language for describing and understanding the relationship between autonomous ”agents” [2]. Agents are considered autonomous if they cannot be forced to make any promises about their behavior by any other agent.

Agents are entities that can make promises, receive promises and evaluate the value of promises.

A promise consists of a

- promiser,
- promise body, which contains a description of what the promise is about
- promisee

In promise theory agents can only make promises about their own behaviour. They cannot make promises on other agents' behaviour.

A promise is made by a promiser to a promisee

$promiser \xrightarrow{b} promisee$

The body b contains a description of what the promise is about.

$A \xrightarrow{+b} C$

$C \xrightarrow{-b} A$

Because agents are autonomous there is no obligation for C to accept a promise given by a A. C must therefore explicitly promise to accept b. A promise with body +b is a promise made to C , while -b is a promise from C to accept the promise from A.

A promise can also be a conditional promise, which means that a promise is only made if a condition is met. If a promise is made conditionally it is not considered a promise, unless the condition is also promised [2].

Let us assume agent A want to make a promise π to agent B (Figure 6.1). Let us further assume that agent A is making the promise to B dependent on an intermediary third agent C. A would therefore be making a promise to B on the condition that it gets what it has been promised ρ by C. For this to be considered a promise, A also has to promise B that it will "use" the promise ρ given to it by C (Figure 6.2).

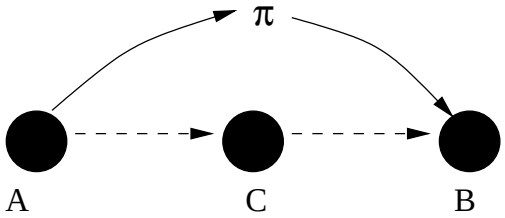

Figure 6.1: A want to promise π to B, but has an intermediate agent C it depends on. Promise theory says A has to have direct contact to B to promise π. Dotted lines show the work flow.

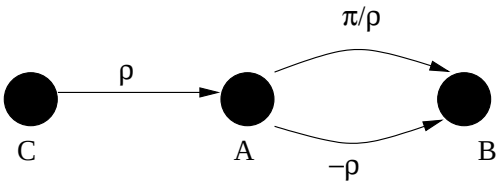

Figure 6.2: C promise ρ to A. A makes a conditional promise π/ρ, and a promise to "use" $-\rho$ the promise given to it by C, to B.

6.1.2 Voluntary cooperation

Every agent either it is human, computer or any part of a system that can change independently is said to be autonomous if it cannot be forced to make any promise about their behaviour. All promises are made voluntarily. At first this may seem like a disadvantage (to assume that we cannot enforce policy) but in fact this assumption is a strength as it forces us to confront the uncertainties involved in getting the parts of a system to comply with policy. Indeed, we have to ask: what promises do agents need to make in order to be able to say with confidence that they will behave in the desired fashion?

6.1.3 Valuation of promises

In promise theory agent can evaluate a promise that it makes or receives [2]. The perceived value tells us why an agent might make or keep a promise or not. Since agents are considered autonomous, each agent must make its own decision about what promises are worth and how much they cost. Agents might measure value differently. Some agents might measure value in currency, but any kind of beneficial trade can be used as a measure for value. This could be in the form of goods, reputation, or goodwill. A valuation of a promise made or received can be written as a function:

$$\mathrm{v}_A(A \xrightarrow{b} C)$$

$$\mathrm{v}_C(A \xrightarrow{b} C)$$

6.2 Promises in Sarbanes - Oxley and the 8^{th} Company Law

To apply promise theory to Sarbanes - Oxley and the 8^{th} Company Law we have to first define the agents in both laws. Promise theory defines agents as *"any and every part of a system that can change independently, or keep independent information"*[16]. Using this definition we defined our agents from both Sarbanes - Oxley and the 8^{th} Company Law (Table 6.1).

Sarbanes - Oxley Act	**Symbol**	**The 8^{th} Company Law**	**Symbol**
Securities Exchange Commission	SEC	Member States	MS
Public Company Accounting Oversight Board	PCAOB	European Group of Auditors' Oversight Bodies	EGAOB
Public company	PC	Public oversight system	POS
Audit committee	AC	Quality assurance system	QAS
Accounting firm	AF	Public compay	PC
State regulatory authority	SRA	Audit committee	AC
Public	P	Auditor/Audit firm	AF
IT system	IT	Public	P
Chief Executive Officer	CEO	System of Investigation and Penalties	SIP
Chief Financial Officer	CFO		
Chief Information Officer	CIO		
Chief Security Officer	CSO		

Table 6.1: Agents defined from Sarbanes - Oxley and the 8^{th} Company Law.

In the process of defining the agents in Sarbanes - Oxley and 8^{th} Company Law we had to read the text in both documents in detail to recognize an agent by the above given definition. The agents were easier to spot in Sarbanes - Oxley than in the 8^{th} Company Law. In Sarbanes - Oxley every entity responsible for compliance is addressed and specified. In the 8^{th} Company Law there are no specific entities defined to deal with the responsibilities. It only states that Member States are responsible for having the appropriate competent authorities to handle the different tasks. In Sarbanes -Oxley the Commission, PCAOB, audit committee, public companies are addressed. And even CEOs and CFOs are mentioned as responsible entities within the public company. In the 8^{th} Company Law the entities are mentioned more general; public oversight system, quality assurance system, system of investigation and penalties. We decided therefore to use the same terms used in the law as agent names.

Also when making the diagrams we had to decide how we would look at the promises and relationship between the agents. We had to decide which promises we wanted to address and from which agents' perspective we wanted to look at the promises.

6.2.1 Agents and promises in Sarbanes - Oxley

We can see in Figure 6.3 the relationship and promises between the agents we defined from the Sarbanes - Oxley Act. Table 6.2 is a summary of promises between agents on Figure 6.3.

The Pubplic Company Accounting Oversight Board (PCAOB) is responsible for the approval and registration of auditors and audit firms. They also carry out investigation and disciplinary actions concerning accounting firms.

The promise with body *+a* indicates the promise made to the SEC by PCAOB. PCAOB promises to report to SEC on investigations carried out concerning accounting firms. Any disciplinary actions taken are also notified to the SEC. *-a* is the promise by the SEC to accept the promise given by the PCOB and is responsible for the oversight of the Board.

Accounting firms carrying out audits for public companies must register with the PCAOB.

Promise *+b* from the accounting firm to the PCAOB is a promise to register with the Board before being able to carry out audits for public companies. *-b* indicates that the PCAOB promise to accept b and approve and register the accounting firm. Promise *+c* is a promise, by the accounting firm to the PCAOB, to provide audit files. The Board promise *-c* to accept the promise given by the accounting firm and inspect the audit files provided to it. *+d* is a promise from the accounting firms to provide cooperation in investigations. *-d* is a promise to accept the cooperation given and carry out investigations of accounting firms when needed.

If PCAOB were to identify any violations related to audit files inspected written reports have to be transmitted to the SEC and each appropriate state regulatory authority. The report should also be available to the public.

Accounting firms are required to report annually directly to the audit committee of the audited company. Audit committee is responsible for overseeing the accounting and financial reporting process. It oversees the audits of the financial statements of the company. The audit committee is also responsible for appointing out and overseeing the work of the accounting firm employed by the company.

The promise *+e* from the accounting firm to the audit committee is a promise to annually report to the committee. *-e* is a promise to accept the promise and oversee the work of the accounting firm.

+f is a promise from the public company to report to their audit committee. *-f* is a promise from the audit committee to accept the promise and oversee the public company.

Public companies listed in the US must file financial reports with the SEC. Important sections in the Act when it comes to the financial reports are 302 and 404. These sections require the CEO and CFO to certify on the accuracy and completness of the financial statements. A more detailed diagram on section 302 can be seen on Figures 6.11 and 6.12.

Symbol	**Interpretation**	**Text**
$PCAOB \xrightarrow{+a} SEC$	Promise from *PCAOB* to *SEC* with body *a*	PCAOB report to SEC on actions taken
$SEC \xrightarrow{-a} PCAOB$	Promise to accept *a*	SEC oversees the PCAOB
$AF \xrightarrow{+b} PCAOB$	Promise from *AF* to *PCAOB* with body *b*	Accounting firms register with the PCAOB
$PCAOB \xrightarrow{-b} AF$	Promise to accept *b*	PCAOB approve and register accounting firms
$AF \xrightarrow{+c} PCAOB$	Promise from *AF* to *PCAOB* with body *c*	Accounting firms provide PCAOB with audit files
$PCAOB \xrightarrow{-c} AF$	Promise to accept *c*	PCAOB inspect audit files of accounting firms
$AF \xrightarrow{+d} PCAOB$	Promise from *AF* to *PCAOB* with body *d*	Accounting firms provide cooperation in investigations
$PCAOB \xrightarrow{-d} AF$	Promise to accept *d*	PCAOB carry out investigation of accounting firms when needed
$AF \xrightarrow{+e} AC$	Promise from *AF* to *AC* with body *e*	Accounting firms report annually to the audit committee
$AC \xrightarrow{-e} AF$	Promise to accept *e*	Audit Committee oversees the work of the accounting firm
$PC \xrightarrow{+f} AC$	Promise from *PC* to *AC* with body *f*	Public companies report to their audit committee
$AC \xrightarrow{-f} PC$	Promise to accept *f*	audit committee oversees the public company

Table 6.2: Sumary of promises between agents in Sarbanes - Oxley.

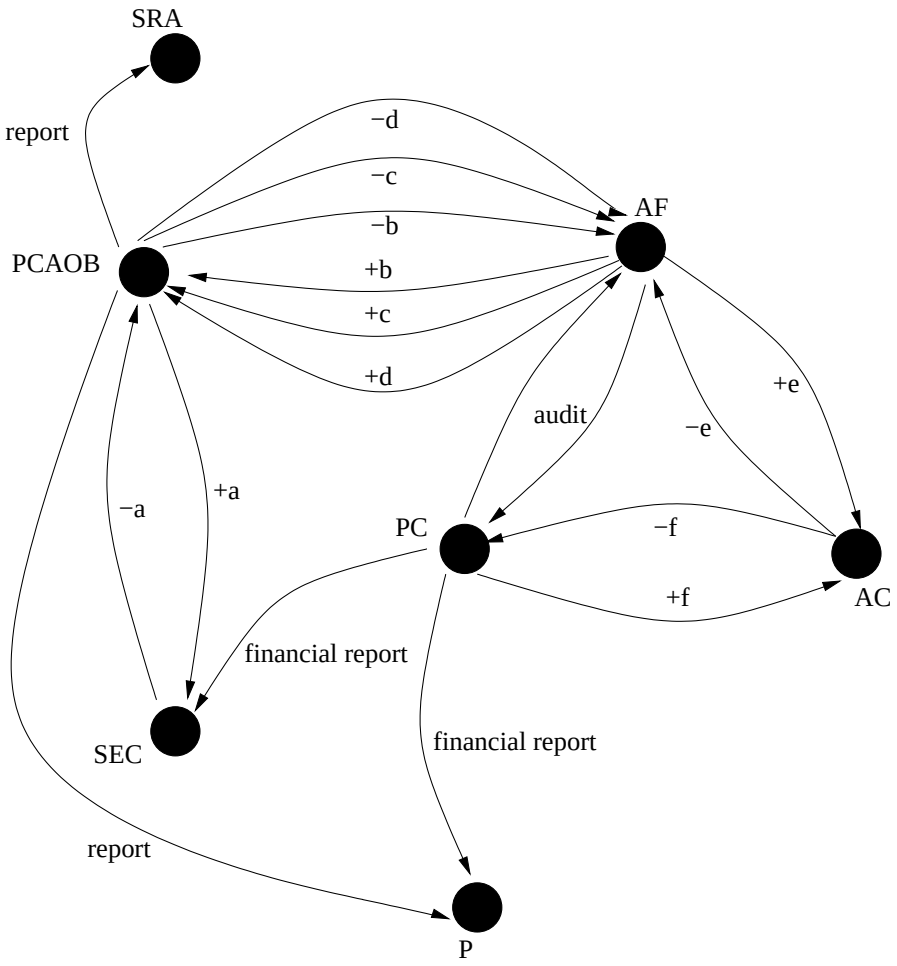

Figure 6.3: Relationship between agents in Sarbanes - Oxley.

6.2.2 Agents and promises in 8^{th} Company Law

Figure 6.4 shows the relationship and promises between agents we defined from the 8^{th} Company Law. Table 6.3 is a summary of the promises between the agents on Figure 6.4.

The European Group of Auditors' Oversight Bodies (EGAOB) was established to ease the cooperation between public oversight systems of Member States.

The promise *+a* from the EGAOB to the public oversight systems of Member States indicates the promise to help the cooperation between public oversight systems in Member States. *-a* is a promise by public oversight systems to accept promise and cooperate across Member States.

Auditors and audit firms are required to be approved and registered to be able to carry out audits for public companies. Public oversight systems are responsible for approving and keeping a register of auditors and audit firms performing audits of public interest companies.

Auditors and audit firms promise, *+b*, to register with the public oversight system to be able to carry out audit. Public oversight systems promise to accept the promise, *-b*, and approve and register auditors and audit firms.

Auditors and audit firms carrying out audits for public companies have to be subject to inspection by a quality assurance system. The quality assurance system inspects auditors and audit firms by testing selected audit files. A finally report with main conclusions of the review should be written.

The promise *+c* is a promise by the audit firm to provide the quality assurance system with audit files in case of inspections. The quality assurance system promise to accept the promise, *-c* and inspect the audit files of the audit firm.

If any recommendations of quality reviews made by the quality assurance system is not followed up by the auditor or the audit firm within a reasonable period the auditor or the audit firm shall be subject to a system of disciplinary actions or penalties. Any penalties imposed auditors and audit firms has to be disclosed to the public.

Auditors and audit firms promise, *+d*, to cooperate with systems of investigation and penalties in investigations. The system of investigation and penalties promise to accept *d* and carry out investigation of auditors and audit firms when needed.

Auditors and audit firms report directly to the company's audit committee. Auditors and audit firms promise, *+e*, to annually report to the audit committee of the audited company on "key" matters arising by an audit. The audit committee promises to accept the promise, *-e*, and oversees the work of the auditors and audit firms.

The audit committee monitors the company's financial reporting process and the effectiveness of the company's internal control, internal audits and risk management.

+f is promise to report to their audit committee, made by the public company. The audit committee promise to accept this promise, *-f*, and monitors the public company.

Public companies must make public its annual and half - yearly financial report.

Symbol	Interpretation	Text
$EGAOB \xrightarrow{+a} POS$	Promise from *EGAOB* to *POS* with body *a*	EGAOB helps the cooperation between public oversight systems in Member States
$POS \xrightarrow{-a} EGAOB$	Promise to accept *a*	Public oversight systems cooperate across Member States
$AF \xrightarrow{+b} POS$	Promise from *AF* to *POS* with body *b*	Audit firms register with the public oversight system
$POS \xrightarrow{-b} AF$	Promise to accept *b*	Public oversight systems approve and register audit firms
$AF \xrightarrow{+c} QAS$	Promise from *AF* to *QAS* with body *c*	Audit firms provide the quality assurance system with audit files
$QAS \xrightarrow{-c} AF$	Promise to accept *c*	The quality assurance system inspect audit files of audit firms
$AF \xrightarrow{+d} SIP$	Promise from *AF* to *SIP* with body *d*	Auditors and audit firms provide for cooperation in investigations
$SIP \xrightarrow{-d} AF$	Promise to accept *d*	System of investigation and penalties carry out investigation of auditors and audit firms when needed
$AF \xrightarrow{+e} AC$	Promise from *AF* to *AC* with body *e*	Auditors and audit firms report annually to the audit committee
$AC \xrightarrow{-e} AF$	Promise to accept *e*	audit committee oversees the work of the auditors and audit firm
$PC \xrightarrow{+f} AC$	Promise from *PC* to *AC* with body *f*	Public companies report to their audit committee
$AC \xrightarrow{-f} PC$	Promise to accept *f*	audit committee monitor the public company

Table 6.3: Sumary of promises between agents in 8^{th} Company Law.

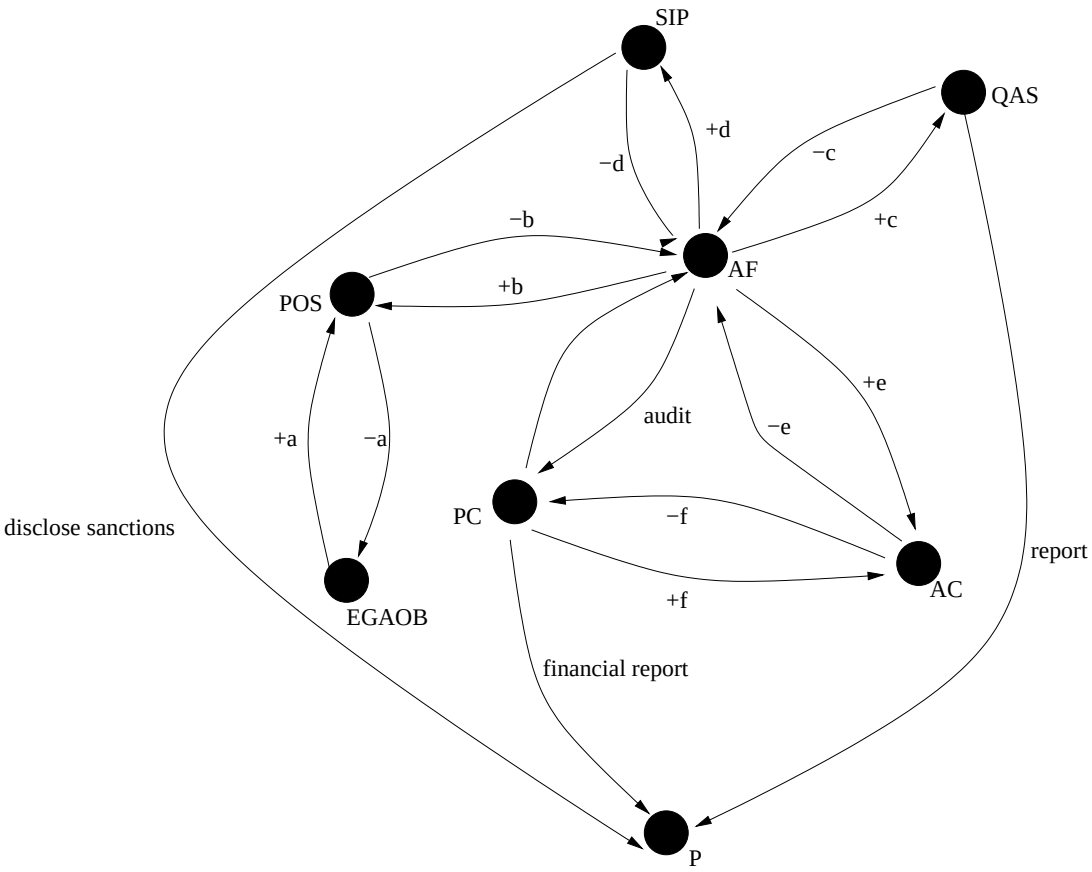

Figure 6.4: Relationship between agents in the 8^{th} Company Law.

6.2.3 Summary

We can clearly see by looking at Figure 6.3 that a lot of responsibility is given to the accounting firm and PCAOB. These responsibilities are mainly to each other. The PCAOB is given the responsibility to approve, register, inspect, investigate and sanction accounting firms auditing public interest companies. All accounting firms are required to register with the PCAOB and provide for audit work papers in case of inspection and investigations.

Looking at Figure 6.4 we see that the responsibilities to approve, register, inspect, investigate and sanction auditors and audit firms are widely spread amongst the ”agents”. This is because no single entity is established in EU to handle all these tasks. Each Member State is responsible of assigning the tasks to one or more competent authorities. The Member State has to make sure that conflict of interest is avoided when designating tasks, and inform the Commission on the different competent authorities responsible of the different tasks. The Directive defines the

- *public oversight system* for the approval and registration of auditors and audit firms,

- *quality assurance system* for the inspection and review of auditors and audit firms,

- *system of investigations and penalties* to detect, correct and prevent insufficient execution of audits.

By looking at Figure 6.4 we can see that the AF agent is given a lot of the responsibility. The AF agent is connected to almost every other agent and we can see clearly see that AF is the most connected agent. This raises the question if agent AF is a target for corruption.

While PCAOB is responsible for all the registration, oversight, inspection and investigation of accounting firms in Sarbanes - Oxley (Figure 6.3), these responsibilities are spread to different systems by Member States in the 8^{th} Company Law. This gives a segregation of duties which is considered as positive in many cases. Giving all responsibility for the oversight of accounting firm to one entity does minimize the amount of systems needed to do the different tasks. This does also mean that the particular entity in charge is overloaded with work.

Now lets look at the relationships and promises showed in Figure 6.3 and 6.4 in detail.

6.2.4 Section 104: Inspection of registered public accounting firms

PCAOB is responsible of inspecting the registered accounting firms. The Board inspects and reviews selected audits and review engagements of the firm and evaluate adequacy of the quality control system of the firm. We have shown this as promise *-c* in Figure 6.5.

The inspections should be carried out annually if the accounting firm has more than 100 companies it audits, and once every 3 years if it audits 100 or less companies.

The accounting firms being inspected is responsible of providing the PCAOB with the needed audit files, indicated as *+c* in Figure 6.5.

The purpose of the inspection is to identify any act or practice by the accounting firm that may be in violation of

- this Act,

- rules of the Board,

- rules of the Commission,

- the firms own quality control policies or professional standards.

If any violation is identified then the Board must report this to the Commission and each appropriate state regulatory authority. The Board can then begin investigation and take disciplinary action.

PCAOB transmits a written report on the findings for each inspection to the Commission and each appropriate State regulatory authority. The report should contain a letter or comment by the Board, and any letter of response from the inspected accounting firm. The report should also be available to the public.

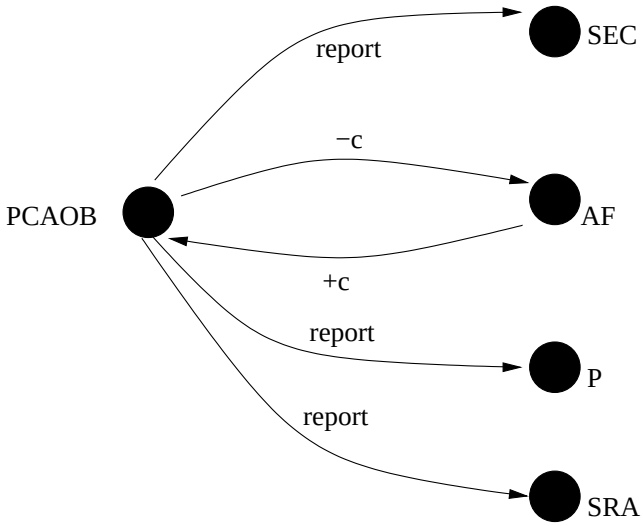

Figure 6.5: Relationship between agents in Section 104."c" is a promise between the PCAOB and accounting firm.

6.2.5 Article 29: Quality assurance

Member States has to make sure that all auditors and audit firms are subject to a system of quality assurance. Article 43 states that quality assurance reviews should be carried out at least every 3 years for auditors and audit firms that carry out audits of public companies. Auditors and audit firms are responsible of providing quality assurance systems audit files needed to make a review.

Figure 6.6 indicates this as a promise *+c* from the audit firm to the quality assurance system. *-c* indicates a promise by the quality assurance system to accept c given by the audit firm.

The quality assurance review consists of "adequate testing" of selected audit files, and should include an assessment of:

- *compliance with applicable auditing standards and independence requirements,*
- *quantity and quality of resources spent,*
- *audit fees charged,*
- *the internal quality control system of the audit firm*

Finally a report with the main conclusions of the quality assurance review should be written. Auditors and audit firms should follow up recommendations of quality reviews within reasonable period, if not be subject to the system of disciplinary actions or penalties reffered to in Article 30 [14].

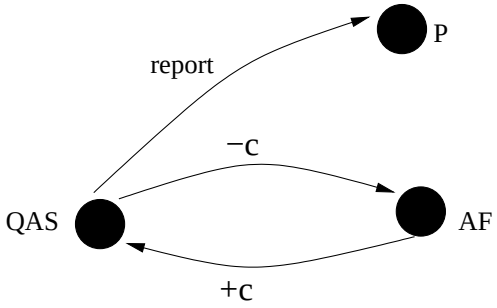

Figure 6.6: Relationship between agents in Article 29, "c" is the promise between the Audit firm and the Quality Assurance System.

6.2.6 Section 105: Investigations and disciplinary proceedings

If the PCAOB should discover any violations by a registered public accounting firm in accordance to the inspections made by section 104, the board may carry out investigation. The Board may require testimony of the firm or any persons associated with the firm, if the Board considers it relevant to an investigation. The accounting firm shall provide audit work papers and any other document or information in its possession, and the Board may even inspect the books and records of the firm to verify the accuracy of the information provided to it.

Promise with body *+d*, in Figure 6.7, given to the Board by the accounting firm is a promise to provide any necessary audit files in investigation. The Board can also request testimony and production of document in the possession of any other person, including any client of the accounting firm, if the Board finds it relevant to an investigation. *-d* is a promise by the Board to accept the promise given by the accounting firm.

If a registered public accounting firm or any associated person should refuse to testify, produce documents or cooperate with the Board in connection with an investigation the Board has the authority to suspend such person from being associated with a registered accounting firm or require that the registered accounting firm to end such association [11]. The Board can also suspend or withdraw the registration of the public accounting firm, otherwise also inflict lesser sanctions the Board considers appropriate.

Any final sanctions taken by the Board, towards any registered public accounting firm or on any associated person of a firm, has to rapidly be filed with the Commission.

+a is a promise by the Board to notify the SEC on actions taken. The SEC promise to accept *c* and oversee the santions taken by the Board.

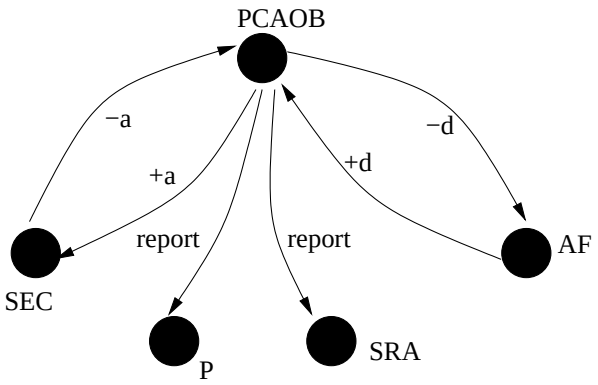

Figure 6.7: Relationship between agents in Section 105, "a" represents a promise between PCAOB and SEC, "d" is a promise between Accounting firm and PCAOB.

Section 107 states that the Commission may enhance, modify, cancel or reduce sanctions imposed by the Board upon registered public accounting firm, if the Commission finds that the sanction is not necessary or appropriate.

The sanctions imposed should also be reported to any appropriate State regulatory authority or any foreign board with which the accounting firm is licensed or certified, and the public.

6.2.7 Article 30: Systems of investigations and penalties

Each Member State is responsible of having effective systems of investigation and penalties to detect, correct and prevent inappropriate execution of audits. If audits are not carried out in accordance to the Directive, appropriate penalties should be inflicted auditors and audit firms. Member States can withdraw the approval of auditors and audit firms, as penalty. $+d$ in Figure 6.8 is the promise, "given" the system of investigation and penalties by audit firms, to provide cooperation in investigation. The system of investigation and penalties promise to accept d and "use" the cooperation to carry out investigation of auditors and audit firms.

Any measures taken and penalties imposed on auditors and audit firms have to be disclosed in a report. The Directive does not specify who the report is aimed for so we have assumed it is intended for the public in general.

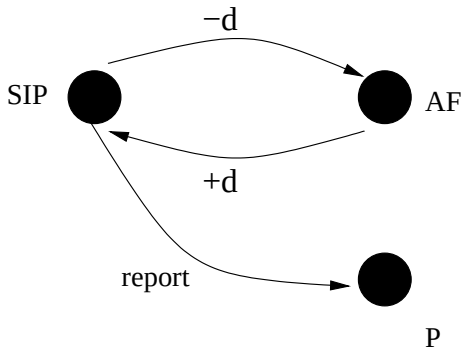

Figure 6.8: Relationship between agents in Article 30, "d" is a promise between the Audit firm and Member State.

6.2.8 Section 301: Public company audit committees

The audit committee of a company is directly responsible of appointing the registered accounting firm to be employed by the public company. The committee is in general responsible for the oversight of the company's financial reporting process, as well as the company's internal and external audits.

The registered public accounting firm performing audit of a public company, reports directly to the audit committee of that company. This is shown as *+e* in Figure 6.9. *-e* is a promise by the audit committee to accept the promise "given" by the accounting firm and oversee the work done by the accounting firm.

The audit committee is responsible for the oversight of the company's financial reporting process. *+f* in Figure 6.9 is a promise to report to the audit committee, made by the public company. *-f* is a promise to accept *f* and oversee the company.

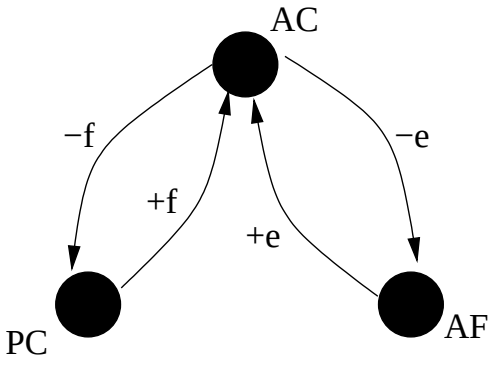

Figure 6.9: Relationship between agents in Section 301, "e" represents the promise between the Accounting firm and the audit committee, "f" is the promise between public companies and their audit committee.

6.2.9 Article 41: Audit committee

The audit committee is responsible of monitoring the financial reporting process, the effectiveness of the company's internal control, internal audits and risk management. The independence of the auditor and audit firm is also reviewed by the audit committee. The auditor reports to the committee on "key matters" arising from an audit and specially on material weaknesses in internal control which may affect the financial reporting process. This is shown as a promise *+e* from auditor to the audit committee in Figure 6.10. The employment of external auditor or audit firm is based on the recommendation made by the audit committee. Article 41 requires the auditor and audit firm to report annually to the audit committee their independence from, and any additional services provided to, the audited company (*+e*). *-e* indicates that audit committee promise to accept *e* and review the work of auditor and audit firm. *+f* is a promise made by the public company to report to their audit committee. *-f* is a promise from the audit committee to accept *f* and monitor the company.

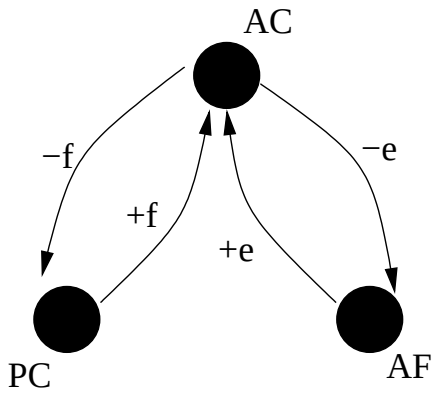

Figure 6.10: Relationship between agents in Article 41, "e" represents the promise between the audit firm and the audit committee, "f" is the promise between public companies and their audit committee.

6.2.10 Summary

In US inspections of registered public accounting firms are carried out annually if the firm has more than 100 clients, and every 3 years if clients equals to 100 or less. In Europe quality assurance reviews are carried out every 3 years for auditors and audit firms auditing public interest companies. Both in US and Europe the inspections and reviews consist of the evaluation of conduct by the accounting firm, auditor and audit firm by testing selected audit files. The inspections finally lead to a written report on the findings by the inspecting entity. In US the PCAOB has to report on the findings for each inspection to the Commission, each appropriate State regulatory authority and the public. The Directive does not specify who the written report is aimed to, so we have assumed it is aimed for the public in general.

If any inappropriate conduct by an accounting firm, auditor or audit firm is identified in accordance to the inspection referred to in section 104 in Sarbanes - Oxley and article 29 in the 8^{th} Company Law, investigations and disciplinary actions are carried out. In Sarbanes - Oxley the PCAOB is responsible for the investigation of accounting firm. The Board has also the authority to inflict sanctions it considers appropriate towards the accounting firm. Any sanctions imposed by the Board shall be reported to the Commission, each appropriate State regulatory authority and the public. Since the Commission oversees the Board, any sanctions imposed on an accounting firm by the Board can be enhanced, reduced or canceled by the Commission, if it should find that the sanction is not necessary or appropriate. In the 8^{th} Company Law investigations are performed by a system of investigation and penalties. Each Member State is responsible of having such a system. Appropriate penalties should be inflicted auditors and audit firms where audits are not carried out in accordance to the Directive. Any sanctions inflicted on auditors and audit firms should be disclosed to the public. In both the Sarbanes - Oxley and the 8^{th} Company Law withdrawal of registration is a penalty that can be imposed on accounting firm, auditors and audit firms.

Audit committee is in both Sarbanes - Oxley and 8^{th} Company Law responsible for the appointment of the companies external accounting firm, auditor and audit firm. The committee oversees the company's financial reporting process as well as the company's internal and external audits. The external accounting firm, auditor and audit firm report annually directly to the audit committee of the audited company.

6.2.11 Section 302: Corporate responsibility for financial reports

This section requires that CEOs and CFOs personally certify on each quarterly report filed stating they have reviewed the report and that the report is complete and accurate. They also have to certify their responsibility for establishing and maintaining internal controls and evaluate the effectiveness of these internal controls.

Significant deficiencies in the design or operation of the internal controls which could affect the financial reporting process in any way, has to be reported to the auditors and audit committee of the company. Any material weaknesses in internal controls have to be disclosed for the company's auditors. The signing officer has to indicate whether or not there have been any significant changes in internal controls, including any correction of significant deficiencies and material weaknesses.

In US there is a clear definition of ”significant deficiency” and ”material weaknesses” in the Auditing Standard No. 2.

This section affects the signing officer more than anyone in the company but depends on a bigger aspect of the company. To be able to certify the requirements of this section it depends on the internal controls and procedures for financial reporting established by section 404.

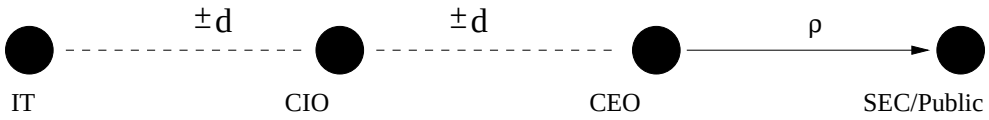

Figure 6.11: Basic promise defined in Section 302.

Using promise theory we try to understand the relationship between the involved ”agents” in this section and how an officer with certainty can sign on the accuracy of a financial report filed.

In promise theory agents can only make promises on their own behavior. Agents cannot make promises on behalf of other intermediate agents. Section 302 requires that CEOs and CFOs certify on the accuracy of the financial report. The financial reporting process depends on the IT system of the company. So for certification of section 302 to be possible it depends on the process control and monitoring system established by management in compliance with section 404.

Let us try to use promises to understand monitoring by voluntary cooperation. Monitoring can be done

- directly (line of sight, face 2 face, direct cable etc)
- indirectly (through intermediary, instrumentation, binoculars etc...)

Indirect monitoring or observation is the most used approach so we will use it to try understanding the relationship between agents and what promises need to be made to be in compliance with section 302.

Using the indirect approach we have to take into account the autonomous intermediate agents involved in the monitoring. Figure 6.11 shows the relationship between agents in the certification process required by section 302. The intermediate agents can be routers, software agents or humans. In our case it is the Chief Information Officer (CIO).

The financial reporting process depends on the IT system in the company. The IT system is not directly visible to the CEO and CFO so they have to rely on the CIO to relay the information. CEOs and CFOs are responsible for their promises to the Commission or the public about the accuracy and completeness of the financial report provided, but they have to rely on other agents that they cannot guarantee. CEOs and CFOs must rely on promises from the intermediate agents, the CIO in this case. For the signing officers to avoid lying they make their own promises conditional on the CIOs promise.

A promise made conditionally is not a promise, unless the condition is also promised [2]. This means the signing officers are making two promises to the public; one that the promise they are making is conditional on the promise made to them by the CIO; the other a promise to use the promise provided to them by the CIO.

To be able to promise the Commission or the public with some certainty that the report signed by the officers is accurate and the integrity of the report

is preserved, CIO need to make a promise to the CEO and CFO. This means the promise ρ made by CEO and CFO to the public depends on the CIO (Figure 6.12).

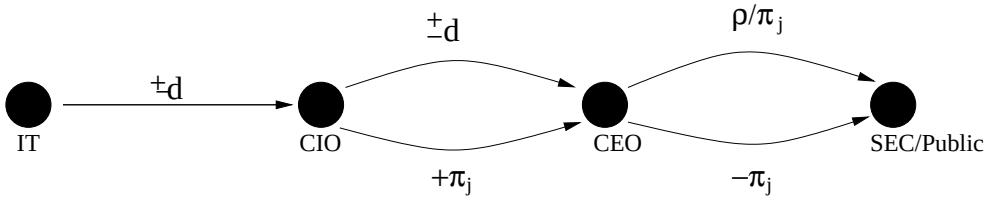

Figure 6.12: Promise ρ given by CEO depends on CIO. $+\pi_j$ is a promise to deliver data from IT to CEO. $-\pi_j$ is a promise to use π_j. CEO promises ρ conditionally if π_j is given by CIO.

We let $+\pi_j$ be a promise to deliver the report along the chain from the IT system to the CEO, $-\pi_j$ would then be a promise to use π_j. This means that CEO and CFO promise ρ conditionally, if π is given by intermediates, and it also promises to make use these promises (Figure 6.12).

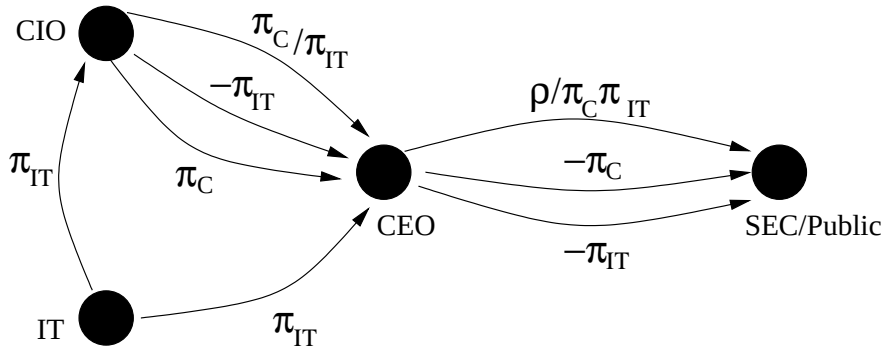

Figure 6.13: Promise dependencies between agents in Section 302.

By re-writing we find implicit promises (Figure 6.13) we did not see in Figure 6.12.

If an other intermediate was to be added (e.g Chief Security Officer (CSO)), additional relationships would be added and we would get an even more complex diagram (Figure 6.14). Promise theory teaches us that for each time we acquire a dependence on something we acquire for additional promises that must be verified. Since each promise is a "verifiable entity", we need to monitor to be sure it's true.

We can start to understand by looking at Figure 6.14 the complexity acquired by section 302, and can only imagine the complexity of the whole Act.

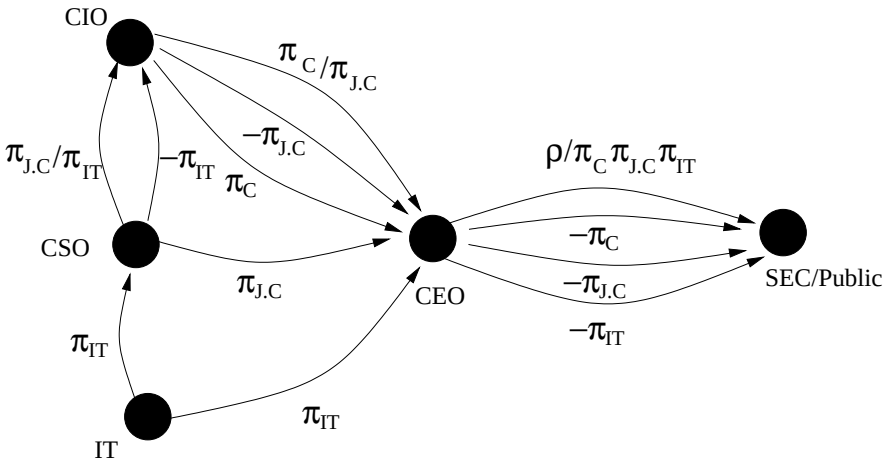

Figure 6.14: Example of complexity if another agent is added.

6.2.12 Section 404: Management assessment of internal controls

Section 404 along with section 302 is definitely the most discussed sections since the passage of the Sarbanes - Oxley. This section contains only 173 words but is considered to be the hardest and most expensive section to comply with. This section requires for the management to first of all claim the responsibility for the establishment of internal control and procedures for financial reporting and secondly annually report on the effectiveness of these internal controls and procedures. The annually report has to additionally be attested to by the external auditor of the company.

Establishing the internal control is one thing, but having to actually report on their effectiveness annually is something else. As companies develop their systems develop, which means the testing of these systems must develop.Mainly this means companies are never done complying with section 404.

We can understand by this section that the IT system affects the certifying CEO at the end. Basically for the CEO to putt his neck on the line, by certifying on the accuracy of the financial reports, which depends on the IT system, he would demand accountability from the IT department. We can see this dependency by looking at Figure 6.13. This diagram also showes us the implicit promises we did not assume by just reading the text in the law.

6.3 Configuration Management (CM)

So where does configuration management fit into all this? Can we determine which promises can be reduced to CM promises?

Definition (Configuration Management) *The process (and lifecycle) responsible for maintaining information about configuration items required to deliver an IT service, including their relationships*

We rely on technology for the verification of promises and Cfengine is a policy based configuration tool that allows you to describe policy, verify and fix promises about IT systems. Policy based configuration can be thought of as a list of promises that the system makes to some auditor about its configuration [17]. Cfengine supports automation for

- probing, testing
- repair
- logging

It is also able to record the history of a machine's compliance over time.

Cfengine make each individual machine responsible for its own state and verification of state. Thus we make each machine make appropriate promises and it is not necessary to check these promises until we need to audit the system.

[18] is a paper written to integrate cfengine 2 and ITIL processes. In this paper some ITIL terms are mentioned, with comments and translations into common cfengine terminology.

We mention some examples of cfengine promises related to ITIL terms, we found could be relevant in compliance with Sarbanes - Oxley [18]:

- *Alert*, a warning if something changes or fails
- *Audit*, a formal inspection and verification to check whether a standard or a set of guidelines is being followed. In cfengine data can be generated by extra logging information, collected and used in examination. This is suitable for use in formal inspection like compliance.
- *Change record*, contains details of which configuration items are affected and how they are affected by an authorized change. Changes made in cfengine can be written as log entries or audit entries.
- *Monitoring*, this is repeated observation of configuration item, IT process to detect events and ensure that current status is known. Monitoring of kept configuration-promises is one of several kinds of monitoring cfengine includes.
- *Repair*, the replacement or correction of failed configuration item. Cfengine promises refer to a desired state of a system and are automatically enforced. If failure were to occur cfengine always returns to a known state.
- *Role*, set of responsibilities and authorities given to an individual or a group of people. Cfengine defines a role as a class of agents that make the same kind of promise. The type of role played by the class is decided by the character of the promise they make.

These are all issues that are relevant when it comes to the compliance of Sarbanes - Oxley, which gives an idea of the possibilities of using cfengine configuration management and ITIL to get in compliance with Sarbanes - Oxley.

An important class of promises about a computer concerns its filesystem data. Change detection for filesystems uses a technique made famous in the program Tripwire, which collects a "snapshot" of the system in the form of a database of file checksums (cryptographic hashes) and permissions and rechecked the system against this database at regular intervals. Files are examined for change in their contents or their attributes. This is a very simple (even simplistic) view of change, but it forms a simple promise about the system. If a legitimate change is made to the system, the system also responds to this as a potential threat. Databases must then be altered, or rebuilt.

Cfengine can do the same thing in a promise oriented way. For example:

```
control:

  ChecksumUpdates = ( true )
  ChecksumPurge   = ( true )

files:

  # A promised template for files

  /my/important/files

        recurse=inf
        checksum=md5
        owner=root,daemon
        group=0,1,4
```

Or a more realistic example:

```
files:

  /usr/local owner=root,bin,man
             mode=o-w          \# check permissions separately
             r=inf
             checksum=best     \# switche on change detection
             action=warnall
             ignore=logs
             exclude=*.log

  # repeat for other files or directories
```

The first time we run this, cfengine collects data and treats all files as "unchanged". It builds a database of the checksums. The next time the rule is checked, cfagent recomputes the checksums and compares the new values to the 'reference' values stored in the database. If no change has occurred, the two should match. If they differ, then the file as changed and a warning is issued.

```
cf:nexus: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
cf:nexus: SECURITY ALERT: Checksum (md5) for /etc/passwd changed!
cf:nexus: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Cfengine can also promise to repair the changes from a trusted source if they are not authorized. Clearly there is a lot of potential for automating aspects of compliance

Chapter 7

Conclusions

In this work we have studied The Sarbanes - Oxley Act of 2002 and The 8^{th} Company Law Directive to understand in more detail the similarities and differences between the two laws. We have done this using promise theory model to get a clearer picture of what really distinguishes them from each other.

Using promise theory to model some specific ”rules” in both laws we certainly made it easier to see what requirements are expected and which relationships are required for public companies, accounting firms, auditors and audit firms to be in compliance. Promise theory helps us to understand the complexity implicit in SOX, by showing us intermediate agents we do not assume by just reading the text.

When Sarbanes - Oxley Act was first signed into law many companies struggled to understand what specifically needed to be done to be considered in compliance with the new law. No directions were given on how to comply with the law. Specially the role of IT in the law was unknown. Companies spent a lot of time and millions of dollars trying to solve the compliance issues. So a question that arouse while doing this project was if the costs had anything to do with the complexity of the law.

ISPartner stated that they used 20 million kroners to comply the first year SOX was passed. They spent large amount of money on licenses, software and extra machines.

In a general matter laws and directives are written in high-level language, which the parties they are aimed for and involve have to take the challenge in translating them into concrete low-level issues. Issues they have to solve to be in compliance. We have taken it to a lower level by analyzing the documents and representing the relationship between the different parties involved as promises between ”agents”.

In promise theory promises between agents are made voluntarily. Before Sarbanes - Oxley, people could claim that they didn’t know what was going on if fraud was detected, but now they have to promise that the financial reports are accurate, or be subject of strict penalties. This raises the question of whether we can call this voluntarily cooperation.

Personally I think Sarbanes - Oxley is a good way of preventing frauds and building investor confidence. It is not a suprise that the European came with

its own version of the American law, but what does suprise me is how little attention the 8^{th} Company Law has gotten compared to Sarbanes - Oxley. On the other hand the 8^{th} Company Law is more flexible when it comes to compliance which doesn't make it a big issue for auditors and audit firm compared to the Sarbanes - Oxley which is more strict. Reading documents like the Sarbanes - Oxley Act and the 8^{th} Company Law was a challenging experience. When it comes to language the Sarbanes - Oxley was heavier to read than the 8^{th} Company Law. The way the laws where devided into chapters and titles did make it easier to spot the similar topics in both documents.

Using Promise theory to model the laws gave me a much clearer picture on the relationships between the parties involved in the laws. Seeing the "rules" as promises gave me a new perspective on voluntary cooperation and obligation. If voluntary cooperation is taken for granted laws and directives may feel as obligations that we have to follow. Promise theory made it clearer that not every agent in a chain of promises is always willing or able to keep all of its promises.

7.1 Future work

The question is now if we can take this model further. Can we use promises to take the model to a lower level?

Cfengine is designed around promises and allows us to deal with complexity cheaply. Can the work done here help us to use cfengine in implementing some of the promises? Since Sarbanes - Oxley is here to stay and the 8^{th} Company Law is apparently the successor we think it is worthwhile a future research to find out if cfengine can be used as policy based configuration management to comply with both laws. Looking at the work of [18] with the integration of cfengine and ITIL processes and recognizing some of the same terms used in talking about compliance with other tools, we think it is worthwhile to research the option for compliance with both laws using cfengine and ITIL.

Bibliography

[1] Jasmine Noel. Sarbanes -oxley as an it-business alignment driver. *SearchCIO.com*, 2004.

[2] Mark Burgess. Business alignment viewed through the eyeglass of promises. 2008.

[3] It control objectives for sarbanes-oxley: The role of it in the design and implementation of internal control over financial reporting, 2nd edition. *IT Governance Institute*, 2006.

[4] Roderick Peterson Christian B. Lahti. *Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools*.

[5] M. Sloman E. Lupu. Conflict analysis for management policies. 1997.

[6] John Strassner. Den-ng: Achieving business-driven network management. 2002.

[7] John Strassner Dave Raymer. End-to-end model driven policy based network management. *IEEE Computer Society*, 2006.

[8] John Strassner Jos Neuman de Souza David Raymer Srini Samudrala Steven Davy Keara Barret Greg Cox, Joan Serrat. An enhanced policy model to enable autonomic communication. *IEEE Computer Society*, 2008.

[9] U.s. securities and exchange commission.

[10] Public company accounting oversight board. *http://www.pcaobus.org/*.

[11] Sarbanes - oxley act of 2002. *news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf*.

[12] Internal market: "european group of auditors' oversight bodies" created. *http://ec.europa.eu/internal_market/auditing/egaob/index_en.htm*.

[13] Commission decision of 14 december 2005, setting up a group of experts to advise the commission and to facilitate cooperation between public oversight systems for statutory auditors and audit firms. *Official Journal of the European Union*, 2005.

[14] Directive 2006/43/ec of the european parliament and of the council of 17 may 2006 on statutory audits of annual accounts and consolidated accounts, amending council directives 78/660/eec and 83/349/eec and repealing council directive 84/253/eec.

[15] James S. Turley. Get ready for the eu's 8th directive. *Directorship*, 2004.

[16] Mark Burgess. Promises, a practical introduction. 2008.

[17] Frisch Mark Burgess. A system engineer's guide to host configuration and maintenance using cfengine. 2007.

[18] Thomas Schaff Mark Burgess. Integrating cfengine 2 and itil processes. 2008.