FAKULTÄT FÜR !NFORMATIK

Developing an IT Management System Compliance Assessment Model for Didactical Learning

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Magister der Sozial- und Wirtschaftswissenschaften

im Rahmen des Studiums

Informatikmanagement

ausgeführt von

Åsmund Realfsen
Matrikelnummer 0250879

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: Ao. Univ.Prof. Dipl.-Ing. Dr.techn. Thomas Grechenig

Wien, 22.04.2009

Unterschrift Verfasser

Unterschrift Betreuer

Developing an IT Management System Compliance Assessment Model for Didactical Learning

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Magister der Sozial- und Wirtschaftswissenschaften

im Rahmen des Studiums

Informatikmanagement

eingereicht von

Åsmund Realfsen

Matrikelnummer 0250879

ausgeführt am

Institut für Rechnergestützte Automation

Forschungsgruppe Industrial Software

der Fakultät für Informatik der Technischen Universität Wien

Betreuung:

Betreuer: Univ.-Prof. Dipl.-Ing. Dr. techn. Thomas Grechenig

Mitwirkung: Andreas Ehringfeld, Paul Pöltner

Wien, 22.04.2009

"It must be remembered that there is nothing more difficult to plan, more doubtful of success nor more dangerous to manage than the creation of a new system. For the initiator has the enmity of all who profit by the preservation of the old institution and merely lukewarm defenders in those who would gain by the new one."

Nicolo Machiavelli

Eidesstattliche Erklärung

Ich erkläre an Eides statt, daß ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfaßt, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien, am 22.04.2009

.....
Åsmund Realfsen

Acknowledgments

This work would not be what it is without the help and support from several persons.

Ao. Univ.Prof. Dipl.-Ing. Dr.techn. Thomas Grechenig and Dipl.-Ing. Mag. Andreas Ehringfeld have contributed with valuable feedback and suggestions for improvement. Especially in the phase of defining the scope of this work and also in the process of research and writing, their help and support has been invaluable.

Moreover my fiancée Dipl.-Ing Livia Prestros and my friend Eva Reichstädter have continually helped and supported me in the writing process. Without their help this master thesis would have had quite many complicated sentences hard to understand.

I am also very grateful that I had understanding employers in the time I have been working with this master thesis. The flexibility given to me by Dr. Bernd Simon at Knowledge Markets Consulting Ges.m.b.H and Institute for Information Systems and New Media at the Vienna University of Economics and Business Administration has been of great help in the work with the master thesis.

Kurzfassung

Der Begriff Information Technology (IT) Governance beschreibt den Prozess der kontinuierlichen Verwaltung von betrieblichen IT-Ressourcen mit dem Ziel, die strategischen Unternehmensziele optimal zu unterstützen.

Eine Organisation kann zur Erreichung dieses Ziels auf verschiedene international akzeptierte Standards betreffend IT-Governance zurückgreifen. Zum Nachweis der Kompatibilität der Organisation mit einem IT-Governance Standard gegenüber Kunden, Eigentümern und andere Akteuren kann eine Organisation sich prüfen und zertifizieren lassen.

Diese Arbeit verfolgt zwei Ziele. Erstens sollen kleine und mittlere Organisationen dabei unterstützt werden, die Anforderungen der internationalen IT-Governance Standards "Control Objectives for Information and Related Technology " (COBIT), ISO/IEC 20000[1] und ISO/IEC 27001[2] zu lernen und das für die Umsetzung erforderliche Wissen zu erarbeiten. Zweitens sollen Methoden entwickelt werden, mit denen eine Organisation ihre Kompatibilität mit den drei genannten Standards beurteilen kann.

Der Ansatz für beide Ziele war, ein gemeinsames Modell zu entwickeln, das sowohl den Lernprozess als auch die Kompatibilitätsprüfung mit den drei Standards unterstützt. Für die Entwicklung des Modells wurden unterschiedliche didaktische Gesichtspunkte herangezogen, insbesondere hatten die kognitivistisches und konstruktivistisches Lerntheorien Einfluss auf die entwickelten Methoden und Strukturen.

Darüber hinaus kann das im Rahmen dieser Arbeit entwickelte Modell auch für die Messung der Reifegrade der implementierten IT-Prozessen verwendet werden. Das diesbezüglich entwickelte Reifegradmodell basiert auf dem Ansatz von "Capability Maturity Model Integration" (CMMI) und kann zur groben Einschätzung von COBIT-, ISO 20000- und ISO 27001-Prozessen verwendet werden.

Keywords: IT-Governance, COBIT, ISO 20000, ISO 27001, ITIL, CMMI, Process Maturity Models

[1] IT - Service management

[2] IT - Security techniques - Information Security Management Systems

Abstract

The term Information Technology (IT) governance can be defined as the continuous management of an organization's IT resources in order to optimally support the overall strategic business objectives.

An IT organization can use international accepted standards for IT governance to achieve this goal. Internationally accepted standards are built on knowledge from a large community and can be valuable as a guideline or template in this process.

In addition to document proven knowledge, several standards for IT governance provide certifications schemes in order to demonstrate quality to customers and shareholders.

The goal of this master thesis is twofold. First, the master thesis is to support small and medium sized organizations managing information technology in the process of acquiring the required knowledge for implementing organizational structures and processes according to the Control Objectives for Information and Related Technology (COBIT), ISO/IEC 20000[3] and ISO/IEC 27001[4] standards. Second, the master thesis should provide methods supporting an organization's internal compliance audit of the three standards.

The approach for solving both goals was to develop a common model that supports the learning process and compliance audit of the three standards. For the development of the model, several didactical considerations were taken into account. Especially the learning theories of cognitivism and constructivism influenced the structure and methods defined for the model.

Moreover, the developed model can be used for measuring the maturity level of an IT organization's implemented business processes. The model's custom maturity levels are based on the Capability Maturity Model Integration (CMMI) approach and measure the maturity of processes as defined in COBIT, ISO 20000 and ISO 27001.

Keywords: IT-Governance, COBIT, ISO 20000, ISO 27001, ITIL, CMMI, Process Maturity Models

[3] IT - Service management

[4] IT - Security techniques - Information Security Management Systems

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Basel Basel Committee on Banking Supervision

BS British Standard

BSI British Standards Institution

BSI Bundesamt für Sicherheit in der Informationstechnik (Germany)

CBT Computer Based Training

CCSC Commercial Computer Security Centre, UK Department of Trade and Industry.

CCTA Central Computer and Telecommunications Agency

CEO Chief Executive Officer

CFO Chief Financial Officer

CIO Chief Information Officer

CM Configuration Management (CMMI)

CMM Capability Maturity Model

CMMI Capability Maturity Model Integration

CMMI-ACQ CMMI for Acquisition

CMMI-DEV CMMI for Development

CMMI-SRC CMMI for Services

COBIT Control Objects for Information and related Technology

COO Chief Operating Officer

COSO Committee of Sponsoring Organizations of the Treadway Commission

DERA Defense Evaluation Research Agency

DoD Department of Defense , USA

ERP Enterprise Resource Planning

IEC International Electrotechnical Commission

IPPD Integrated Process and Production Development

ISACA Information Systems Audit and Control Association

ISMS Information Security Management System

ISO International Organization for Standardization

ISSEA International Systems Security Engineering Association

ITGI IT Governance Institute

ITIL Information Technology Infrastructure Library

ITS Intelligent tutoring systems

ITSM IT Service Management

NGOSS New Generation Operations Systems and Software

NSA National Security Agency

OECD Organization for Economic Co-operation and Development

OGC Office of Government and Commerce

PBL Problem Based Learning

PDCA Plan-Do-Check-Act

RD Requierments Development (CMMI)

REQM Requierments Management (CMMI)

RSKM Risk Management (CMMI)

SCAMPI Standard CMMI Appraisal Method for Process Improvement

SEI Software Engineering Instutitue (Carnegie Mellon University)

SISP Strategic Information System Planning

SOX Sarbanes-Oxley Act

SPICE Software Process Improvement and Capability Determination

Chapter 1

Introduction

Small and medium sized businesses often lack the knowledge and experience for implementing an international accepted IT governance framework.

The scope of this master thesis is to develop a didactical model assisting the self learning of the three IT governance supporting standards COBIT[1], ISO 20000[2] and ISO 27001[3]. In addition the model could be used as a foundation for internal compliance audits.

1.1 Motivation and Problem Description

Improving the quality of IT processes with the use of international accepted standards requires detailed knowledge and experience of the standards in question. In addition detailed knowledge of the operations of the organization itself is required.

The latter is an implicit part of the organizational knowledge. Detailed knowledge about and experience with international accepted standards supporting IT governance are usually something small and medium sized IT organizations do not have.

In order to fill this gap of knowledge, an organization can choose to obtain the knowledge internally or externally.

If the required knowledge is to be developed internally, costs for courses and employee time occurs. If an external consultant is hired the organization might get quicker results in the short run, but the knowledge transfer to the organization might be poor.

Regardless of internal or external approach, costs will occur. These costs, in addition to the complexity and abstract level of many of the international accepted standards, are most likely a major obstacle for small and medium

[1] Control Objectives for Information and Related Technology

[2] ISO 20000 - Information technology - Service management

[3] ISO 27001 - Information technology - Security techniques - Information security management systems - Requirements

sized organizations in their pursuit of excellence in their internal IT related business processes.

The scope of this master thesis is to develop a model for supporting a small or medium sized organization in the process of learning about the requirements and the practical appliance of the COBIT, ISO 20000 and ISO 27001 standards.

The model will be centered on the Plan-Do-Check-Act (PDCA) cycle for continual process improvement, as this serves as the underlying basis of all of the three standards. Moreover the model will focus on grouping requirements into relevant categories and link them to each of the phases in the PDCA cycle.

As large parts of the three standards have overlapping areas, a goal of this master thesis will be to achieve synergetic effects for companies needing support in the process of learning how to implement a combination of the standards.

This can be achieved by focusing on shared content between the standards. The model should for example cover the aspects of risk management only once even though risk management is covered slightly different in each standard.

A nice side effect of this is the possibility to assist in the internal compliance audit of an organization's IT governance system. The result of such audit should be a report of how compliant the organization is with the requirements defined in COBIT, ISO 20000 and ISO 27001.

The model developed in this master thesis is supposed to serve as the theoretical foundation for a new software tool[4]. The model will provide the software tool with structured content and a didactical concept for learning and execution of internal audits.

In general the master thesis can be summarized in the following sentences:

- The scope covers the three standards COBIT, ISO 20000 and ISO 27001.
- Develop a model that assists an organization
  - in acquiring required knowledge and
  - in the execution of internal compliance audits.
- The model serves as the theoretical foundation for a software tool by
  - providing a didactical concept and
  - designing a structure for content.

[4]The development of the software tool itself, or a detailed requirement specification for it, is not a part of the master thesis.

1.2 Research Objectives

The three standards COBIT, ISO 20000 and ISO 27001 are selected for investigation in this master thesis due to wide spread use and acceptance. [Wol06] [SSA08]

While ISO 27001 focuses on the secure operation of IT organizations with special attention to the tasks of establishing, operating, reviewing and improving an Information Security Management System (ISMS) [105c], the two other standards cover a broader scope. However, implementing one of the standards does not exclude the implementation of the other. They are all mutual compatible, but simply vary in scope and level of detailedness. [Von05] [oGCU05] [SSA08]

ISO 20000 and COBIT share a common scope of service management. Both require e.g. the implementation of change management and performance management processes. While ISO 20000 only covers service management [105a], COBIT on the other hand describes 34 processes with the aim of providing a complete IT Governance framework.[COB07]

A research objective for the master thesis is to provide a mapping between the three standards on a higher level. Some literature and research exist in this field, but not for the latest version of the standards. E.g. research exists that compares COBIT with ISO 17799[5] [2705], and ITIL. [oGCU05] In order to develop one model for all three standards a high level mapping between the latest versions of the various standards is a necessity.

The scope of the master thesis is to develop a model assisting in the learning and execution of internal audits in relation to COBIT, ISO 20000 and ISO 27001.

Derived from this research objective the following four hypotheses are presented and expected to be confirmed or disproved in the master thesis:

1. One combined model can be developed for assisting the learning process of COBIT, ISO 20000 and ISO 27001 in a self training context.

2. One combined model requires less time of the learner than it would be the case if learning programs for the standards were developed independently of each other.

3. The same model can be applied in the context of a combined internal audit of the implementation of COBIT, ISO 20000 and ISO 27001.

4. In the context of internal compliance audit of the three standards the maturity of the organizational IT processes can be investigated.

The main objective of the master thesis is formulated in the first hypothesis. It simply states that it is possible to develop one model assisting

[5] In 2007 ISO 17799 (the code of practice guide for information security management) was renamed ISO 27002.

the learning of the required parts of COBIT, ISO 20000 and ISO 27001. Most standards and especially the ISO 20000 and ISO 27001 standards are divided into required and optional parts. The focus of this master thesis will be on the required parts.

Hypothesis two could be verified by demonstrating that the three standards have overlapping areas and that synergetic effects are achieved by mapping the different parts of the standards to the PDCA cycle.

ISO 20000 seems to be completely overlapped by COBIT, ISO 27001 seems to have a partly overlap with both COBIT and ISO 20000. Mapping the required parts to several standards results in less content in total and probably less time consumed in the learning process.

Hypothesis three states that the same model can be used for assisting the learning process as well as for internal audits. The reason for this claim is that the development of the model for learning will include a detailed mapping of requirements between the standards, and that this mapping could build the foundation for an internal audit.

Implicit in hypothesis three is also the synergetic effect as claimed in hypotheses two. Meaning that less time should be required to perform an internal audit based on one model for all three standards than separate audits for each standard.

Regarding hypothesis four a custom process maturity model has to be developed. COBIT uses a derived version of the Software Engineering Institute (SEI) Capability Maturity Model (CMM) which specifies six distinct levels from "non-existent" to "optimized".[Deb06] As COBIT and ISO 20000 seem to have a complete overlap, this maturity model would probably fit ISO 20000 as well. The master thesis has to investigate if the same maturity model is meaningful for ISO 27001 as well.

Some research suggests that the process maturity model used in COBIT is not sufficient for evaluating the maturity of process groups, but only for single processes.[SJW07] If this is the case, the COBIT model cannot be directly used in the model developed in the master thesis. Several other well known maturity models exist as well, and a custom maturity model probably has to incorporate ideas from more than one defined model in order to fulfill the requirements of being a meaningful scale of measurement for processes in all three standards.

1.3 Document Structure

The master thesis is divided into five main parts from chapter 1 to 6, whereas chapter 2 to 5 cover the required background information and chapter 6 documents the process of developing the conceptual model.

In specific chapter 2 covers IT governance as a concept. The term IT governance has a slightly different meaning depending on industry and the point of view. This chapter explores some of the many definitions of IT governance and searches for common ground. Included is also an overview of some of the legal implications on the governance of information technology.

In chapter 3 tools and methods supporting the implementation of IT governance systems are presented. Directly relevant for the development of the model are COBIT and ISO 20000, which are both described in detail. Moreover descriptions of IT Infrastructure Library (ITIL) and the Capability Maturity Model Integration (CMMI) are included. The first provides a deeper understanding of ISO 20000. The latter is included as an example of one of the best known maturity models for IT related processes.

Chapter 4 deals with Information Security Management System (ISMS). Specifically ISO 27001 as an international accepted standard for certification of ISMS is analyzed with special attention on requirements and control objectives.

As one of the main uses of the model is to support learning a didactical concept has to be developed. The theories of didactics and relevant theories of learning are presented in chapter 5. Special attention is given to the theories of behaviorism, cognitivism and constructivism.

The development of the model itself is described in chapter 6. This involves a five step process including the selection of relevant parts of the standards to include, identify areas of overlapping content, description of didactical principles and designing a usable structure. The chapter also includes sample content for the model as well as suggestion of suitable process maturity levels.

Chapter 2

Defining IT Governance

Information is an important asset of every company. From a corporate point of view information can be seen as the fourth factor of production next to land, labor and capital. In order to support business processes effectively, the creation, preparation, sharing and archiving of corporate information need to be supported by relevant technology.[Sur05] The managed corporate information is not only used for supporting the business processes, but is also the basis for almost every strategic and tactical decision made by the management and the board of directors.

In addition to being supportive, the management of information can represent a value in itself, increasing the competitiveness and market value of a business in addition to improving the general return on investment. Studies of more than 250 organizations in 23 countries show that companies with better than average IT governance earn at least 20 percent higher return on assets than organizations with weaker governance.[RW04]

For most organizations the cost of IT is substantial and makes up approximately four percent of gross revenue with a rising trend.[WPR06] The cost of managing information includes not only computer hardware, software, people, training and skills. In a broader perspective the real cost of an IT system includes the cost of failing to support the strategic business processes adequately, and hence directly decreasing the financial performance and competitiveness of a company.

Well managed information systems that support business processes correctly can enable companies to reduce time to market for new products, enable new business concepts to vital processes and open up new business opportunities. It would be virtually impossible to operate within e.g. the automotive industry today without a functional IT governance system, not only in the company itself, but also between the company and its suppliers. Production concepts like e.g. just-in-time delivery of goods would hardly be possible without the use of information technology itself, as well as a well managed information creation, processing and sharing process.

In an academic context the term IT governance was first used in the early 1990s to describe the complex relationships involved in obtaining strategic alignment between several companies in respect to business processes and IT.[SJW07] [HV93] [LV95] Since then several incidents, most famous the Enron fraud scandal in 2001, have increased the awareness of the need for transparency of corporate decisions.

Governments responded to this awareness, and laws and regulations were implemented in more than 50 countries that enforced tighter control of how corporations are to be managed and how information from companies is to be validated and communicated.[WPR06] The goal of governmental regulations for corporate governance is a higher degree of accountability and transparency in order to minimize risk and secure the rights of stakeholders, in particular the shareholders.

New laws and regulations for corporate governance do of course also affect how information is to be managed within an organization. In addition this has increased the interest and awareness of a systematic approach to IT governance in a broader perspective, and IT governance is no longer an academic issue only.

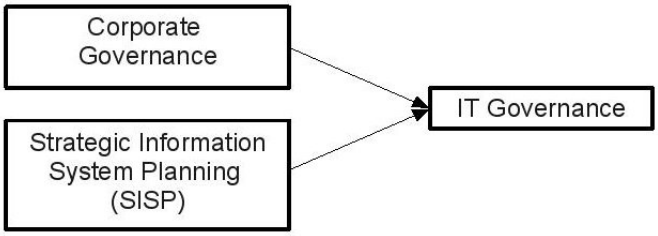

Figure 2.1: The Evolution of IT Governance.[WPR06]

Webb, Pollard and Ridley argue that IT governance has evolved from and is influenced by the fields of Strategic Information System Planning (SISP) and corporate governance.[WPR06]

SISP has its roots in the late 1970s[FH96], and is defined as: *"The process of identifying a portfolio of computer-based applications that will assist an organization in executing its business plans and realizing its business goals."*[HBS00]

The key objective of SISP is to ensure that an organization's IT strategy is compatible with and supports the business strategy. The focus of SISP is on applications, IT systems and IT resources, and how these items can be applied for strategic advantage, strategic planning and management of the technology.

IT governance is more far-reaching than SISP and focuses on goals, risks, processes, people and technology on a strategic and tactical level. There is considerable overlap between the three concepts IT governance, corporate

governance and SISP. IT governance is often defined as a sub-process of corporate governance. The difference between IT governance and SISP lies not only in the issues covered but also in with whom and at which level responsibility lies. While SISP could be seen as an operational or tactical issue, the focus of IT governance is lifted to the ranks of senior management and - if appropriate - the board.[WPR06]

2.1 Corporate Governance

In a small company, the owner and the manager might be the same person. In any case is the owner likely to have direct control over the major strategic decisions made, and is informed about the day to day running of the business. In an incorporated company the shareholders and the executive management are two distinct entities that do not necessarily have the same objectives. E.g. while the shareholders are interested in achieving a high return of investment, the management might follow other objectives like increasing their own salary, reputation etc. In economic literature the possible interest gap between a company's owner and a company's management is referred to as the principal-agent problem, where the principal is the owner and the management is the agent acting on behalf of the owner. [RSG06]

Even though the principal-agent problem is probably one of the more important factors driving the awareness and motivation for better corporate governance, other factors like globalization, financial crises, fraud and out of scale remuneration of the top management contribute as well.

The Organization for Economic Co-operation and Development (OECD) defines corporate governance in the following way:

> *"the system by which companies are directed and controlled, and whose structure specifies the distribution of rights and responsibilities between the different participants of the company, such as the board of directors, shareholders and other economic agents, who maintain some interest in the company. Corporate governance also provides the structure through which the objectives of the company are established, the means to reach these objectives, as well as the way of doing a follow-up of the company's performance".* [OEC06]

OECD has specified six principles of corporate governance[OEC04]:

- Ensuring the basis for an effective corporate governance framework.
- The rights of shareholders and key ownership functions.
- The equitable treatment of shareholders.

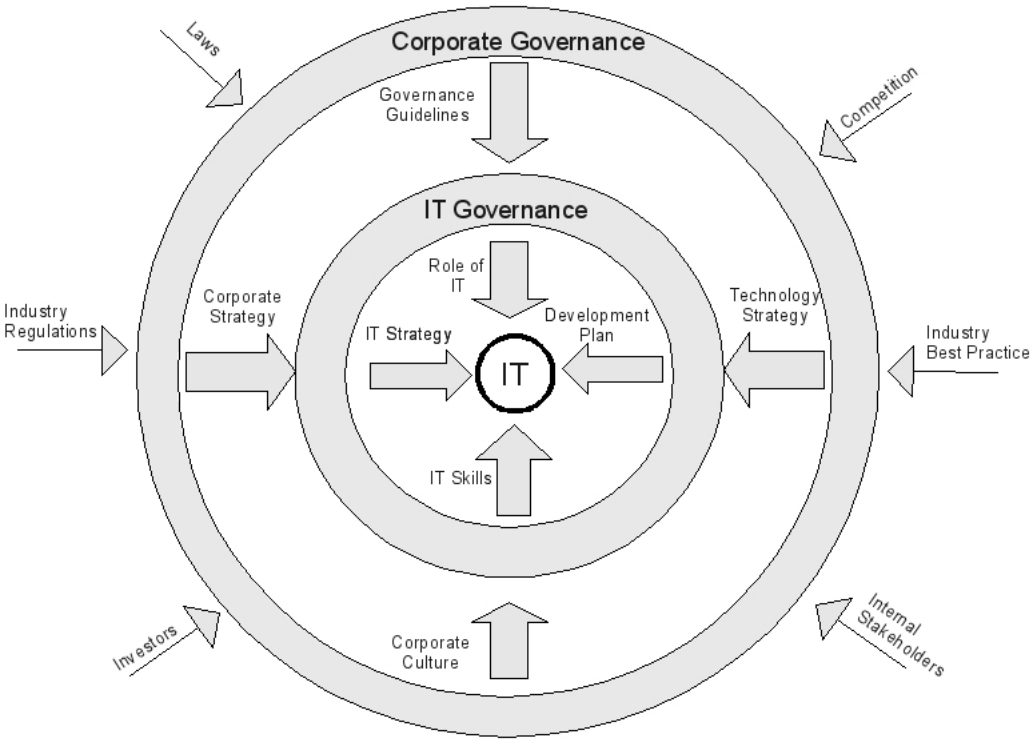

Figure 2.2: IT governance as an implicit part of corporate governance according to Rüter, Schröder and Göldner.[RSG06]

- The role of stakeholders in corporate governance.
- Disclosure and transparency.
- The responsibilities of the board.

The OECD corporate governance definition and principles set the focus on the top level management and the external stakeholders of a corporation, in particular the shareholders' right to information. However, the quality of the corporate governance also has an internal effect. If a company's corporate governance system is used actively, especially by the management, it will also result in a higher degree of employee satisfaction and employee identification with the company.[RSG06]

IT governance is often regarded as sub process of corporate governance. The model from Rüter, Schrüder and Göldner in figure 2.2 visualizes this, in addition to internal and external factors that influence the implementation of IT governance systems. A company's corporate governance is influenced by factors like laws and regulations, competitors' performance, financial situation, relationships to investors and other stakeholders etc. The input parameters to corporate governance in addition to the company culture,

business and technology strategy, comprise the environment IT governance has to operate within.

2.2 Legal Requirements

As a result of accounting scandals like the cases of Enron in 2001 and WorldCom in 2002, the awareness of good corporate governance or a lack of such rose to the public mind. The scandals involved not only fraud in the top management of the corporations, but also well known auditing firms and banks. As a result, several countries have implemented laws and regulations specifying requirements for corporate governance. Not only the USA, but also european countries like Germany, Austria and Switzerland have changed their legislation in order to ensure good corporate governance.[Sur05]

Legal requirements also have a direct effect on IT and on how it is managed in the business process. In order to prove compliance with legal requirements the internal control system of a company has to report trustworthy and correct financial data, and be able to account for how they are compiled. This requires a tight integration of IT with the business processes and is not a static system, but needs to be developed and changed dynamically according to an ever-changing business environment.

About 30% of errors in internal control systems can be traced back to IT and how it is applied. The cost of compliance with legal corporate governance requirements in the USA is estimated at $80bn in 2009. One third of the cost is estimated for IT hardware and software, and two thirds for the cost of the use of internal human resources, external consultants and auditors. [RSG06]

Legal requirements for corporate governance have a significant effect on how IT governance is implemented and operated in an organization. But the effect is also the other way around, efficient IT systems that support the business with trustworthy data are critical for fulfilling the legal requirements for corporate governance.

In the following text, examples of two legal requirements with international effects are outlined. The Sarbanes-Oxley Act regulates corporate governance for all public listed companies on stock exchanges in the USA, and Basel II that specifies governance requirements for banks.

2.2.1 Sarbanes-Oxley Act

In 2002 the Sarbanes-Oxley Act (SOX) was passed in the USA, and in 2006 a change in the requirements for all corporations listed on US stock exchanges, including foreign companies, came into effect. With SOX the legislator follows three principles:

- Securing the integrity of financial data.

- Management responsibility.
- Independent auditing.

SOX requires the management to implement an internal control system on the basis of a generally accepted framework. In addition the management has to test and evaluate the system. Moreover an independent auditor is required to check the internal control system and the management's evaluation of it.

In SOX the responsibility of the management is especially important. According to SOX the CEO and CFO have a personal liability, and in case of non compliance can be jailed or fined.

The implications for IT governance are that tasks related to the internal control system have to be given a high priority and cannot be regarded as an optional task due to its internal nature and distance from more production near business processes.

2.2.2 Basel II

The Basel Committee on Banking Supervision is an institution that creates policy recommendations for its member countries on supervision of the banking sector. Member countries include eight EU countries in addition to the USA, Canada, Japan and Switzerland.

In 1988 the Basel I accord was released which specifies minimum capital requirements used by international operating banks. Basel II from 1999 is a revised version of Basel I and extends the specification with operational risk management.[Brü03] The objectives of the Basel accords is to contribute to the stability of the international banking system by setting a standard for risk management and making capital more risk sensitive.[APZ07] The Basel accords are voluntarily implemented by all banks in industrialized countries.[Sur05]

Basel II consists of three pillars: market discipline, supervisory review process and minimum capital requirements. The latter is divided in:

- credit risk,
- market risk
- and operation risk.

Market and credit risks were also a part of Basel I and can be evaluated with standard techniques. Operational risk on the other hand is not that easy to measure. In the Basel II specification, operation risk is defined as:

> *"... the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.* "[oBS04]

This definition is very general and includes issues like internal fraud, theft, business disruption due to e.g. natural disasters, unsatisfied customers due to bad product quality etc.

A distinct characteristic of operational risk in comparison with credit and market risk is the typical influence from internal events.[APZ07] Hence, operational risk is the one factor in Basel II that is closely connected to the IT services in corporations.

A company that is estimated to have grave problems with its IT security or other problems with information management that could have a considerable negative effect on the operation of the company, could be given a lower credit rating. The result would be a higher interest rate on the individual credit capital.[Eck08] Of course the same effect also occurs the other way around. The higher the quality of IT governance in an organization the lower the operational risk estimated by banks, and hence the cost of future credit capital will be lower.

2.3 IT Governance Definitions

IT governance is often referred to as a sub process or integrated part of corporate governance. In general terms the objectives of IT governance are to apply processes and take measures in order to let the IT systems support the business processes optimally, to ensure a responsible use of resources and to monitor and manage risk.

In general terms it is easy to find consensus about what IT governance is. But still - no internationally accepted standard definition of IT governance exists. Instead a number of organizations, universities, consultants and researchers provide their own.

Definitions differ in the way they put focus on specific aspects of IT governance. One definition might try to communicate that alignment of IT with business processes is a crucial issue, whereas others regard IT governance more as a framework for decision making. Research based on a survey of more than 200 CIOs world-wide shows that no general IT governance model is accepted. Instead the conception of IT governance depends on the business environment and the general conditions.[RSG06]

Confusing the picture even more there is considerable overlap between the concepts corporate governance, strategic information system planning (SISP) and IT governance. (As visualized in figure 2.1 on page 7.) In addition there is discrepancy between what academic and practitioners understand by the term.[WPR06]

It is evident that the term "IT governance" is unclear and means different things to different groups of people. Based on this, this work will not rely on one definition of IT governance. Instead, three definitions will be reflected upon. One from the IT auditing industry, one from the academic world, and

one trying to merge the definitions from the academic world with the world of practitioners.

2.3.1 A Definition from the IT auditing Industry

Even though the term IT governance is unclear due to lack of an official standard or definition, some definitions seem to be more cited than others.

The definition from the IT Governance Institute (ITGI) is one of the prevalent used ones, probably due to the popularity of the ITGI's IT governance framework "Control Objects for Information and related Technology" (COBIT). ITGI is a research organization founded by Information Systems Audit and Control Association (ISACA) and the aspects of control and auditing of IT systems are central issues for ITGI.[Gol06]

According to ITGI IT governance is the durable responsibility of the whole IT organization, and not only the CIO. In COBIT IT governance is defined as:

> *"... the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that enterprise 's IT sustains and extends the organisation's strategies and objectives."*[COB07]

The ITGI's definition specifies the who, what and why of IT governance, but fails to say anything about how. This is probably due to the fact that ITGI has its roots in the IT auditing industry, hence is less concerned about how IT governance is implemented.

Even though the ITGI's definition is very far-reaching, the auditing industry does of course have its main focus on measurement and control. ITGI states that value, risk and control constitute the core of IT governance.[COB07] The focus on control is even more dominant if we consider COBIT, the framework for IT governance developed by ITGI.

COBIT describes 34 typical corporate IT processes ranging from planning and acquiring to operating and monitoring IT systems. The core of each process description is a set of control objectives used to measure the maturity of the process. The maturity of the process is an indicator for how well implemented the process is, and how much risk is involved. If a process has a high maturity rating, it has been well implemented, and the risk of this particular business process's negative contribution to the overall business objectives is low.

2.3.2 An Academic Definition

Although the management of IT and IT resources has been an issue since the early days of computing, the actual term "IT governance" was not used in academic papers before 1992/93.[SJW07] At that time it was used in

order to describe the strategic alignment of business and IT in an interfirm context.[LV95][HV93]

Since the 1990s a number of academic papers describing IT governance and its relation to other concepts, issues and assets have been published. However, still no generally accepted academic definition has emerged.

In a paper from 2006, a group of researchers (Webb, Pollard and Ridley) connected to the University of Tasmania did an extensive literature research in order to derive a definitive definition of IT governance. They argued that the current definitions did not capture the broad reach of the concept, instead each definition describes one or another aspect of IT governance or its supporting mechanisms.[WPR06]

By analyzing twelve well known IT governance definitions from literature and reviewing these in the light of the context they were provided, the researchers were able to identify five distinct elements describing IT governance[WPR06]:

- Strategic Alignment.
- Delivery of business value through IT.
- Performance Management.
- Risk Management.
- Control and Accountability

Several of the definitions reviewed included policies, procedures and decision-making structure as an important part of IT governance. Webb, Pollard and Ridley on the other hand argue that the presence of these do not define IT governance, but are merely artificially created devices that assist and enable an effective governance system.

Using the five identified elements, the researchers propose a definitive definition of IT governance:

> *"IT governance is the strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management."*[WPR06]

While the definition from the auditing industry did not say anything about how IT governance is to be implemented, the academic definition is more specific. In the academic definition IT control, performance and risk management are considered to be tools for achieving the goal of strategic alignment of IT and enabling maximum business value.

The proposed definitive definition from Webb, Pollard and Ridley says nothing about who is responsible for IT governance. This is a contrast to the definition by ITGI that explicitly mentions IT governance as the responsibility of executives and the board of directors.

2.3.3 Practitioners vs. Academics - a combined Definition

The definitions from IGIT and Webb, Pollard and Ridley show that there are differences in what the IT auditing industry and the world of academics understand by the term IT governance. Clearly the two definitions have more in common than what separates them. The difference between them has more to do with which issues are regarded to be important, and should find the way into the core definition of IT governance.

In the same way as there is a conflict between the IT auditing industry and the academic conception of IT governance, there is a difference between what academics and practitioners, like consultants and CIOs, understand by the term.

Research shows that theories from the literature are not very frequently used by practitioners.[CVDV06][DK06] A survey by ISACA Sweden chapter in 2004 suggests that even though a large part of participants claimed to know about IT governance frameworks like COBIT and ITIL, few applied these frameworks in order to support their organizations.[SE06]

The three-dimensional Cube Model

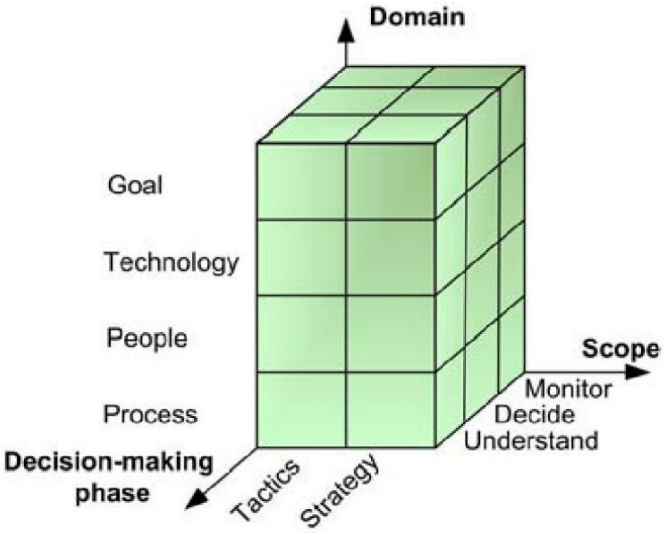

Figure 2.3: Simonsson and Ekstedt's three-dimensional Cube Model of IT Governance.[SE06]

Simonsson and Ekstedt from the Royal Institute of Technology, Stockholm, Sweden, investigated in a paper from 2006 the relationship between the academic and practitioner conception of IT governance. Rather than ending up with a one line definition of IT Governance, a model representing the dimensions of IT governance is presented.[SE06]

Figure 2.3 shows the three-dimensional cube defining IT governance according to Simonsson and Ekstedt. The focus of the model is on decision making. IT governance decisions are viewed in the light of the domain and the scope it is operating.

The dimension domain describes which assets IT governance is concerned about and contains the dimensional units goals, technology, people and processes.[SE06]

Goals includes decisions regarding IT policies, guidelines and metrics to be measured against.

Technology is primarily about the physical things like infrastructure such as servers, communication devices, firewalls and storage solutions. Moreover all kind of software applied and facilities used to host the physical assets and the personnel is regarded as technology in this model.

The dimensional unit people represents how the organization is organized and the responsibility of different roles within the organization. This includes decisions like who is responsible for what in respect to IT, and what responsibilities and roles different stakeholder groups have.

Processes include the design, implementation, and measurement of IT related processes, activities and procedures. Processes could typically be supported by an IT governance framework like e.g. ITIL for service management.

The decision making dimension describes different phases or steps required for making a decision.[SE06]

The first step is to understand the decision to be made. This includes the collection of decision relevant information, analysis of the available data in order to understand the situation and assess the possible outcomes of alternative decisions.

In the decide phase it is determined how and by whom the decision is to be made. Of course this phase also includes the actual decision itself.

In order to improve implemented processes and the quality of further decisions the monitoring phase is decisive. This includes the selection of what to monitor, assess the performance of the organization and enable and support periodical audits.

The model's scope dimension describes the impact of an IT governance relevant decision.[SE06]

A decision could have a long term or short term effect on the organization. The short term decisions are regarded as tactical decisions and require a high level of details, but less preparation than the long term decisions. Tactical decisions include whether to upgrade a workstation, how to design an intranet web page or how to staff a small IT project. Tactical decisions are normally done by lower management.

A strategic decision has a long term effect on the organization and the business. Typically these kinds of decisions require fewer details, but a longer period of preparation. Examples of tactical decisions could be whether to

make or buy a core business process supporting software or whether to outsource parts of the IT organization like e.g. the helpdesk functionality. Strategic decisions are the responsibility of the board of directors or the top level management like the CEO or CIO.

Practitioners vs. Academic Conception of IT Governance

In their research Simonsson and Ekstedt compared how practitioners[1] and academic literature prioritized the elements of the three domain model.

Differences can be found in the decision making domain as well as in the scope domain.

According to the practitioners, IT governance is primarily a strategic issue, and tactical decisions are of less importance. This is interesting viewed in the light of which tools and framework to apply for optimal IT governance. ITIL is a process based IT governance framework with a rather tactical focus and provides little support on development of e.g. strategic IT plans. The findings of the Simonsson and Ekstedt's study suggest that ITIL is less appealing to practitioners than COBIT, which is more concerned about the strategic issues of IT governance.[SE06]

Moreover the practitioners regarded the understanding phase in the decision making domain to be more important than the decision or monitoring phase. The academic literature on the other hand regards monitoring to be most important. The reason for such differences could be that consultants are more concerned with setting up an IT governance framework than operating one, and that few organizations are mature enough to fully monitor their IT governance processes. Additionally consultants and CIOs are often occupied with tactical problems in the IT organization, hence monitoring is given a lower priority.[SE06]

Practitioners and academic literature do however agree that setting specific and relevant goals and management of people and processes are core issues in IT governance.[SE06]

2.4 IT Governance in the Practice

In the practice an IT governance project is often started due to corporate reorganization, or the wish to sustainable improve the efficiency of the IT organization and its services.[RSG06]

However, reorganizing an organization and defining IT governance on a high level, does not automatically mean that the organization actual uses IT governance to improve its services. Developing a model is just the first

[1] Simonsson and Ekstedt only used consultants and CIOs with experience in IT governance projects when researching practitioner's prioritization of the elements in the three domain model.

part. An organization does not achieve a higher degree of quality in its IT related processes before IT governance is actually implemented.

Structures, processes and frameworks are often used to describe the implementation of IT governance.

2.4.1 Structures

Structures often describe hierarchies or entities used for managing IT systems. [May06]

Sambamurthy and Zmud have identified three modes of structures to be prevalent: centralized, decentralized and federal. [SZ99]

A centralized mode indicates that one central organizational unit has the authority to make all IT related decisions.

The decentralized mode can be represented in different ways, but generally it represents a shift from a central authority towards divisional authority or directly to line managers.

The federal mode is a mixture of centralized and decentralized mode, in which parts of the central authority are delegated to divisional units and/or line managers.[WPR06]

2.4.2 Processes

While an organizational structure is concerned about how people are organized in order to take decisions, processes describe what is to be done, and with which resources. In the ISO 20000 standard a process is described like this:

> *"For an organization to function effectively it has to identify and manage numerous linked activities. An activity using resources, and managed in order to enable the transformation of inputs into outputs, can be considered as a process. Often the output from one process forms an input to another."*[105a]

Moreover a process does not have a time constraint and it is arbitrary repeatable.[SZ08]

The goal of IT governance is to manage IT in a way that the core business processes are optimally supported. Hence the IT processes have to be customized around these core processes. Examples of IT processes include planning, acquiring and implementing new hardware and software, managing customer/user support and handling the security of an IT system.

It is regarded to be harder to implement IT governance processes compared to IT governance structures.[HG08]

2.4.3 Frameworks

Frameworks are high level tools for implementing IT governance.

One can define frameworks as a collection of structures and processes including relevant documentation like procedure and policy descriptions required for an organization to assess, monitor and apprehend their current situation.[WPR06] In addition frameworks can be used in order to create metrics for a service, in order to measure the effectiveness against a predefined benchmark value.

Normally a framework does not prescribe how processes and structures are to be implemented; instead it focuses on what should be in place. This strategy has the advantage that a framework can be quite generally designed. In addition it enables an organization to customize the implementation and still be within the border of the framework.

In this work several IT governance frameworks are presented. Each framework has its own focus, depending on what is regarded to be important. The use of one framework like e.g. COBIT does not exclude the use of another framework like e.g. ITIL.

As most frameworks are quite extensive, organizations tend to use a long time before they have implemented all aspects of it. An organization has of course also the possibility to only implement parts of the framework, depending on the unique situation of the company.

2.4.4 Shortcut to effective IT governance

The advantage of effective IT governance is, due to dynamical changes in the business environment, hard to measure. Research among Belgian midsize financial service organizations indicates that high performing companies have more mature IT governance structures and processes than the average.[HG08] This implies that well implemented IT governance can be a competitive advantage.

It is easy to see the positive effects of a good IT governance system. To estimate the implementation cost in advance is however troublesome. Implementing IT governance is much about changing how employees and stakeholders work with technology. Factors like scope of IT governance implementation, corporate culture, attitude towards change and focus and experience of the management can have a major impact on the cost.

Implementing an IT governance system tends to be an incremental process in contrast to a big bang release. Based on research of Belgian financial institutions[HG08] the following six structures and processes are regarded most effectively and easy to implement, and could be considered as the first steps in implementing IT governance in an organization:

- IT steering committee.

- IT project steering committee.
- Portfolio management.
- IT budget control and reporting.
- CIO reporting to the CEO/COO.
- Project governance/management methodologies.

There is probably no easy shortcut to effective IT governance. IT governance is not like a machine that is implemented and then works for a long time without change. It is more correct to view it as a continuous process that is regularly reviewed and improved.

However, by working incrementally, focusing on the most important aspects for the industry and organization in question, taking advantage of existing IT governance frameworks and if possible employing experienced people, the result would most likely be acceptable in a cost - profit perspective.

Chapter 3

Implementing IT Governance

A range of standards, tools, frameworks and documentation has been developed in order to support the design and implementation of IT governance based management systems.

However, none of them is comprehensive enough to cover all needs in the process of implementing an IT management system. Research suggests that combining several frameworks could be more effective when designing an IT management system. E.g. ITIL could be used for defining strategies, plans and processes and COBIT for metrics, benchmarks and audits.[SSA08]

In this chapter two frameworks, COBIT in section 3.1 and ITIL in section 3.2, and one standard, ISO 20000 in section 3.3, are presented. The three were selected for detailed presentation in this work due to wide spread use and acceptance.

Maturity models measure how well an organizational process is operated in respect to performance and quality. Depending on how the different models define the term, either "capability level" or "maturity level" is used.

Capability Maturity Model (CMM) is one of the oldest and most wide spread used maturity models for IT, and have strongly influenced the development of other maturity models, including the COBIT maturity model as described on page 31. In this chapter CMM and its successor Capability Maturity Model Integration (CMMI) are presented in section 3.4 and 3.5.The concepts presented in those models do also influence the custom process maturity model developed in this work.

3.1 COBIT

COBIT is an abbreviation for "Control Objectives for Information and related Technology", and has, as the name suggests, its roots in the auditing industry. COBIT is a set of best practices for management of IT and is an international accepted framework for IT governance.[SSA08]

Originally COBIT was developed by ISACF (Information Systems Au-

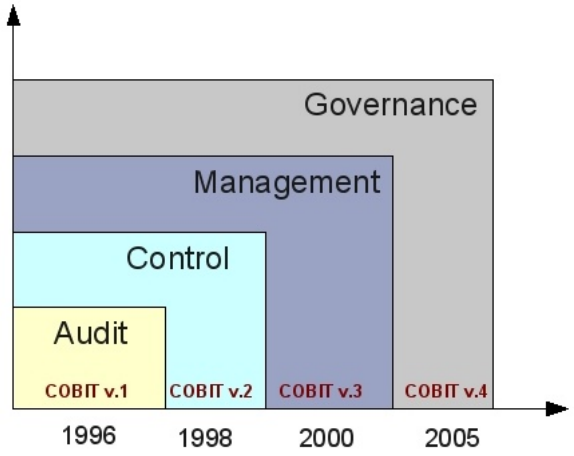

Figure 3.1: The historical development of COBIT. [May06]

dit and Control Foundation), the research institute of ISACA (Information Systems Audit and Control Association). ISACA is an international professional association with more than 75.000 members in 160 countries.[Wol06] [ISA08]

Since 1999 ITGT (IT Governance Institute) has been responsible for the COBIT development. ITGI is an independent research institution connected to ISACA with the objective of developing and providing information about IT enabled governance systems.[Gol06]

The first version of COBIT was released in 1996 with primary focus on auditing. New major versions were released in 1998, 2000 and 2005 and focused on control, management and governance respectively. As figure 3.1 shows, the scope of COBIT was extended with each new version released. Version 4.1, the newest version of COBIT, was released in 2007 and includes a full framework for IT governance. However due to its history, COBIT is still in many cases preferred by IT auditors and IT risk managers as the framework of choice.[Von05]

The main goal of COBIT is to manage IT resources in such a way that a maximum contribution towards the overall business goals of an organization can be achieved.

COBIT supports the implementation of IT governance by providing an extensive description of control objectives for IT processes. The control objectives describe what the desired output of a process should be. Additionally COBIT describes a system for measurement of the maturity of processes.

3.1.1 Acceptance and Awareness

Since its first release in 1996 COBIT has enjoyed attention and focus from the professional IT community, and as a result has been implemented in corporations world-wide. The rising awareness of IT governance due to regulatory restrictions like the Sarbanes-Oxley Act and Basel II has probably also contributed to the success.

Another explanation for COBIT's popularity is the extensive documentation that can, except for the audit guideline, be downloaded free of charge from the ISACA website.[RYC04] In addition to the full framework documentation, documents for a range of special purposes or target groups have been developed. Documents like e.g. "Board Briefing on IT governance", "IT Control Objectives for Sarbanes-Oxley" and "COBIT Quickstart" contribute to the popularity of COBIT as an IT governance implementation tool.

Surveys conducted by PricewaterhouseCoopers on behalf of ITGI claim that the awareness of COBIT among CEOs and CIOs has increased from 18% in 2003 to 27% in 2005. If analyzed by region, North America has the highest awareness with 32%, and Europe has the lowest awareness with 22%. Of the participants that were aware of COBIT, about 30% worked in organizations that used the framework to implement its IT governance strategy.

The surveys also show that organizations tend to use the control objectives, the audit guidelines and the executive overview in their COBIT implementation. The "COBIT Quickstart" document was not so often used. This can probably be explained by the fact that the quickstart guide is created specifically for smaller companies, and that smaller companies in general have lower COBIT awareness.[Pri06]

Several large organizations have implemented IT governance systems based on COBIT. This includes Daimler in Germany, Royal Philips Electronics in the Netherlands and the Department of Defense in the USA.[RYC04]

3.1.2 COBIT's Focus on IT Governance

According to ITGI the most important drivers for IT governance are lack of transparency of IT cost, value and risk. In COBIT transparency of IT cost is solved with the use of control objectives.

Control objectives are an essential part of COBIT and describe the quality of the output from defined processes. Moreover the control objectives describe on an abstract level how the processes are to be performed.[COB07]

COBIT defines five distinct focus areas for IT governance. Each defined process relates to one or more of these IT governance focus areas. Together all the 34 defined processes in COBIT are intended to provide complete IT governance in all focus areas. The five focus areas are:

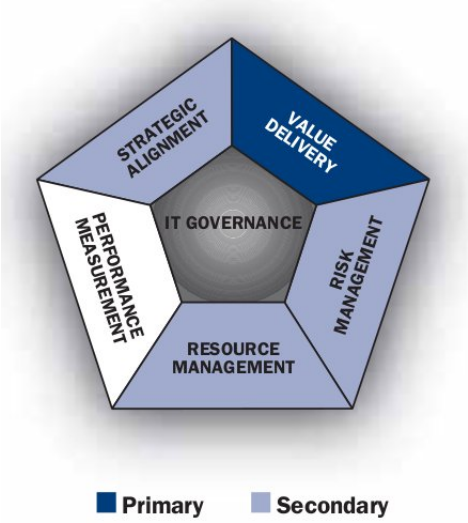

Figure 3.2: The IT governance focus areas of the COBIT process "Educate and Train Users."[COB07]

- Strategic Alignment - Processes focus on the compliance between IT goals, plans and operations with the overall business objectives.
- Value Delivery - Ensures that processes deliver the promised benefits, that costs of IT service delivery are optimized and that the intrinsic value of IT to the organization is used for competitive advantage.
- Resource Management - Processes tagged with this focus area deal with the investment and management of IT resources. COBIT defines IT resources as applications, information, infrastructure and people. Knowledge (people and information) and infrastructure are considered to be most important.
- Risk Management - These processes promote risk awareness, define risk strategies, estimate risk or embed structures for risk management into an organization.
- Performance Measurement - Ideally all strategic IT related processes and activities should be subject to some kind of monitoring in order to benchmark and improve the performance of delivered services. In specific performance measurement processes should monitor the use of resources, projects, and delivery of IT services.

Figure 3.2 shows the IT governance focus area of the process "Educate and Train Users." By educating users in the use of IT systems, several positive effects are expected. E.g. better quality of produced products

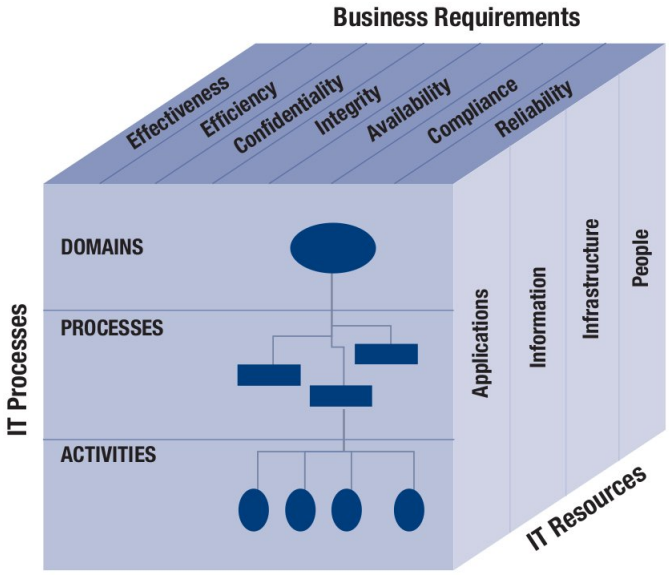

Figure 3.3: The COBIT cube.[COB07]

or services, increased productivity, better job satisfaction and better IT security.

Due to this, the "Educate and Train Users" process is tagged with "value delivery" as its primary IT governance area. In addition the process is tagged with several secondary focus areas, due to the fact that the process output has an effect on several aspects of an organization.

3.1.3 Structure

COBIT provides a framework for how IT resources and IT processes are to be organized in order to satisfy business requirements. This is visualized in figure 3.3.

The business goals and the strategy how to achieve them should determine the IT goals and the IT strategy. Moreover IT strategy is derived into processes that contain a series of linked activities. Hence the strategy of the business is executed by a range of activities which all are compliant with the goals of the business.

The general idea is that IT resources and information are managed in three layers, as visualized in the IT process dimension of the COBIT cube: domains, processes and activities.

In the activity layer of the COBIT cube, all kind of IT tasks are performed. An activity is a task with a defined result, as e.g. upgrade the software on a server, or register a helpdesk request.[Gol06] Activities are not described in COBIT, due to the high level business and auditing focus of the framework.

Several linked activities with a defined input and output are grouped into a process. COBIT defines 34 processes. Each process is assigned a set of control objectives in order to control the quality of the output from the process. In addition a description of the different maturity levels is provided, in order to measure how well implemented the process is.

Processes descriptions and associated control objectives and maturity levels are the core of the COBIT framework.

At the top level of the cube processes are consolidated into domains. Domains are often consistent with organizational requirements to IT.[Gol06]

According to COBIT information needs to comply with seven criteria, known as the business requirements for information. The criteria have some overlap and are supposed to provide a generic method for defining business requirements[COB07]:

- Effectiveness - Information should be relevant for the business process and should be delivered at the correct point in time and in a usable format.
- Efficiency - Provision of information should contribute to the productivity of the business process.
- Confidentiality - Sensitive information should be protected from unauthorized disclosure.
- Integrity - Information should be accurate and complete.
- Availability - Processes should have access to relevant information when needed.
- Compliance - Laws, regulations and contract arrangements need to be taken into account.
- Reliability - Management needs to rely on the provision of appropriate information in order to exercise their governance responsibility.

IT resources are the last dimension of the COBIT cube and consist of applications, information, infrastructure and people. People and Information are self explaining.

Applications are all kind of automated or manual procedures used to process information needed by the business. Infrastructure includes technology like servers, routers and operating systems in addition to facilities like server rooms and housing.

3.1.4 Processes

COBIT consists of 34 processes, all documented with the following structure:

- Process Description - Contains a general description of the process including the relevance to the business requirements for information, IT resources affected and to which IT governance focus area the process apply.(As described on page 23)
- Control Objectives - Describes which process activities should be measured. Control objectives are described in more detail on page 28.
- Management Guidelines - Describe the input and output of a process, a chart of responsibility, and how goals are derived into processes and activities.
- Maturity Model - Description of what is considered to be a well implemented process or not. More information about the COBIT process maturity model on page 30.

All COBIT processes have a unique identification based on which domain the process is assigned to. The 34 COBIT processes are divided into the following domains:

- Plan and Organize.
- Acquire and Implement.
- Delivery and Support.
- Monitor and Evaluate.

Generally the four process domains are to be considered as a loop where the output from one domain is the input to the next domain. E.g. the processes in the "plan and organize" domain primarily deliver input to the processes in the "acquire and implement" domain, and secondarily to the processes in the "monitor and evaluate" domain.[Gol06]

The "plan and organize" domain deals with the strategy and tactic of how to reach the business goals. Important aspects that have to be taken into account include the optimal use of resources, assessment of risks and comprehension of core business compliant IT objectives.[May06] The implementation of the strategy has to be planned and communicated throughout the organization.

Processes for the implementation of IT strategy are collected in the "acquire and implement" domain. In order to implement an IT strategy, the application portfolio needs to be extended with either externally acquired or internally developed products. Important issues are the transformation of high level strategy plans to detailed product requirement specifications, the security of the quality of developed or acquired solutions, and knowledge transfer to the end users and supporting staff.

In the "deliver and support" domain processes for operating the IT systems are collected. This is the domain that contains most processes, and ranges from processes for system security to cost control. In addition processes for management of user reported failures or problems and education of users are described.

The "monitor and evaluate" domain contains processes that on a regular basis should assess the quality of the implemented IT processes. Structural or procedural problems related to how IT governance is implemented should be discovered and improvements should be continually implemented. Moreover the performance of the implemented IT processes should be compared with the initial IT strategy defined in the "plan and organize" domain. If strategy and reality differ, corrective actions have to be taken.

Figure 3.4 on page 29 shows all 34 COBIT processes in relation to the four domains described above.

3.1.5 Control

Controls are implemented in order to be able to measure into what extent business objectives are achieved, and to discover undesired effects or events of an IT process implementation. Control of IT processes plays a key role in COBIT, and all the 34 defined processes have their associated control objectives.[COB07]

COBIT provides two types of controls for IT processes: specific control objectives for each process and generic process controls for all processes.

The specific control objectives are adapted to each process and could serve as a template for a specific implementation. E.g. the process "assess and manage risk" has six distinct control objectives. The control objectives are normally specific, like to ensure that risk assessment is performed or to check that a response to defined risks is defined.[COB07]

The process controls(PC) are generic for all processes and can also be used to check the quality of customized IT processes. The process controls are numbered from one to six:

- PC1 Process Goals and Objectives - A process should be clearly defined and linked to the business goals.
- PC2 Process Ownership - Ownership of processes should be defined.
- PC3 Process Repeatability - A process needs to be repeatable and produce the expected results. Processes should however allow exceptions to occur.
- PC4 Roles and Responsibilities - It should not be unclear, who is responsible for which step in the process.

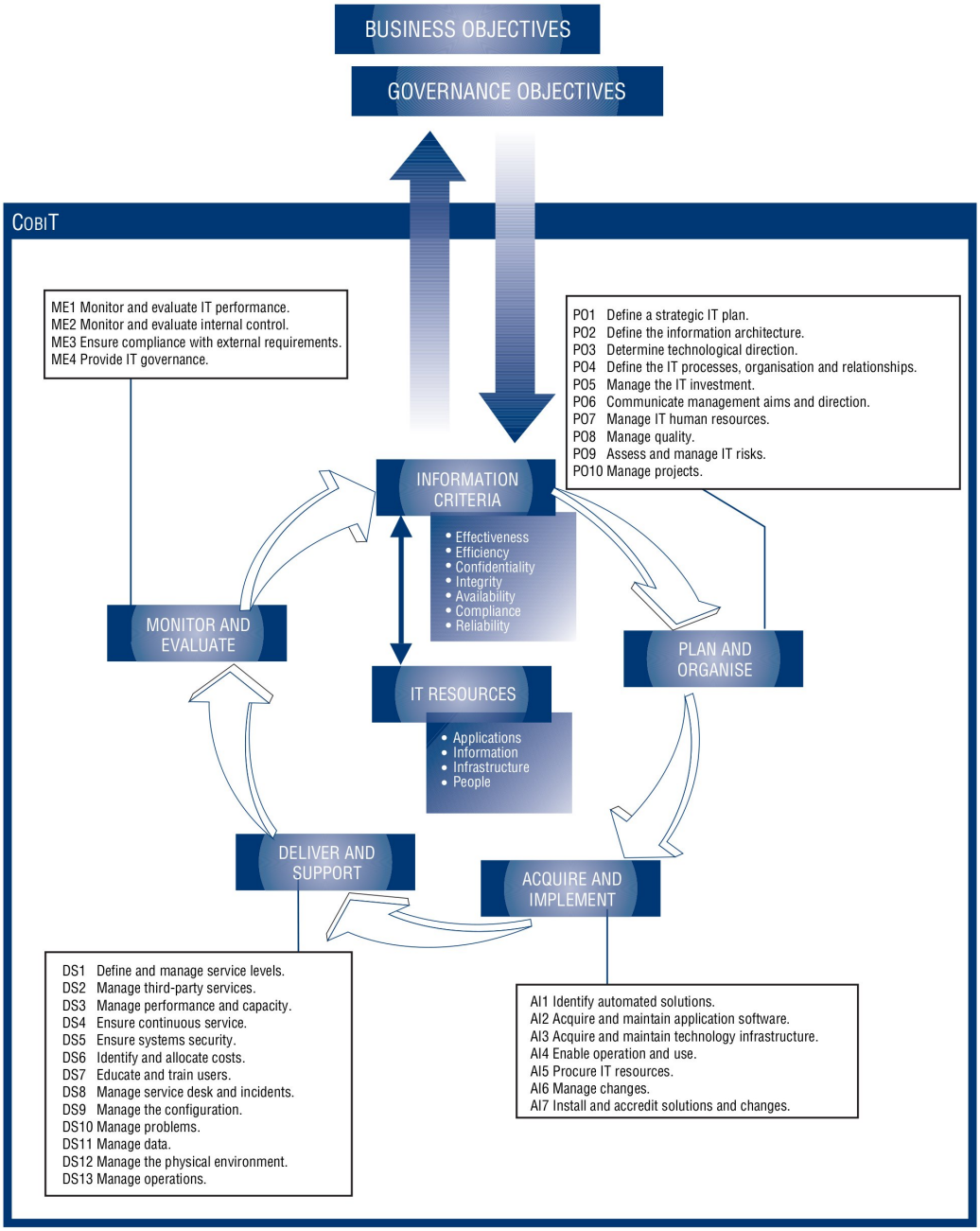

Figure 3.4: Overview of all COBIT processes.[COB07]

- PC5 Policy, Plans and Procedures - Sufficient documentation should exist, and on regular basis be reviewed and updated.
- PC6 Process Performance Improvement - The process outcome should be compared with the expected outcome, and the process should be optimized if necessary.

3.1.6 Business Goals and Performance Measurement

Setting goals and measure into which extent they are achieved is vital for all organizations working to improve their governance structures.

COBIT differs between business, IT, process and activity goals.

Ideally a top-down approach is used when defining goals. Business goals will determine IT goals. Process goals will be derived from IT goals, and activity goals will be determined by the process goals.

COBIT provides goals for the IT, process and activity level for the 34 defined processes. Business goals are not defined.[COB07]

Due to unique business environments, corporations probably have a unique set of business goals. These business goals will influence the IT, process and activity goals of the organization. Hence, the COBIT defined goals are to be considered as guidelines, and should not be implemented without a careful review and prioritization in relation to the specific business goals of the business.

In order to measure whether a goal is achieved or not, COBIT defines two metrics:

- Outcome Measure[1] - indicates if the corresponding goal has been reached or not.
- Performance Indicator[2] - investigates if a goal is likely to be achieved. It can be used before the outcome is clear.

3.1.7 Process Maturity Measurement

All corporations need to measure the performance of implemented IT processes. Measurement provides answers to how well IT processes are managed, and how well they support the core business processes. Additionally process owners need to know the current status of their processes in order to recognize areas of improvement. Moreover a performance measurement enables the benchmarking with either other companies in the industry or company internal.

[1] In older versions of COBIT are Outcome Measures referred to as "Key Goal Indicators" (KGI).

[2] In older versions of COBIT are Performance Indicators referred to as "Key Performance Indicators" (KPI).

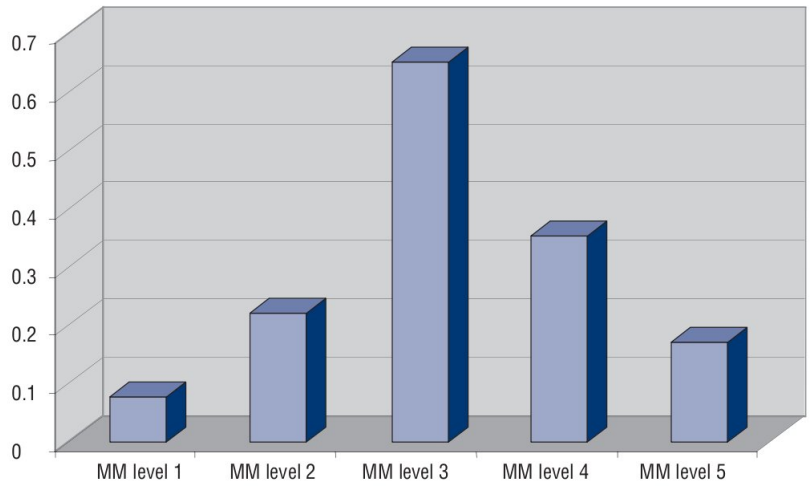

Figure 3.5: Possible profile of the maturity level of a COBIT process. [COB07] (MM=Maturity Model)

COBIT provides a maturity model that in six levels classifies how well managed a process is. The maturity model is derived from the "Capability Maturity Model" (CMM) originally created by the "Software Engineering Institute" (SEI).[Pop07]

In contrast to CMM the COBIT process maturity model does not measure the maturity in a detailed and precise way, and does not pinpoint a process to a single maturity level. Instead the model indicates how mature a process is, and should be used in order to create a profile of the process maturity.[COB07] Figure 3.5 shows an example of such a profile, where the process satisfies some of the requirements for several maturity levels, even though level three is the predominant one.

Each of the 34 COBIT processes contains a description of what attributes the six maturity levels. The six levels are in general terms described in the list below:

0 Non-existent - There is no evidence that the process exists or that the management recognizes the need for the process.

1 Initial/Ad Hoc - The management recognizes the need for the process, but no process exists.

2 Repeatable but Intuitive - The process is implemented, but no formal training is undertaken. The process relies on knowledge by individuals.

3 Defined Processes - Process is implemented, documentation exists, and training is undertaken. Deviation from the defined workflow will most likely not be detected.

4 Managed and Measurable - The process is monitored and improved. Some use of automation and tools.

5 Optimized - The process is continuously improved, benchmarking with other organizations is done. Tools and automation are applied. The process enables quick adaptation to new business requirements.

3.2 ITIL

Information Technology Infrastructure Library (ITIL) is a collection of best practice methods enabling effective IT Service Management (ITSM). In ITSM the customer and the service provider are connected through the delivery of IT services.

In this work, and in ITIL, are the terms "customer" and "supplier/service provider" used for describing an entity requiring, respectively providing, an IT service. The terms are used for both the entities that are external (e.g. a supplier) and internal (e.g. another business unit in the organization) to an organization.

The focus of ITSM is on customers, processes and quality. ITIL provides a set of best practices in order to combine the ITSM focus areas for optimal customer value.[Köh07] ITSM is process-oriented, and is concerned with issues like delivery and support of IT services and management of IT infrastructure and applications. In addition the alignment of IT services with the business goals is a core issue.[SZ08]

ITIL defines "service management" simply like this:

> *"Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services."*[itS07]

The "specialized organizational capabilities" in the ITIL definition refer to all processes, methods, functions, roles and activities a service provider has to carry out in order to deliver a service.

The outcome of a service is the reason for the customer to buy a service from the supplier. Hence the focus of the supplier should be to deliver the expected value to the customer. ITIL supports the process of making the supplier understand the real needs of the customer and implement and deliver the required service.[itS07]

Even though ITIL defines "what" to do and not "how" to do it, ITIL itself is not a standard, but a collection of best practice methods. Hence it is not possible for an organization to obtain a "ITIL certification."

If an organization claims to be ITIL compliant it normally means that it has adopted all or some of the ITIL core processes. Currently the only

possible official formal validation of ITSM an organization can obtain is the ISO 20000 certification.[3][SZK08]

ITIL tries to solve the IT governance challenges in almost the same way as COBIT does. However, COBIT tends to be more general in its form and is more focused on the auditing perspective than ITIL is.

Research has recognized that the two frameworks both have their strengths and weaknesses and that they can be combined in order to gain an optimal effect. It is suggested that ITIL based processes are used for defining strategies, plans and processes and that COBIT builds the foundation for metrics, benchmarks and audit processes.[SSA08]

The implementation of ITIL in an organization does not exclude the implementation of COBIT. They are both to be considered as recommendations or templates and not as standards that do not allow customization.[Köh07]

3.2.1 Acceptance and Use

Due to a long history and worldwide use and acceptance, one can assume that the quality of the ITIL framework itself and the applicability as a general purpose framework for management of IT services is ensured[Hei08]

Examples of organizations that have selected ITIL as their framework of choice include corporations like Procter & Gamble, Microsoft, Hewlett-Packard and several governmental organizations and academic institutions.[MD07] [Gre07]

ITIL is claimed to be the best known IT service management framework in the world with 98% awareness level.[SZ08] [itS07] A survey among 160 decision makers in large German and Austrian IT organizations shows that the rate of implementation is rising. While 50% of the companies had ITIL based IT service management systems implemented in 2005, the number was 76% in 2007.[Gmb07]

Even though ITIL is often associated with large corporations, it is supposed to be a general framework for all kind of IT organizations, irrespectively of size or technology in use.[itS07]

3.2.2 Development of ITIL

In the 1980s the "Central Computer and Telecommunications Agency" (CCTA) was appointed by the British government to investigate if the use of IT resources in the public sector could achieve a higher degree of cost effectiveness.[SZ08] The results were published from 1989 to 1995 under the name ITIL and consisted of 31 books covering all aspects of IT service provision.

The CCTA was later renamed "Office of Government and Commerce" (OGC). OGC is now the official owner of the ITIL framework.

[3]ISO 20000 superseded BS 15000.

In 1999 ITIL Version 2 was published. The original 31 books were revised and replaced by seven more closely connected books. ITIL V2 became accepted worldwide as the framework for IT service management. Most organizations that claim to be ITIL compliant have based their implementations on ITIL V2.

In 2007 OGC released the third version of ITIL. This version combined and revised the knowledge of the previous versions into five books plus an official introduction to the framework in general and the service life cycle in special.[itS07]

While ITIL V2 was divided into seven books, where "Service Support" and "Service Delivery" was the most famous one, ITIL V3 is more closely connected to the service life cycle, as illustrated in figure 3.6. Moreover version three is more focused on the business value and provides the basis for the use of the Balance-Score-Card (BSC) system in an organization.

Version two and three are compatible. All version two processes are present in version three, but the arrangement of them within the books has changed. Version three is compliant with ISO 20000.[SZ08]

In addition to the five core books, ITIL V3 comes with a set of complementary publications. These publications include case studies, templates, an executive summary, a detailed list of quick wins, documents on scalability etc. In addition a website with the address www.itil-live.portal.com will provide more information on the process model.[itS07]

Even though ITIL V3 has not yet become as dominant as ITIL V2, all subsequent references to ITIL in this work will refer to the third version of the framework.

3.2.3 The ITIL Service Life Cycle Model

The service life cycle contains five elements, as shown in figure 3.6. These five elements are described in five corresponding ITIL books. Each of the five elements relies on a set of service design principles, processes, roles and performance measures. The five core elements are:

- SS - Service Strategy
- SD - Service Design
- ST - Service Transition
- SO - Service Operation
- CSI - Continual Service Improvement

The service life cycle has a "hub and spoke" design. Normally an IT service would go through all the five elements in a sequential order. From

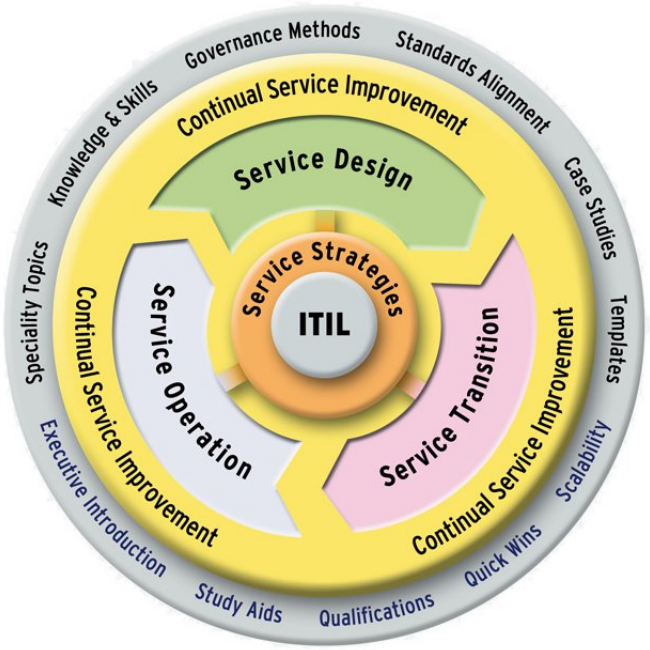

Figure 3.6: The ITIL Service Lifecycle.[ITI08]

the Service Strategy as hub, the service goes through Service Design, Service Transition to Service Operations as spokes. At the end the processes will be measured and improved by the processes in Continual Service and Improvement.[oGC07f]

ITIL does however recognize that the world is not always that static and allows for every element in the life cycle to provide feedback and control, meaning that a service can be continually improved without delay due to bureaucratic reasons.[itS07] [oGC07f]

In detail Service Strategy provides guidance in defining strategic objectives, prioritizing investments and defining key measures for the effective implementation of services.[oGC07d]

Further Service Strategy deals with analyzing the need of the customer and from that derives which services should be offered. Decisions have to be taken in order to determine the general borders of the subsequent management of the service. E.g. who should offer the service, what should distinguish the service from other similar competitive services and how is the performance to be measured.

Service Strategy defines several key processes in order to achieve its defined goals. The most predominant ones are Financial Management, Service Portfolio Management and Demand Management.

The Financial Management process is about budgeting and accounting, in addition to operational forecasting. Financial Management enables IT organization and the business to express in financial terms the cost and benefit of the consumed IT services.[oGC07f]

In the Service Design phase the output from the Service Strategy is made concrete and services are defined and prepared for implementation.

The goals of Service Design is to design IT services that meet agreed business outcomes and support the service life cycle. Relevant assets to this phase are the ITIL defined four Ps of design: People, Products, Processes and Partners. Good service design combines the four Ps in an optimal mix in order to achieve effective IT service management.[oGC07b]

Some of the key Service Design processes include Service Level Management, Capacity Management and Information Security Management.

In the Service Level Management process the levels of the delivered services are negotiated and documented. In addition the running services are monitored and in reports compared with the agreed service level.

Capacity Management determines, monitors, plans and forecasts the capacity of the IT processes and the underlying technology throughout the whole service life cycle. All capacity relevant information is stored in one central place called the Capacity Management Information System (CMIS), and is used by all processes demanding capacity information for planning, reporting etc.

The purpose of the Information Security Management Process is to align IT security with business security and ensure that information is well managed in respect of availability, confidentiality, integrity and authenticity. Security management should be controlled by a central policy.

The goal of Service Transition is to plan and manage service changes and to successfully implement service releases into the production environment. [oGC07e]

Key principles of the Service Transition phase include understanding of the service and its utility, establishment of a formal policy for changes, supporting knowledge transfer, proactive adapt and adjust services and ensure involvement in the whole service life cycle.[itS07]

In the Service Transition part of ITIL several processes are defined. Some of them have a global perspective of the whole service life cycle process, and some are local to the Service Transition phase.

One essential process of ITIL is the global process of Change Management. The objective of the Change Management process is to ensure that changes to a service are traceable and not implemented in production before the change is evaluated, tested and documented. A workflow is defined which ensures that a Request for Change (RFC) is not implemented before the objectives of the Change Management process have been fulfilled.[oGC07e]

Process Groups	**Processes**
Service Strategy (SS)	Strategy Generation Financial Management Service Portfolio Management Demand management
Service Design (SD)	Service Catalog Management Service Level Management Capacity Management Availability Management IT Service Continuity Management Information Security Management Supplier Management
Service Transition (ST)	Transition Planning and Support Change Management Service Asses and Configuration Management Release and Deploy Management Service Validation and Testing Evaluation Knowledge Management
Service Operation (SO)	Event Management Incident Management Request management Problem Management Access Management
Continual Service Improvement (CSI)	7-Step Improvement Process Service Measurement Service Reporting

Table 3.1: Complete list of processes in ITIL V3. [itS07]

The focus of the Service Operation book of ITIL is to manage the day to day operation of the IT services. At this stage the actual value for the business is created. In addition the greater context of the ITIL service life cycle has to been taken into account in order to optimize the quality and cost of the provided services.[oGC07c]

Incident Management is a key process of Service Operations. An incident is an unplanned disturbance of the delivered service. This can be reported to the help desk by a user, or detected by other processes like the event management process.

An incident is either resolved quickly by e.g. the service desk, or it might be passed on to a technical support team with the required skills. If the incident has an impact on the business, a notification or escalation to the management might be appropriate as well. An incident is closed, when the problem is solved and the service desk can confirm this with the user.[itS07]

When an IT service is designed and successfully implemented in the ITSM system, many corporations are satisfied with simply maintaining status quo. This is not a very wise strategy. An implemented process always has room for improvement and ever changing business environments require adaptation.

The Continual Service Improvement part of ITIL consists of processes that focus on increasing efficiency and lowering production cost of IT services. Continual Service Improvement's processes are not to be executed at the end of a service implementation, instead improvement and optimization opportunities have to be identified in all phases of the life cycle.[oGC07a]

Table 3.1 displays a complete list of all the ITIL processes in relation to the five phases in the service life cycle model.

3.3 ISO 20000

ITIL provides guidelines for effective operations of IT service management. It does not however provide requirements for IT service management, hence cannot be used for certification purposes. This means that an organization cannot be ITIL certified. [4].[Hei08]

With ISO 20000 it is possible to certify the IT service management implementation in an organization.

A common misconception is that ISO 20000 is an ITIL standard or certification. Even though ITIL and ISO 20000 are compatible and have close historical ties, ISO 20000 is specifically and intentionally developed so that other best practice frameworks can be used as a basis for meeting the requirements as well.[DT08]

A certification is a proof that the managed IT services are delivered according to formal and international accepted specifications. The audit and certification are always done by an independent and approved audit organization.

Corporations and IT organizations might have different reasons to obtain the ISO 20000 certification. In industries where the quality of IT services is especially important, such as in financial and health service industries, it is important to demonstrate to stakeholders and customers that the IT services are produced correctly. For outsourcing organizations a certification is important for building customer trust and for creating or maintaining a good reputation. In addition an ISO 20000 certification can be used in order to prove compliance with different regulatory requirements like the Sarbanes-Oxley act.[Tur08]

ISO 20000 operates with the term service provider. A service provider is defined as the organization that tries to achieve the ISO 20000 certification.[105a]

[4]Persons can be ITIL certified in a three layer program: Foundation, Diploma and Advanced Service Management Certification.[itS07]

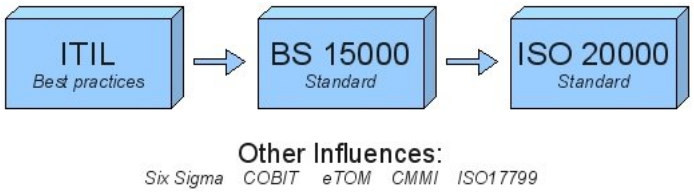

Figure 3.7: Evolution of ITSM.[GQDC07]

This does not mean that ISO 20000 is a standard for IT companies. The service provider might as well be the internal department of a corporation in a complete different industry, delivering only internal IT services.

The ultimate goal of ISO 20000 is to reduce exposure to operational risk, to meet contractual requirements, and to ensure the quality of delivered services.[Tur08] This is achieved by requiring the implementation of certain processes organized in five domains. The processes are described with objectives and a set of output requirements for the processes.

The ISO 20000 standard is a result of standardization work done by the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO). Hence the official identification of the standard is ISO/IEC 20000.

The standard itself consists of two documents:

- ISO 20000 Part 1: Specification - In this document processes including goals and outcome requirements are defined. This is the part an organization seeking the certification is tested against.
- ISO 20000 Part 2: Code of practice - This document contains the guidance and recommendations for the standard and provides extended information of how the standard is to be implemented. It should however always be used in conjunction with part 1.[105b]

3.3.1 Development of ISO 20000 in the context of ITIL and BS 15000

Several different standards and frameworks were consulted when ISO 20000 was developed. Predominant in the development was the British Standard (BS) 15000 that served as a kind of template for ISO 20000.

BS 15000 was developed by British Standards Institution (BSI) in close cooperation with the IT Service Management Forum (itSMF)[5] and a set of commercial and public partners.[TK05] It describes an IT service manage-

[5]itSMF - IT Service Management Forum - is an international, non-profit, independent association of IT service management professionals[BMOP06]. Homepage: http://www.itsmfi.org/

ment system according to ITIL and was the first formal standardization in this area. BS 15000 was released in 2000 and consists of two parts.[Köh07]

The first part is called "specification" and describes the requirements for an ITSM system. The second part, with the name "code of practice", contains information about the auditing process.[Köh07]

Moreover BS 15000 provides a manager's guide and a self assessment workbook. The latter can be used by a service provider organization to test the compliance of their processes with BS 150000.[Hei08]

Figure 3.7 shows how ITIL and BS 15000 influenced the development of ISO 20000 in the context of IT service management.

BS 15000 was an important reason for the increased focus on IT service management around the world. Due to its popularity it was considered imperative by ISO/IEC to develop an international standard for IT service management. ISO 20000, released in 2005, was developed in a special fast-track process with BS 15000 as template.[CJ07]

Due to the special fast track process and general acceptance of BS 15000, the ISO 20000 standard does not introduce many changes for companies that have implemented an ITSM system based on BS 15000.[IT08]

ISO 20000 contains some minor differences to ITIL V2. ITIL V3 was published in May 2007, and one of the goals was to make the framework more aligned with the ISO 20000 standard. One of the major changes in ITIL V3 is that the service life cycle approach is more in line with ISO 20000 than the approach used in ITIL V2. Studies show that ITIL V3 in general is more compliant with ISO 20000 than what ITIL V2 was. Nevertheless, both versions describe ITSM systems that fulfill the general requirements of ISO 20000.[DT08]

Even though BS 15000 and later ISO 20000 both have a close connection to ITIL, they are generic, and can be used to certify the quality of ITSM systems based on any other framework or practice as well.[DT08]

ISO 20000 supersedes BS 15000.[Tur08]

3.3.2 Continual Improvement

One of the core issues of ISO 20000 is the continual improvement of the implemented processes. This is done in ISO 20000 by using the Plan-Do-Check-Act (PDCA) model.

Originally the model was developed by Walter Shewhart and later by Edward Deming for the use in the area of quality management in the manufacturing industry.[JPKS+98] Due to the generic nature of the model, it is easy to adapt to different situations and industries. The PDCA model has been applied to different IT related quality issues as e.g. service management and IT security.

In ITIL V3 the PDCA model is incorporated in the form of a service life cycle model as displayed on page 35, which also has the ultimate goal of

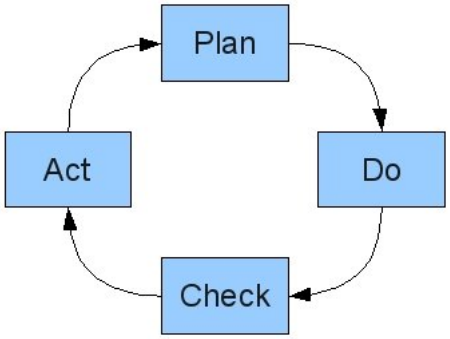

Figure 3.8: The PDCA model.

continual process and service improvement.

As figure 3.8 shows the PDCA model is displayed as a cycle, where one iteration equals one major quality improvement implemented in the system.

ISO 20000 describes the four stages in the PDCA model as the following[105a] [105b]:

- Plan - A plan for how ITSM is to be implemented in the organizations has to be created. The plan should most importantly contain documentation of the objectives of the ITSM together with the necessary processes. The scope of the ITSM in relation to e.g. organization, location or managed services should also be documented. In general the plan should contain all relevant aspects of the system, however, if the goal is to obtain an ISO 20000 certification, the plan needs to at least address some specific issues listed in part one of the ISO 20000 documentation.

- Do - In this phase the plan created in the first phase is implemented in the organization. Funds and budgets for service management are ensured, employees are assigned roles and responsibilities, teams are built, documentation is created and maintained, risks are managed and the service management process is coordinated.

- Check - The third phase of the PDCA model is concerned with the monitoring, measuring and reviewing of the ITSM performance in relation to the documentation created in the first phase. Reviews on regular intervals are to be conducted by the management. An audit program should be implemented with the objective of checking the correct implementation of the defined processes. The audit criteria should be documented in the process documentation. Auditors do not need to be company external, but auditors should of course not check their own work.

- Act - The objective of the last phase is to improve the service delivery and the management. Information from the check phase is used in order to identify areas of process improvements. A policy for improvement of the services should exist, and roles and responsibilities for service improvement activities should be assigned. As in the ITIL life cycle model, the improvement of processes and services should not be an activity merely at the end of Check phase. It is a requirement in ISO 20000 that room for improvements has to be identified, reported and managed on a continual basis.

3.3.3 ISO 20000 Requirements

Figure 3.9 shows that the ISO 20000 requirements for an effective ITSM are divided into eight groups. This is also the document structure of the specification itself.

Three of the requirement groups are generic requirements to the whole ITSM system and five groups are requirements for the ISO 20000 defined processes.[105a]

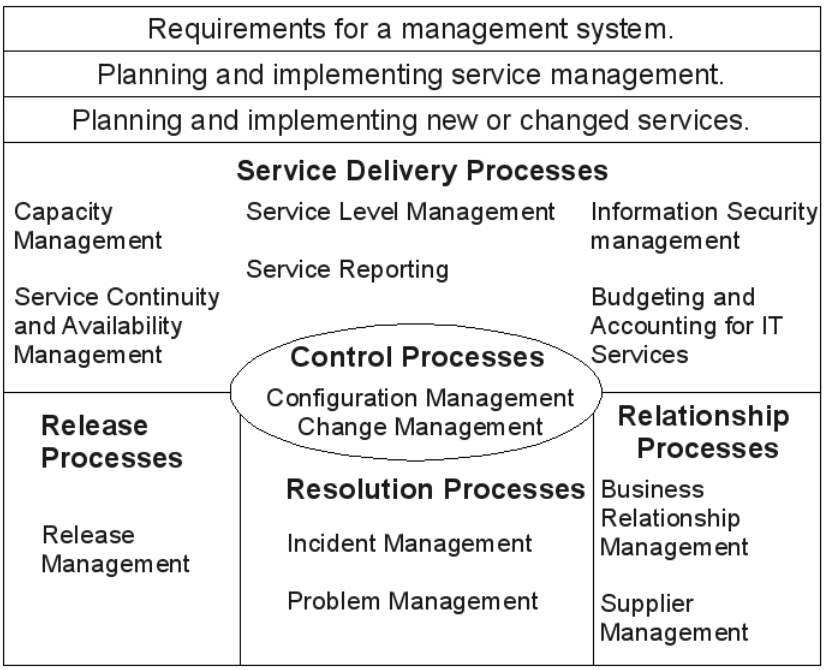

Figure 3.9: Groups of ISO 20000 requirements.

In the group "requirements for a management system" the responsibility of the management, documentation requirements and management of competencies and knowledge are defined. All requirements in this group are

quite general and have the objective of enabling the effective management and implementation of an ITSM system.[105a]

The requirements presented in the "planning and implementing service management" group are concerned with the continual improvement of services and processes with the use of the PDCA model, as described in more detail on page 40.

The objectives of the requirements group "planning and implementing new or changed services" are to ensure that the proper considerations have been done before a new or changed service is implemented. This includes everything from cost, organizational impact and technical challenges to commercial issues. Control is ensured by demanding the implementation of a change management process and that all service changes, including closure of a service, are to be done within the realm of this process.

In ISO 20000 eleven processes are described and organized into five different process groups. Each process is associated with a set of requirements.

The Service Delivery Processes

Service Level Management - Defines, stores and manages service levels. For each service a Service Level Agreement (SLA) is defined. The SLA documents the service and ensures that the customer and the service provider have the same level of expectation. All SLAs are stored in a service catalog. The service catalog should be easily accessible for both customer and service provider.[105b]

Service Reporting - Collects data and creates reports in order to provide information for decision making. All other ITSM processes depend on the information produced in the service reporting process. Reports can be of reactive, proactive or forward scheduled type. Reactive reports present data from the past. Proactive reports uses collected data to predict issues that could cause problems in the delivery of the services. The forward scheduled reports inform about planned activities. This process produces reports for both the customer and the internal management of the service provider.[105b]

Service Continuity and Availability Management - The goal of this process is to ensure the continual delivery of the agreed services to the customer under all circumstances. The agreed service level in respect to availability, in form of an SLA, is the input to the process. When the requirements are found, availability and service continuity plans have to be developed. The plans should additionally to the provision of information on how to keep the service running, include data on how to restore a service to normal, in case of an unplanned service halt. The plans are to be reviewed at regular intervals. The change management process should update the plans when appropriate.[105b]

Budgeting and Accounting for IT Services - The cost of service provision

can be very complex to calculate. This process ensures that service providers do not simply estimate their cost of production, but truly investigate the real cost of the services. This includes dividing indirect costs in an appropriate ratio to the relevant services and control the relevant direct costs. In ISO 20000 this process is required for budgeting and financial control, but not for charging the customer, as the standard is supposed to be applicable for company internal as well as company external IT organizations.[105b]

Capacity Management - Every change has an impact on the performance of an IT system. Changes include not only hardware, software and other assets, but also organizational changes due to e.g. regulatory requirements. The capacity management process shall ensure that the service provider has at all time the necessary capacity to fulfill the SLA. This includes the monitoring of service capacity and the estimation of the impact a change request has on future capacity.[105b]

Information Security Management - ISO 20000 requires the development of an information security policy. The policy should be approved by the management and all relevant personnel should have access to it. The process should ensure that the security plan is implemented and that risks regarding access to the system or service are managed. Formal agreements should regulate the access persons from external organizations have to restricted information. Security incidents should be recorded and monitored and used as a basis for the improvement of the process.[105b]

The Relationship Processes

Business Relationship Management - The process regulates the relationship between the service provider and the customer. The service provider is required to document all stakeholders and customers of a service and invite them at least annually to a service review meeting. A complaint process should be implemented by mutual consent with the customer. The service provider should appoint an employee to be responsible for the business relationship process.[105b]

Supplier Management - The service provider needs a structured management of its suppliers. A named individual is responsible for the contract management for each supplier. The interface between processes on the supplier and the service provider side has to be documented. The service provider has to monitor all its suppliers in order to ensure that the suppliers fulfill the agreed service level.[105b]

The Resolution Processes

Incident Management - All incidents that cause a disruption of services should be recorded. This includes problems reported from users (e.g. to Helpdesk), but could also be incidents found by the service provider orga-

nization. Incidents should be recorded with meta information like impact on the business and priority. The customer should be kept informed of the progress of the reported incidents. Escalation procedures should be in place.[105b]

Problem Management - Several incidents can be reported, but they might be caused by one underlying problem. If e.g. one user cannot print documents and another user can not send e-mails, the underlying cause could be a defect switch in the network. This process identifies and solves the real cause of incidents. In addition number and type of incidents and problems should be monitored in order to take preventive actions. Moreover the problem management process should keep the incident management informed about known errors and solved problems.[105b]

The Control Processes

Configuration Management - All items relevant for the delivery of the agreed IT services should be documented and recorded in a Configuration Management DataBase (CMDB). With the use of the CMDB items should be identifiable, controllable and traceable. The relationship between items should be documented. This process provides information to other processes, as e.g. to the change management process in order to estimate the impact of a proposed change. The goal of this process is to maintain accurate configuration information of the service and required infrastructure.[105b]

Change Management - In order to minimize the risk of service disruption, changes need to be assessed, approved, implemented and reviewed. This includes service as well as infrastructure changes. Before a change is considered for implementation, it should be documented with certain meta information as classification, urgency etc. Assessment of possible changes should include risk, impact and benefits for the customer/business. All changes should also provide a fallback plan, in case the changes need to be reversed. After implementation the change should be reviewed. A special fast track procedure should exist for emergency changes.[105b]

The Release Process

Release Management - The service provider is required to plan the release of services and infrastructure like software and hardware in a controlled manner. Release plans should be approved by all relevant stakeholders and especially the customers of a service. All releases should be tested and accepted in a test environment before distribution. The process should include a plan for how to revert to a previous state in case a release was unsuccessful.[105b]

3.4 CMM

The Capability Maturity Model (CMM) is a framework for improving processes in software developing organizations. CMM describes the maturity of processes on a five levels scale and can be used for increasing the quality and predictability of these processes. [EDBS05]

Even though CMM and its successor Capability Maturity Model Integration (CMMI) are developed by the Software Engineering Institute (SEI) at the Carnegie Mellon University, it is not solely a theoretical or academic construct but is applied to many large governmental and commercial organizations world-wide. About two thirds of the organizations working with CMMI have a commercial character and the rest are military or governmental agencies including their contractors. [SEI07]

3.4.1 Critique of CMM

CMM is focused mainly on measuring and improving processes in software developing organizations. Software development life cycle models like the waterfall, the prototype or the spiral model apply technical oriented engineering activities for quality improvements. CMM on the other hand works with less technical oriented activities like e.g. project management and supporting activities in order to achieve its goals.

The authors of CMM designed the framework to be independent of a specific software life cycle model. A study of the relation of CMM and the software life cycle model does however criticize CMM to bear close resemblance to the waterfall model. [SZ07]

Another critique of CMM is that it requires a high degree of attention on processes and that this can cause less focus on customers and shareholders. If the business objectives and the changing business environment are not given enough focus, a CMM implementation could risk being an obstacle for change and adaptability. [EDBS05]

3.4.2 Evolution of CMM

In the 1970s an 1980s the Department of Defense (DoD) in the USA experienced problems related to quality, cost and time of delivery of its software development projects outsourced to external contractors. [Tat08] In order to avoid future problems the DoD requested in 1986 the Software Engineering Institute at Carnegie Mellon University to develop a model for how to assess their software contractors. [BH02]

The initial model, which was developed with the assistance from MITRE Corporation, was released in 1987 and contained two methods and one questionnaire. Combined they could be used for appraising the process maturity and process capability in software developing organizations. [PWCC95]

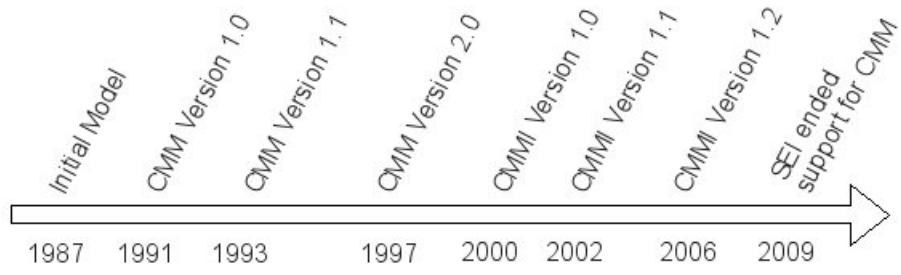

Figure 3.10: Evolution of CMM and CMMI

In 1991, after four years of experience and development based on the two developed methods and the questionnaire, SEI released the first version of CMM. The goals of CMM were on the one hand to provide a method for assessing the maturity of processes in software developing organizations and on the other hand to provide methods for process improvements. [Tat08]

The initial version of CMM was used by the software community, and feedback from industrial and governmental organizations contributed to the ongoing SEI research in the field of process maturity and capability determination. Special studies were conducted into how CMM had to adapt in order to support non-software developing organizations. In 1993 CMM was released in version 1.1. [PWCC95]

In 1997 a version 2.0 of CMM was developed, but was withdrawn shortly before actually released on request from the DoD. It was considered to be a problem how CMM had evolved since its initial version. The first version of CMM was focused on software development. Later other CMM models, like for e.g. system engineering, were developed. The critique was that the different CMM models had compatibility issues and were hard to combine.

Due to these reasons a new project with the name Capability Maturity Model Integration (CMMI) was initiated. The goal of this project was to build a common framework for the different CMM models and make them compatible with each other.

In 2000 the pilot version of CMMI was released. This version covered software and system development. Later another CMM module, the Integrated Process and Production Development (IPPD) module, was adapted and added to this version as well. The CMMI version 1.1 was released in 2002 and continued the integration of the different models into one model. [Kne06]

The latest CMMI version is version 1.2 released in 2006. It currently consists of two models:

- CMMI for Acquisition (CMMI-ACQ)
- CMMI for Development (CMMI-DEV)

CMMI-ACQ provides a best practice framework for acquiring products and services. The focus of the model lies on the acquirer. It contains 22 process areas covering all parts of the purchasing process, including project and risk management. [Uni07]

The purpose of CMMI-DEV is to provide a best practice framework for improving and assessing the product or service development processes in an organization. While the original CMM and CMMI version 1.1 were designed to assess and improve software development processes, the CMMI version 1.2 has a more generic nature. Older versions of CMMI contained models for system engineering (CMMI-SE) and software engineering (CMMI-SW). Both these models are now superseded by the more generic CMMI-DEV. [Uni06b]

In addition to CMMI-ACQ and CMMI-DEV the CMMI version 1.2 describes a third model, CMMI for Services (CMMI-SRC), that was released in February 2009. The CMMI-SRC is designed for managing services from the establishment to the delivery phase. In the terms of CMMI a service is simply an intangible, non-storable product. CMMI-SRC is supposed to support all kind of organizations delivering services regardless of industry. [Uni06a]

In 2003 SEI limited the support of CMM and recommended an upgrade to CMMI. The official SEI support for the software development part of CMM (SW-CMM) ended in 2005 and the support for the software acquisition part of CMM (SA-CMM) ended on December 31, 2008. [Kne06] [Uni08]

Starting with 2009 CMMI is the only supported SEI standard.

3.5 CMMI

CMM and CMMI have some important differences in scope and in the organization of the models. Important for this work are maturity and capability levels of processes and that part has not significantly changed between CMM and CMMI. Due to this, subsequent descriptions of structures and maturity levels relate to CMMI version 1.2 as this is the newest version.

3.5.1 Structure

The CMMI model is organized in process areas. CMMI-DEV has 22 process areas. Some process areas, like Configuration Management (CB) or Risk Management (RSKM), are similar to processes defined in ITIL, COBIT or ISO 20000. Others are more specifically designed for the development of products, like the process areas Requirements Development (RD) or Requirements Management (REQM).

In CMMI a process area is defined as *"a cluster of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making improvement in that area."* [Uni06b]

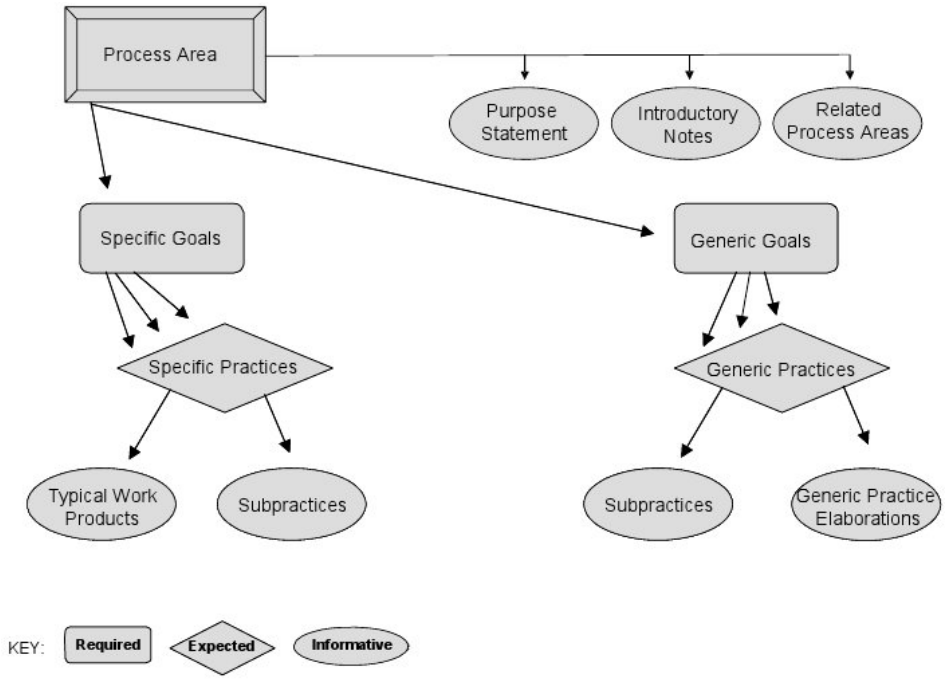

Figure 3.11: Structure of the CMMI model. [Uni06b]

Figure 3.11 shows the components contained in each process area. Components are of one of three types:

- **Required components** are used to describe what an organization without exception has to achieve in order to satisfy the requirements for the process area. Required components are specific and generic goals. Generic goals apply to multiple processe areas and specific goals apply to just one process area. Both generic and specific goals are used in order to assess if an organization has fulfilled the requirement for a process area. [Uni06b]

- In order to achieve the generic and specific goals, an organization has to implement a set of practices. A practice is a set of activities that leads towards the fulfillment of the associated goal. For each generic and specific goal, CMMI describes a set of recommended practices. These practices are **expected components** and describe recommended ways of achieving goals. This means that the specific and generic practices are one, but not the only way to fulfill the specific and generic goals. If an organization chooses to use other means to achieve the defined goals, they could still use CMMI to assess and improve their processes. [Uni06b]

- **Informative components** provide information that is not taken into

account in an assessment of the process area. Informative components are only used for helping organizations to start a thinking process and assist in implementing the specific and generic practices and goals. [Uni06b]

3.5.2 Continuous vs. Staged Representation

The goals of CMMI are to provide tools for assessing and improving organizational processes. For this "Levels" are an important concept.

Levels are used to describe a path of improvements recommended to organizations in order to achieve optimal implementation of their processes. For reaching a specific level organizations must satisfy all appropriate goals, as displayed in figure 3.11, for a process area or a set of process areas. Levels are building on each other and it is not possible or recommended for an organization to skip a level. [Uni06b]

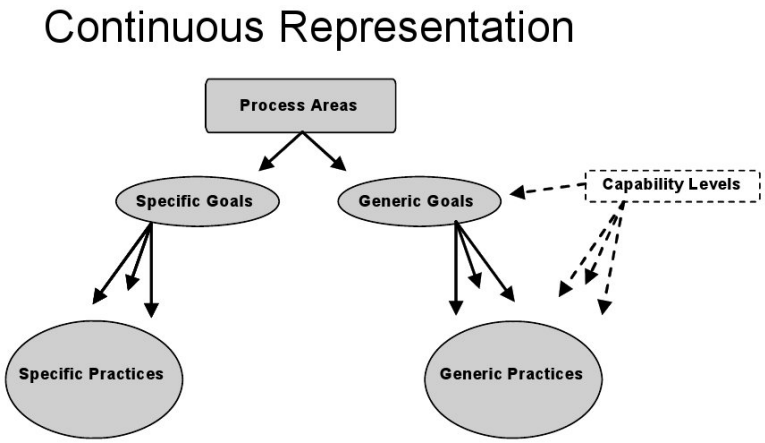

Figure 3.12: CMMI Continuous Representation. [Uni06b]

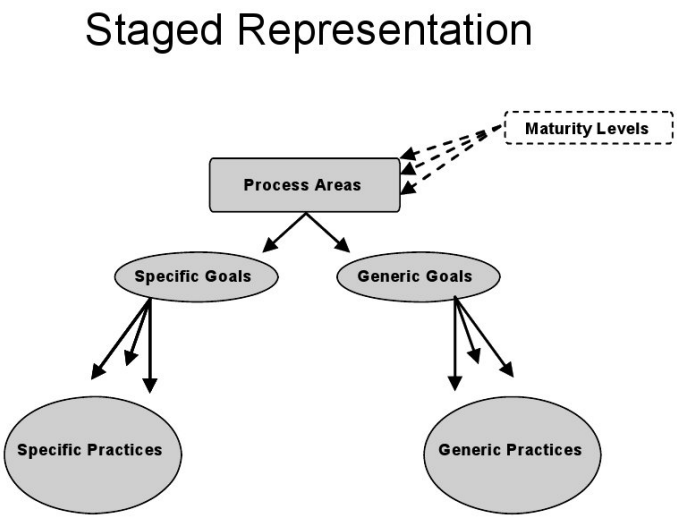

Figure 3.13: CMMI Staged Representation. [Uni06b]

CMMI defines two paths for improvements:

- The **continuous representation**, as displayed in figure 3.12, focuses on process areas and is used by organizations that want to improve or assess their processes incrementally. The improvements in different processes can be done separately of each other. The continuous representation is being measured by **capability levels**. Capability Levels describe how well an individual process is implemented. CMMI defines six capability levels ranging from 0 to 5. [Uni06b]
- The **staged representation**, as displayed in figure 3.13, focuses on a set of related process areas and is used in order to improve or assess an organization's ability to perform. The staged representation is measured by five **maturity levels** ranging from 1 to 5. [Uni06b]

3.5.3 Capability and Maturity Levels

Table 3.2 shows the different CMMI levels for the continuous (capability levels) and staged (maturity levels) representations. Levels two to five have the same name for both capability and maturity levels. This is intentionally due to the fact that they represent overlapping concepts in these levels. [Uni06b]

Another difference between the capability and maturity levels is that there are only five maturity levels whereas six capability levels, ranging from 0 to 5, are defined.

In the following text capability level 0 and 1, and maturity level 1 are described separately. Level 2 to 5 share the same descriptions for both

Level	Capability Level	Maturity Level
0	Incomplete	N/A
1	Performed	Initial
2	Managed	Managed
3	Defined	Defined
4	Quantitatively Managed	Quantitatively Managed
5	Optimizing	Optimizing

Table 3.2: Comparison of CMMI levels. [Uni06b]

capability and maturity levels due to their overlapping concepts and general similarities.

Capability Level 0 - Incomplete

Level 0 exists only in continuous representation and defines incomplete processes. An incomplete process is a process that is either not performed or not well enough performed for level 1.

One or several specific goals for the process are not fulfilled. No generic goals for the process exist. [Uni06b]

Capability Level 1 - Performed

At level 1 processes are operated on a level which to some extent enables and supports the production of output. All specific goals for the process area are achieved. The process area is not formalized and generic goals are not met. [Uni06b]

Maturity Level 1 - Initial

Processes on this level are rather unstructured and ad hoc. Quality and time of delivery depend very much on the competences and commitment of individuals and less on the quality in the processes.

Even though, organizations operating on level 1 might produce products and services that have the proper quality. However, budgets are often exceeded and products are often delivered later than expected. Other typical problems are the inability to reproduce a successful product or service and that shortcuts that break the process are taken in time of crisis. [Uni06b]

Level 2 - Managed

Generally, managed processes produce products and services according to planned time, budget and quality. Processes are supported by basic infrastructure.

People with required knowledge are employed in the processes and supported by adequate resources. Relevant stakeholders are involved and committed to the project or process.

All level 2 processes are monitored and reviewed. Analyses are done in order to identify areas where the process execution differs from the process plan.

In time of stress shortcuts that destroy the execution of the processes are not performed. [Uni06b]

Level 3 - Defined

Defined processes are more mature, formal and understood than managed processes. Moreover, they are documented in a more rigid and structured way than level 2 processes.

Defined processes are documented with purpose, input, entry criteria, roles, activities, measures, verification methods, output and exit criteria.

In level 3 the relationship between process activities and measures of the process is clearly understood. This understanding is subsequently used for a proactive improvement of the process.

A distinction between level 2 and level 3 processes is that level 2 processes might be quite different from project to project, whereas level 3 processes tend to be similar between projects. This is due to an organizational pool of process descriptions serving as a template for processes in projects or departments. Such process templates document not only the process itself, but also how it is allowed to adapt in order to serve specific needs. [Uni06b]

Level 4 - Quantitatively Managed

In level 4 quantitative and statistical techniques are used for controlling and managing the processes. Statistical terms are used in order to describe, understand and analyze process quality and performance.

The needs of customers, end users and relevant stakeholders to the processes are investigated and matching quantitative objectives are created.

A set of selected sub processes is measured in detail and data about process quality and performance are collected and analyzed. A central measurement repository is used for storing the data. This repository also enables the organization's management to make informed decisions based on analysis of up-to-date information.

If a process is not executed as planned due to transient circumstances, the underlying cause is to be identified in order to avoid further occurrences.

A distinct difference between level 3 and level 4 processes is the predictability of process performance. Typical level 4 processes use statistical methods to analyze process data, and are able to predict process performance quantitatively. Whereas level 3 processes are only able to predict

performance in qualitative terms.

In order to be assessed as a level 4 process, the process needs to fulfill the criteria of level 3. Hence level 4 processes are normally able to predict both quantitative and qualitative performance. [Uni06b]

Level 5 - Optimizing

The core of level 5 is a continual and incremental improvement and an optimization of the implemented processes and the organization's set of defined standard processes.

The improvements are based on quantitative analysis of process variations due to expected interaction between components in the process. The goal of the improvements is of course to have as few variations from the organizations standard processes as possible, and at the same time optimally support the realization of the business objectives.

Improvements to a process do not necessarily mean that the process has to be reorganized or undergo a significant change. A process could as well be improved by technological means, like better support from an Enterprise Resource Planning (ERP) system. However, a technological change might also cause the process workflow to change.

Organizations working on level 5 have defined quantitative process improvement objectives and have implemented a system for them to be continual revised to reflect changing business objectives. These objectives are used as criteria in the process improvement work, in addition to evaluate the effect of implemented process changes. [Uni06b]

3.5.4 Advancing through Levels

The CMMI standard suggests that the best way to advance through the capability levels in the continuous representation (the capability of single processes as displayed in figure 3.12 on page 50) is to use the generic processes in order to achieve the generic goals. [Uni06b]

This implicit means that all the specific goals have to be fulfilled as well, due to the nature of the first generic goal. CMMI defines five generic goals, named GG1 to GG5. The first goal specifies that the specific goals for the process have to be achieved.

In case of the maturity levels in the staged representation (the maturity of multiple process areas as displayed in figure 3.13 on page 51) the CMMI documentation recommends to an organization to first start the process improvement on a project or department level. Later a system for organization wide continuous process improvement, using both quantitative and qualitative collected and analyzed data, might be implemented. [Uni06b]

3.5.5 SCAMPI

In order to demonstrate to customers, shareholders and other stakeholders the quality of the implemented processes, SEI has developed a program for the validation of an organization's compliance with CMMI.

The program called Standard CMMI Appraisal Method for Process Improvement (SCAMPI) is a set of defined procedures for an official CMMI compliance assessment of an organization. In SCAMPI three classes (A, B and C) of requirements are defined. Class A represents the most comprehensive and demanding set of requirements.

Class A appraisals are always performed by a so called lead appraiser. A lead appraiser is a person that is certified by SEI to perform SCAMPI-A appraisals of organizations.

The results of a SCAMPI-A appraisal is reported to SEI and is optionally published on the SEI website[6]. [FSR08]

The SCAMPI-B and C appraisals are less extensive, and requires less time and resources than a full SCAMPI-A appraisal. For example can a SCAMPI-C appraisal be conducted by one person, while SCAMPI-B requires a team of at least two persons and SCAMPI-A four persons.[CMU06]

[6]Published CMMI Appraisal Results: `http://sas.sei.cmu.edu/pars/`

Chapter 4

Implementing an ISMS

Several methods, tools, frameworks and standards have been developed to support the implementation of Information Security Management Systems (ISMS) in organizations. In this work the focus is however put on ISO 27001, an internationally accepted standard for IT security.

ISO 27001 has a normative character, meaning that it specifies the requirements for obtaining a certification, but not how to fullfill those requirements.

Other standards like e.g. the IT-Grundschutz framework from Bundesamt für Sicherheit in der Informationstechnik[1] are more focused on how to fullfill the requirements and can be used as a kind of organizational template for achieving the ISO 27001 certification.

4.1 Defining ISMS

A management system created for building and maintaining a secure environment for information can be defined as an Information Security Management System (ISMS). [SVFMP06] An ISMS is an integrated part of the overall management system and is influenced by the systems for corporate and IT governance applied to organizations.

If ISMS was to be displayed in the model of corporate governance by Rüter, Schröder and Göldner (figure 2.2 on page 9), it would find its place as an integrated part of IT governance. However it would still be under strong influence by the elements of corporate governance, in addition to many external factors like laws and industry regulations.

[1] Federal Office for Information Security, Germany.

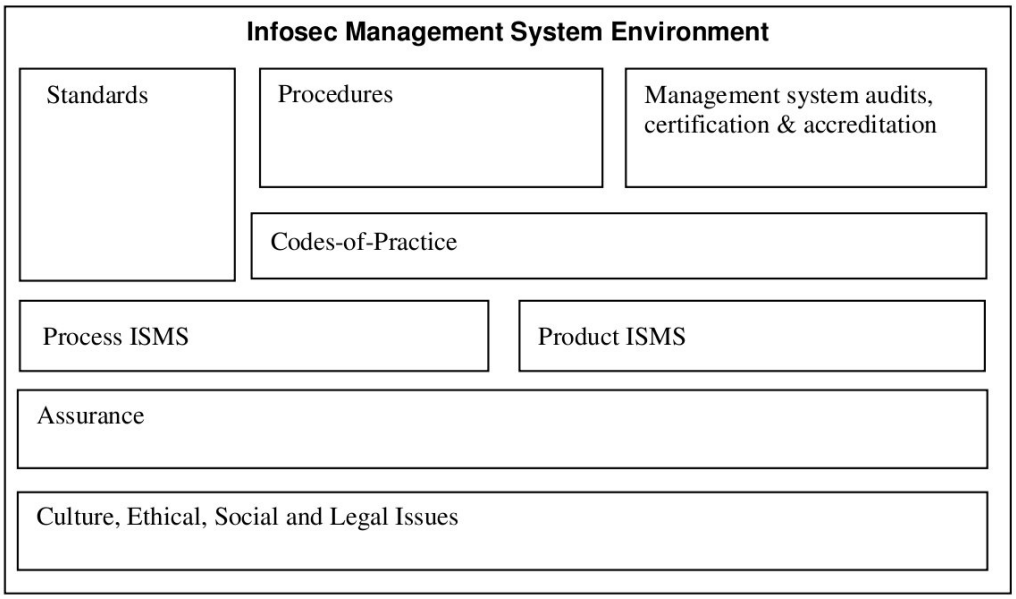

Figure 4.1: The elements of an ISMS. [EE03]

An ISMS must identify the security needs of an organization, design and implement strategies to meet those needs, measure the effects, and work with the continual improvement of the information security. [EE03]

Figure 4.1 shows the elements of a typical ISMS. An ISMS can be quite complex due to influence and connections to virtually all parts of an organization. Hence, it can be helpful to look at an ISMS from at least three different perspectives that have to be combined for a satisfying information security implementation:

- The strategic perspective.
- The human perspective.
- The technical perspective.

Viewed from a strategic perspective, an ISMS consists of governance techniques, policies, procedures and pure management issues. Central to this perspective is the information security policy, which describes the management's intentions with the ISMS and defines the high level controls the organization is going to use for protecting information. The security policy will also be an important part of the security audits. [EE03]

An ISMS does also have a human side where elements like organizational culture, awareness, knowledge, moral and ethics are in focus. In order to attack the human side of an ISMS, an attacker would apply social engineering techniques.

For someone to get access to information the three step process of Identification, Authentication and Authorization (IAA) is ideally involved. The meaning of these steps can be explained with the following questions: "Do I know you?" (Identification), "Are you who you say you are?" (Authentication), "Are you supposed to be here?" (Authorization). [Tho04]

By applying social engineering techniques an attacker would try to bypass the IAA process with deception in order to get access to protected information. Typical social engineering techniques include:

- *"Posing as someone with authority."* [Tho04]
- *"Posing as a new employee requesting help."* [Tho04]
- *"Offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call the attacker for help."* [Tho04]
- *"Using insider lingo terminology to gain trust."* [Tho04]

A well implemented ISMS should recognize the risks involving the human components and initiate appropriate actions if necessary. Research suggests awareness training, posters, bulletins, newsletters, websites, and special "awareness days" as possible measures for keeping a high employee awareness of the dangers of social engineering.

The third perspective is the technical one and is visualized by the "Product ISMS" element in figure 4.1. This perspective includes everything needed for implementing information security on a technical level like hardware, software and physical access restrictions. [EE03]

An ISMS is not solely to be regarded as a property of the internal IT organization. Information security should be regarded not only as a technical issue, but also as an issue concerning other departments like the audit or legal department of an organization. The result of this is that the budget for building and operating an ISMS may not only come from the IT budget, but from other parts of the company as well.

A study from 2008 shows that 53% of participated organizations spent less than 5% on information security expressed in terms of percentage of the general IT budget. [Ins08]

4.2 The need for an ISMS

Ernst & Young, an international auditing firm, conduct annual studies of information security in a global context. In their report from 2007 the top drivers that influence information security are identified. The findings presented in figure 4.2 shows how the participants of the study rank the top three drivers. [You07]

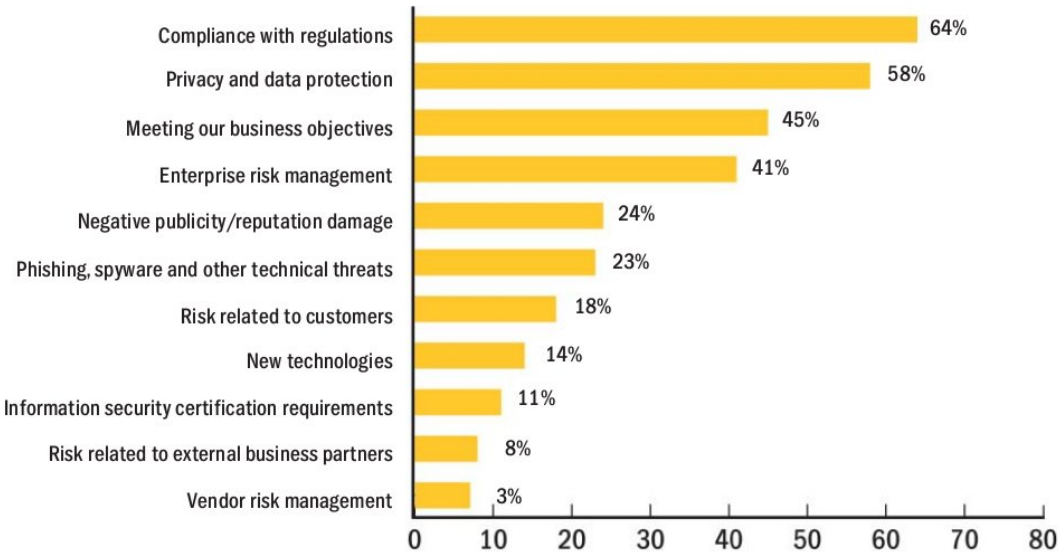

Figure 4.2: Drivers that influence information security. [You07]

The findings clearly communicate that technology is not a major driver for ISMS. The category "New technologies" is only rated with 14% and the category "phishing, spyware, and other technical threats" is rated with 23%.

The dominant factor influencing information security according to the Ernst & Young study is the requirement to comply with regulations.

Looking at the required regulations for an international corporation in e.g. the financial sector, several regulations relevant for information security emerge. Basel II, Sarbanes-Oxley Act and different EU directives in addition to specific national requirements represent a major driver for an international company to build and operate an effective ISMS. [Ger08]

Even though the compliance with regulations can be a challenging, cumbersome and time consuming task, the effect of meeting the requirements had a positive effect on the information security for 80% of the participants' organizations in the survey.

4.3 ISO 27001

The main motivation for implementing an ISMS is the need for compliance with governmental regulations. The problem with regulations is that they specify *what* is to be required, but not *how* the requirements are to be fulfilled.

Another problem for an international operating company is the number of regulations that have an effect on information security. To obtain detailed knowledge about what is required of an ISMS is not a trial task.

To solve these problems technical regimes and best practice frameworks like e.g. COBIT, ITIL and ISO 27001 can be applied. However, none of them are legal norms.

ISO 27001 has a normative character, meaning that it can be used as a basis for a certification. [105c] Such a certification is not legally binding, but is due to being a commercial as well as governmental industry standard for information security an international accepted evidence of a well implemented ISMS. [Eck08]

The standard defines an ISMS through a set of concrete requirements called control objectives. If an organization fulfills the requirements defined by the controls and obtains the certification through an external audit, the evidence of an effective information management is documented. [Wec07]

An ISO 27001 certification can be issued to a whole company or parts of a company like e.g. a department or a business process. The direct costs of a certification will be at least 10.000 €. The cost depends on the size of the company and the complexity involved and does not include the implementation of the ISMS system itself or the resulting organizational changes. [KRS08]

4.3.1 Scope

In ISO 27001 the goal of the standard is defined as:

> *"... provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).“* [105c]

The establishment of an ISMS is a strategic decision with a long term effect for the organization and requires the support of top level management.

The use of ISO 27001 is not defined as a standard for only large organizations. It is explicitly documented that an ISMS implementation is expected to be scalable, and that smaller organizations with less complex needs require simple ISMS solutions. [105c]

Further the standard is designed to cover all kinds of organizations regardless of industry or type. It can be used by commercial, governmental or non-profit organizations as well as internal IT organizations and specialized IT companies.

ISO 27001 is compatible with other management systems, in specific ISO 9001:2000[2] and ISO 14001:2004[3]. [105c]

[2]ISO 9001:2000 - Quality management systems
[3]ISO 14001:2004 - Environmental management systems

4.3.2 Development of ISO 27001

The ISO 27000 series of standards have their roots in the UK agency Commercial Computer Security Center (CCSC), a part of the UK Department of Trade and Industry. [Sys07]

CCSC was assigned two major tasks. The first was to define a set of information security evaluation criteria in addition to tools and methods for certification. The second task was to develop a set of good information security practices. [Ger06]

Later the National Computing Center, an UK research and membership organization, joined the development and together with CCSC they developed what was to be British Standard (BS) 7799.

BS 7799 part 1 was first released in 1995 with the title "code of practice for information security management." BS 7799-1 is a collection of implementation tips, activities and good practices for information security.

The second part, BS 7799-2 got the name "specification with guidance and use". It describes a model for an ISMS. BS 7799-2 was released in 1998 and revised in 2002. [KRS08] [Fle07]

In 2000 BS 7799-1 was used as a basis for the ISO standard 17799 with the name "Code of practice for information security management". The latest revised version of ISO 17799 is from 2005.

ISO was also planning to create a new standard based on BS 7799-2, but through a long international voting process it was decided to re-design the whole area of information security. As a result it was decided to develop a series of new information security standards in the 2700x series.

In 2005, based on BS 7799-2, the ISO 27001 standard was released. It defines the requirements for an ISMS and has a normative character.

Standard	Status	Content
ISO 27000	in development	Definitions relevant for information security and ISMS.
ISO 27001	published	Specifies requirements for an ISMS. Normative. Used for certifications.
ISO 27002	published	Code of practice for management of information security. Based on BS 7799-1.
ISO 27003	in development	Introduction and implementation guide for how to establish and maintain an ISMS.
ISO 27004	in development	Descriptions of measurement techniques and metrics for information security.
ISO 27005	published	Guidelines for risk management in an information security context.
ISO 27006	published	Specifies requirements for organizations that are auditing ISMS based on ISO 27001.

Table 4.1: ISO 2700x standards published or in development. [KRS08]

As table 4.1 shows, ISO is releasing a number of standards for information security in the ISO 27000 series. For this work, the focus will be on ISO 27001, as this is the only standard specifying an ISMS.

4.3.3 PDCA

As a method for continuous improvement of the implemented information security processes, ISO 27001 builds upon the Plan-Do-Check-Act (PDCA) model. This is basically the same model as the model used for continuous improvement in ISO 20000 and is described in more detail on page 40.

In general the PDCA model in context of ISO 27001 defines the phases of designing (Plan), operating (Do), monitoring (Check) and improving (Act) an ISMS. [KRS08]

4.3.4 Structure of requirements

The ISO 27001 documentation is divided into informative and normative parts. In the following text only the normative parts are described.

Figure 4.3 displays the normative sections of ISO 27001. If an organizations claims to be ISO 27001 compliant it needs to satisfy, without exceptions, all requirements specified in part 4,5,6,7 and 8 of the standard.

Control objectives specified in annex A are required as well. It is possible to omit some of the controls provided they do not affect the organizations ability to provide information security. Information security is always provided in the context of requirements identified by risk assessment and regulatory requirements where it might apply.

Figure 4.3: Normative requirements in ISO 27001. [105c]

In part 4 the Plan-Do-Check-Act (PDCA) cycle of continuous improvement is used in order to structure requirements into groups. This can be viewed as the core of the standard and all other parts are connecting to the PDCA cycle in part 4.

Due to this, this work will focus on part 4. The content of part 5, 6, 7 and 8 will be semantically covered by the descriptions of the 4th part.

4.3.5 Part 4 - ISMS

Part 4 of the standard defines requirements for establishing, operating, monitoring and improving an ISMS. The standard uses the PDCA model as a reference model for this process. [105c]

The following parts describe the major elements of part 4 of the standard. The numbers refer to the corresponding part of the ISO 27001 standard.

4.3.6 Part 4.2.1 - Establish the ISMS (Plan)

This part matches the "plan phase" of the PDCA cycle. The purpose of the plan phase depends on the situation.

The first time an ISMS is implemented the plan phase is used for designing a not yet existing information security system. In all other situations the plan phase is used for designing changes to an existing ISMS. The changes can be necessary due to a number of reasons like e.g. changing regulatory requirements. [KRS08]

Scope

In the plan phase the scope of the ISMS should be defined. The scope includes aspects like description and characteristics of the business, technology in use and possible elements of the organization that is not to be included in the ISMS. Basically most of the requirements for this step are already fulfilled when the organization has made the decisions that it is going to start an ISO 27001 compliance project. [KRS08]

ISMS policy

Further an ISMS policy and information security policy should be defined. The information security policy describes the business requirements and legal regulations in addition to the liability of all employees.

The ISMS policy describes conditions for achieving information security. Moreover the ISMS policy is aligned with the organization's risk management. [KRS08] According to the standard the policies can be defined in one document. [105c]

Risks

Moreover the standard requires an organization to define how risks are to be managed. The first step is to plan how risks are to be assessed. The standard does not prescribe a method for risk assessment, but gives a reference to another ISO standard that might be of help[4].

Systems and procedures for identifying, analyzing and evaluating risks should be in place. In detail this means that identified risks have to be associated with the assets they affect and the owner[5] of those assets. Moreover the threat, vulnerabilities and possible impact of risks have to be identified.

The result of the risk assessment should be a number of risks classified as either acceptable or requiring treatment based on predefined rules. The residual risk that are not treated by either avoidance or transference of risk to e.g. an insurance company need to be approved by the management. [105c]

Controls and Control Objectives

Further the part 4 of the standard requires an organization to select control objectives for treatment of risks. Annex A of the standard defines a number of controls suitable for risk management. This should only be seen as a starting point and an organization would probably have to develop own custom controls in addition.

Management approval

As the last step of the planning phase ISO 27001 requires an organization to obtain management approval of the implementation and operations plan of the ISMS. [KRS08]

[4]ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security

[5]In ISO 27001 the owner of an asset is defined as the person or role that is responsible for the operation or maintenance of the assets - not the person with the property rights of the asset.

4.3.7 Part 4.2.2 - Implement and operate the ISMS (Do)

This part of the standard constitutes the "do phase" of the PDCA cycle. In this phase the plan designed in the previous step is implemented into the organization. If an ISMS is already in place, this phase is used for implementing changes instead.

Risk treatment Plan

An important part of this phase are the requirements defining that a risk treatment plan has to be formulated and implemented. The risk treatment plan assists in the management of risks. This includes activities like monitoring of operational activities, assigning resources and roles, set priorities and risk analysis and treatments of risks.

At a first glance this seems to fit well into the "plan" phase of the PDCA cycle. In ISO 27001 these tasks are placed in the "do" phase. The reason for this is probably that the activities required for defining and implementing a risk treatment plan have more the characteristics of performing than planning. [KRS08]

Control Objectives

In the planning phase a number of control objectives and associated controls were selected from annex A to be a part of the ISMS, in addition to possible custom defined control objectives. In the "do" phase the selected control objectives should be implemented into the ISMS.

This means that the necessary part of the organization's operation has to be monitored in order to collect relevant data used for measurement of the control objectives. [105c]

Effectiveness of Controls

Next, the "do" phase requires an organization to define how to measure the effectiveness of control objectives and implemented controls. The actual measurement of the effectiveness is however done in the next step - in the "control" phase.

The goal of the measurement of the effectiveness of controls for managers and staff is to get a picture of how well controls achieve the defined control objectives. [105c]

The method of measurement should apply the following three principles: [KRS08]

- consistent for all controls
- deliver comparable results of controls

- deliver the same results for equal controls under the same conditions and assumptions.

The three principles make a quantitative approach unsuitable or hard to implement. Instead it is recommended to create a measurement method based on classification. Several thematically similar controls could be grouped into groups of controls which fit a defined control objective. [KRS08]

Training and Awareness

Training programs can be quite expensive, not only because of the cost of the training itself, but also because of the non-productive time of the employees. Even though, an effective ISMS requires that the employees know the organizations information security policies and how to enforce them.

Employees should attend training and awareness programs on regular basis e.g. annually. The training should not only cover the daily routines, but also what to do in unexpected situations. The training program should be planned and documented.

Important tasks of the management include communicating why an ISMS is implemented in the organization and what the advantages for the organization are. [KRS08]

Operating the ISMS

The management should implement tasks and activities as required by the ISMS. This includes that relevant measures have to be build into the daily work routines of the employees, and make sure that they are followed. [KRS08]

Manage Resources

The management is required to plan and document how resources are to be used in the ISMS. The plan should cover the whole process of planning, implementing, operating, monitoring and refining the ISMS.

This is a recurring task. A resource plan should be created at the beginning of the project, and then be e.g. annually review and updated. The resource plan should estimate the cost of operating the ISMS on all levels of the organization.

In the context of an ISMS a resource plan includes not only the hardware and software needed, but also people like employees and if necessary external consultants.

A resource plan fulfills several purposes. First of all, it enables the ISMS project team to document the need for resources and hence develop a project plan for the implementation process. Secondly it enables the project team

to obtain a management commitment for the ISMS based on something concrete. And last it enables the creation of cost benefit analysis, which again can be used for estimating the success of the ISMS in monetary terms. [KRS08]

Detection of Security Incidents

Simply defined a security incident is not more than an event that violates the security objectives of an organization.

It is not possible to avoid all kind of security incidents. The objective of an ISMS is to manage the organization in such a way that security incidents are responded to in a best way possible.

To do this an organization should define in an incident management plan how an incident should be classified, and how incidents in given classification categories are to be managed.

In addition to the procedures defined for the normal classified incidents, a special classification for emergency incidents should be in place. These contingency procedures should define things like escalation plans, who to inform, how to solve the problem in the best way possible etc. [KRS08]

4.3.8 Part 4.2.3 - Monitor and review the ISMS (Check)

Monitoring is an important tool for managing the information security system. Monitoring enables the management to get a correct picture of how well implemented the ISMS is, and is a fundamental part of identifying possibilities for improvements.

This part of the standard describes what corresponds to “Check” in the PDCA cycle. [105c]

Monitor

ISO 27001 defines four distinct characteristics of the monitoring process in the “check” phase: [105c] [KRS08]

1. The monitoring process should detect errors in the processing of data,
2. detect and identify successfully and attempted security breaches,
3. provide management the possibility to check if security related activities are performed as expected
4. and provide metrics for early warning and detections of information security related problems.

In the management review process of the ISMS the effectiveness of the implemented monitoring process should be evaluated. An important detail

to the review process is that it should probably not be the same person operating and reviewing the ISMS. [KRS08]

ISMS Review

On regular intervals the effectiveness of the ISMS should be reviewed. An ISMS review should take several elements, like results of security audits, information security incidents, measured effectiveness and feedback from users, management, suppliers, customers and other stakeholders, into account.

Regarding security incidents, the scope of the review process is not only to investigate incidents coming from the internal organization, but also to consider known security incidents from suppliers and service providers that had or could have had an impact on the organization's information security. [105c]

Review the effectiveness of Controls

ISO 27001 requires an organization to review the effectiveness of selected controls in regular intervals. How often such a review should be performed depends on the cost of the review and the potential damage of not detecting potential problematic controls.

The result of this review should be a list of controls or control objectives that are not optimally working and possible a description of why. This list is then handed over to the responsible persons for the corresponding controls, and a redesign process should be started. [KRS08]

Review the Risk Assessment

In the "plan" phase a risk assessment is performed (page 64) in order to classify risks, determine risk treatments and get a management approval for residual risks.

In the "check" phase the risk assessment is reviewed. This could be done e.g. annually or every second year. Review process should consider elements like the organization, the business objectives, the technology and identified threats. [105c]

Internal Audits

An internal audit, also called a first party audit, is a review of the whole or parts of the ISMS. An internal audit can be performed by either the organization itself or by an external consulting firm. [105c]

An internal audit can have several purposes. An organization might want to know the current situation in order to get an objective view on the

quality of the ISMS, or an internal audit could be a preparation and final test before an ISO 27001 certification process is started. [KRS08]

Update Security Plan

The ISO 27001 documentation requires the "check" phase to include an update of the security plan. The security plan is not defined in the standard and it is unclear what a security plan according to ISO 27001 is. [105c]

Kersten, Reuter, and Schröder [KRS08] suggest that a security plan is a part of, or is equivalent to the incident management plan as described in the do phase of the standard. (Page 67)

The update of the security plan should include findings from the other monitoring and reviewing activities defined. [105c]

Record Events

The standard requires events and actions that could have an influence on the operation of the ISMS to be recorded. Examples of relevant events that should be recorded are: [KRS08]

- Planning of resources.
- Training and courses.
- Internal and external audits.
- Security incidents.
- Changes of employment contracts, in special termination.

4.3.9 Part 4.2.4 - Maintain and improve the ISMS (Act)

The four PDCA cycles serve the goals of maintaining and improving the ISMS. An organization already in the "act" part of the cycle has gone through the phases of planning, implementing and reviewing the information security system. Hence, in the "act" phase an organization is ready for improving the ISMS in the organization, based on experience collected in the previous phases.

The ISO 27001 standard requires an organization to perform four activities on regular intervals: [105c]

1. Implement changes - In the "check" phase a set of information was collected that is relevant for improvements to the ISMS. This information needs to be discussed by the management and the responsible persons for the ISMS in order to identify and determine actions for improvements. [KRS08]

Decisions about changes need to be made based on cost-benefit analysis, and hence the quality of the data collected in the "check" phase is of great importance. However, the expected benefit of an implemented change is just an estimation and a decision is never going to be completely risk free.

2. Corrective and preventive actions - This task is mostly about learning from security incidents from own or other organizations in the industry.

   The goal of this task is to improve the organizations conformity with the ISMS, and make sure that the ISMS covers all likely security incidents. [KRS08]

3. Communicate improvements in the organization - Relevant stakeholders should always be informed when important changes to the ISMS have been implemented.

   The type, form and level of detailedness of information communicated should be adapted to the type of stakeholders addressed. E.g. an employee that is affected by a change in his or her daily work would probably need more detailed information and instructions than a more remote stakeholder.

4. Control of Success - Control of the ISMS is a permanent task of the management. Depending on the nature of the change implemented in the "act" phase, the control of the change could wait until next internal audit or management review.

   If changes involve e.g. large costs or extensive use of personnel, or in case of complex changes, it might not be feasible to wait for the next scheduled review.

   Due to this, the management should make a decision on how the success of change is to be checked at the same time as the decision on implementing the change is done.

4.3.10 Part 4.3 - Documentation requirements

In addition to the requirements for the PDCA cycle, part 4 of the ISO 27001 standard contains some general requirements for how to manage documentation. The documentation requirements required in ISO 27001 are almost identical to the documentation requirements described in ISO 9000[6] and ISO 14000[7].

Documentation can be managed and maintained in any form that is convenient to the organization. It does not have to be on paper, but could be e.g. web based in form of an intranet system. [KRS08]

[6] ISO 9000 - Quality management systems.
[7] ISO 14000 - Environmental management.

What

All management decisions regarding the ISMS should be documented. This could be e.g. in form of minutes of meetings. The decisions need to be documented with so many details that resulting actions are traceable back to the corresponding management decision.

Moreover the standard requires the following information to be included in the ISMS documentation: [105c]

- The ISMS policy as described in the "act" phase.
- Description of what the ISMS is to manage.
- Procedures and controls used for operating the ISMS.
- Description of the methodology used for assessing risks.
- A risk assessment report and a risk treatment plan.

The size of the documentation might vary between organizations depending on size, scope of the ISMS and complexity of the security requirements. [105c]

How

The standard requires all documents to be protected from unauthorized access and be the subject of a procedure managing the management actions needed for changes.

The latter includes that new documents should be approved before implemented into the official documentation. Updated documents require a re-approval.

Further documents needs to be identifiable and contain a revision status. Documents from external sources should be identified as such. [105c]

4.3.11 Annex A - Control Objectives

ISO 27001 provides a set of control objectives and controls in annex A of the documentation. Annex A has a normative character, meaning that the requirements within will be controlled in a certification process.

The control objectives and controls defined in ISO 27001 are derived from and aligned with the requirements defined in ISO 17799:2005.

A control objective in the context of ISO 27001 is an overall goal of the ISMS. The control objectives defined in the standard are quite general in order to fit almost all kind of organizations. In practice an organization would probably want to design and implement additional control objectives as well. However, this is not required by the standard.

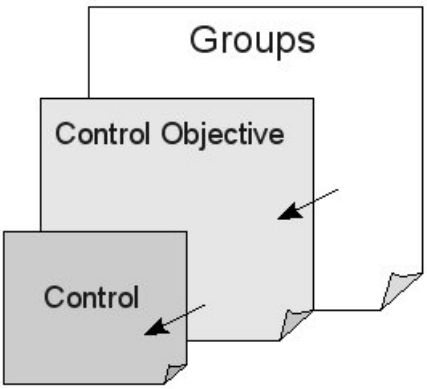

Figure 4.4: The organization of controls in ISO 27001.

Following is an example of a control objective for backup[8]:

> *"To maintain the integrity and availability of information and information processing facilities."* [105c]

Each control objective is accompanied by one or several controls. A control is a specific requirement of how the control objective is to be achieved.

The control objective "backup" has only one associated control with the name "information back-up," which states that

> *"back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy."* [105c]

Figure 4.4 shows how controls are used to fulfill control objectives, and how control objectives are gathered into groups.

ISO 27001 defines 11 groups with the IDs A.5 to A.15. Each group contains a set of control objectives as showen in table 4.2.

[8]Control objective "backup" has the ID A.10.5 in the ISO 27001 standard.

Group	Control Objectives
A.5 Security policy	A.5.1 Information security policy
A.6 Organization of information security	A.6.1 Internal organization A.6.2 External parties
A.7 Asset management	A.7.1 Responsibility for assets A.7.2 Information classification
A.8 Human resources security	A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination of change of employment
A.9 Physical and environmental security	A.9.1 Secure areas A.9.2 Equipment security
A.10 Communication and operations management	A.10.1 Operational procedures and responsibilities A.10.2 Third party service delivery management A.10.3 System planning and acceptance A.10.4 Protection against malicious and mobile code A.10.5 Back-up A.10.6 Network security management A.10.7 Media handling A.10.8 Exchange of information A.10.9 Electronic commerce services A.10.10 Monitoring
A.11 Access control	A.11.1 Business requirements for access control A.11.2 User access management A.11.3 User responsibilities A.11.4 Network access control A.11.5 Operating system access control A.11.6 Application and information access control A.11.7 Mobile computing and teleworking
A.12 Information system acquisition, development and maintenance	A.12.1 Security requirements of information systems A.12.2 Correct processing in applications A.12.3 Cryptographic controls A.12.4 Security of system files A.12.5 Security in development and support processes A.12.6 Technical vulnerability management
A.13 Information security incident management	A.13.1 Reporting information security events and weaknesses A.13.2 Management of information security incidents and improvements
A.14 Business continuity management	A.14.1 information security aspects of business continuity management
A.15 Compliance	A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards, and technical compliance A.15.3 Information system audit considerations

Table 4.2: Control objectives and group of control objectives as defined in ISO 27001. [105c]

Chapter 5

Didactics and Theories of Learning

In this chapter some of the concepts and theories of didactics relevant to this work are presented. Definitions of didactics are outlined and theories for learning and teaching are described.

The behavioristic, cognitivistic and constructivistic view on learning and teaching are presented in more detail as those views are regarded as specially important for the model developed in chapter 6.

5.1 Defining Didactics

The word didactic has its roots in the Greek verb didaskein which can have three different meanings:

- The *active* meaning is to teach or instruct other persons.
- The *passive* meaning is to learn or to be taught new knowledge.
- The *medial* meaning is to acquire new knowledge through self learning or to learn something from oneself.

The derived noun of the Greek verb "didaskein" is *didaktikos* and can be translated with lore, teaching or instruction. [FSUJ]

The founder of didactics as a systematical and methodical scientific area is J.A.Comenius. Many of the principles of didactics described in his book *"Didactica Magna"*[1] from the 17 century are relevant even today. [Brä06]

5.1.1 Definitions from the Literature

A number of different definitions of didactics exist.

Traditionally didactics is viewed as the scientific field of

[1] The Great Didactica

- management of learning processes,
- theories about curriculum
- and the appliance of psychological learning and teaching theories. [Mül06]

From this traditional view on didactics one can derive that *what* and *how* to optimally teach is an important part of didactics.

Other definitions of didactics support this traditional view. Arnold, Jürgen & Meili [WS06] state that didactics is concerned with *learning objectives*, *selection of content* and *teaching methods*.

Included in this definition of didactic are also the methods that are not directly applied in a learning or teaching situation but still contribute to the learning process. This includes e.g. advisory services, presentations and practical training. [WS06]

The different definitions of didactics can be summarized in the triangle of didactics displayed in figure 5.1 and the following definition from Jank and Mayer:

> *"Didactics is the theory and practice of learning and teaching."* [Mül06]

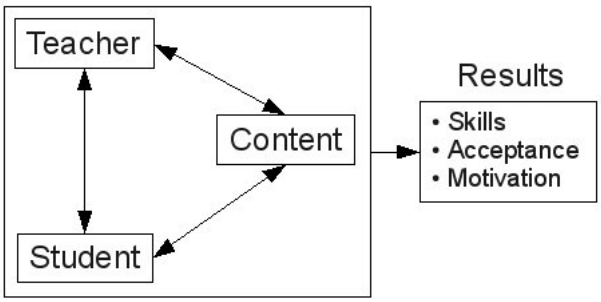

Figure 5.1: The triangle of didactics. [Var07]

The triangle of didactics contains the three elements teacher, student and content. In e.g. the context of a primary school the content is only partly determined by the teacher, due to a preassigned curriculum.

In the context of e.g. a university the teacher or professor might have more room for customization of the content.

The role of the student is to learn and understand the content presented by the teacher. The result of the process is knowledge transfer from teacher to student. The student acquires new skills and gains increased motivation.

When discussing different theories of didactics one has to take into account that all theories and models are just a simplification of the reality.

The real world is far more complex than what can be displayed in a simple drawing.

This is also the case with the triangle of didactics. Learning is a complex process which involves a number of psychological phenomena like motivation, emotions and cognition. Its outcome depends on the student's previous knowledge, learning style and other individual conditions. [Brä06]

Depending on what kind of theories of learning one supports the methods for teaching might be designed and performed in quite different ways. The most important theories for learning are presented later in this chapter.

5.1.2 General vs. Specialized Didactics

Didactics can be categorized into a general and a specialized part.

The general didactics is concerned with the science of teaching and learning. In specific the structure of teaching, compilation of subject areas and curricula is considered to be a part of the general didactics.

The specialized didactics is focused on specific subject areas or learning in a distinct context like e.g. primary school or university. [WS06]

While the general didactics tries to develop theories for all types of institutions and for all kind of subjects, the specialized didactics are only concerned with one subject area or one type of institution. [Mül06]

The core question in specialized didactics is:

> *When is what, how and with which objectives to be taught?* [Pre08]

The core processes of specialized didactics are: [Pre08]

- Definition of the objectives.
- Development of concepts for methodology and organization of the training.
- Definition of ideas, methods, and cognitions of the subject area that should be included in the teaching.
- Aligning the content of the subject area with the general curriculum and keep it up to date.

5.1.3 Didactics of Informatics

Didactical research in a specific subject area is also referred to as subject didactics. An example of this is the research in the area of teaching and learning informatics.

Other specialized areas of didactics are focused on the institution or method of teaching. Examples of this include didactical models for teaching

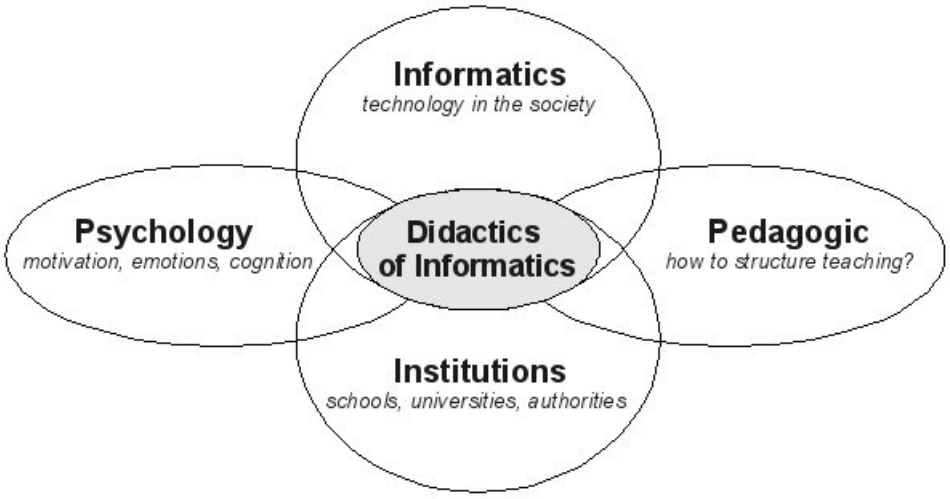

Figure 5.2: Didactics of informatics is influenced by other sciences. [Pre08]

an arbitrary subject, but with the use of - or the support of - information technology.

This research field of didactics in informatics has influenced how e-learning is applied in different contexts. In the beginning the research field focused on Computer Based Training (CBT) as an instrument for self learning. Later this focus has shifted more in the direction of using information technology to assist in normal learning processes - so called blended learning.

Figure 5.2 shows that didactics of informatics is not a static science. Several other scientific areas like e.g. psychology and institutions like schools or public authorities have a strong influence and create a dynamic environment. [Pre08]

5.2 Learning Theories

Several learning theories exist that have an impact on how information technology can be applied for optimal support of learning processes. However, most of them can be reduced to the three classical theories behaviorism, cognitivism and constructivism which are presented in this chapter.

The three theories build on quite different philosophical assumptions. Hence the theories do not only have an effect on the development of the content, curriculum, teaching and learning methods, but to a certain degree on the whole educational system as well. [Jud05]

The following listing summarizes the differences between the three classical learning theories.

- Behaviorism: *"Teaching and learning consists of information transmission, memorization and reproduction."* [Nab03]

- Cognitivism: *"Teaching and learning consists of the transformation of information into knowledge.* [Nab03]
- Constructivism: *"Teaching and learning is concerned with the generation of new knowledge."* [Nab03]

Another difference between the theories is that behaviorism and cognitivism are focusing on the teacher and the teaching, while constructivism is concentrating more on the student.

Behaviorism and cognitivism were both developed in the beginning of the 20th century. Constructivism is younger with its roots in the second half of the 20th century.

5.3 Behaviorism

Behaviorism deals with the objectively measure of the stimuli (input) and the resulting reaction (output) of an individual. The processes of the brain like learning, thinking, reasoning, feelings and motivation are not taken into account in behavioristic theories, as it is regarded impossible to measure these activities objectively.

Hence the brain is regarded as a black box, which is impossible to look into. The result of this is that behaviorism is only focusing on input and output.

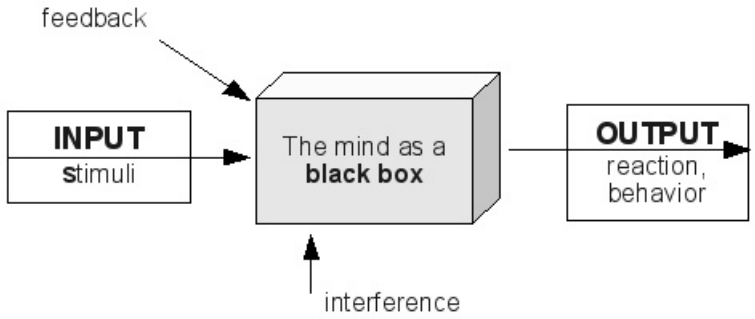

Figure 5.3: Behaviorism as a model with the mind as a black box. [Brä06]

The English philosopher John Lock (1632-1704) described human to be born as *"tabula rasa"*[2] - an empty page. According to behaviorism a human is formed through all kind of stimuli from the environment, and this results in a certain behavior - an output. [Brä06]

Learning is then simply reduced to training the reflexes of an individual. The effect on didactics is that the teacher has to find an optimal mix of inputs in order to produce the required output. [Brä06]

[2]tabula rase (Latin) - empty (undescribed) page.

Input is used to reinforce or suppress a behavior and can be positive (reward) as well as negative (punishment). [Nab03]

5.3.1 Conditioning

In behaviorism conditioning is identified as a universal learning process. Two types of conditioning are identified, which both result in different behavioral patterns: [Nab03]

- *Classical conditioning* is defined as natural reactions to stimuli. The Russian psychologist Iwan Pawlow (1849-1936) observed that animals reacted with a built in reflex to stimuli. [Brä06] For example a dog will start salivate when it eats or looks at food. In the theory of classical conditioning also humans are meant to have a "wired" connection between some stimuli and corresponding reactions. [Nab03]

- In *operant conditioning* stimuli is used in order to reinforce or suppress a specific response. Basically operant conditioning is built around a system of feedback. If a certain behavior is answered with a positive response, the behavior will be more likely in the future. One American behaviorist, Burrhus Frederic Skinner (1904-1990), used the feedback technique in order to reinforce certain behavior in pigeons, and in such way taught the birds tricks like dancing. [Nab03]

5.3.2 Criticisms of Behaviorism

Since its appearance in the early 20th century Behaviorism has been criticized for not being a learning theory suitable in all situations. Some of the critiques are summarized in the list below:

- Behaviorism considers the mind as a black box and is therefore not a suitable theory for all kind of learning. [Nab03]

- Behaviorism can not be used for explaining e.g. how small children learn languages, due to the fact that small children are not given a response to each word they pronounce. [Nab03]

- Experiments on rats have demonstrated that knowledge can be adapted to new situations without going through the stimulus-response cycle. (A rat that has through behavioristic techniques been taught to find its way around in a maze can change its behavior in order to respond to a change of the maze.) [Nab03]

- Memory is only regarded as a storage box for information. Knowledge is only saved to the box, but never worked with in order to learn or derive new information. [Nab03]

5.3.3 Behaviorism and Didactics

The effect of behaviorism on didactic is easy to understand. In the same way dogs or pigeons can be manipulated to change their behavior, students can in a system of feedback to desired response be manipulated to learn. In a school context a teacher would reward or punish the student based upon the student's behavior. (E.g. when the student is correctly or wrongly answering a question.)

Today behaviorism is to some extent regarded as outdated. It is however still used in computer based learning systems. Especially so called "drill and practice" computer programs, which are based on memorizing things, are based on behavioristic techniques. E.g. a system for learning Spanish that only lets you proceed to the next unit/level if you correctly have answered all the given questions. [Nab03]

Also in a university context behaviorism is not totally outdated. Certain type if information, like the name of body parts learned by medicine students, need to be learned by heart. Hence behavioristic learning exercises are not completely irrelevant in today's society.

5.4 Cognitivism

In contrast to behavioristic learning theories cognitivism does not look at the brain as a black box. In cognitivism the thought processes of the student are regarded as an important part of the learning process. In addition each person is recognized as a unique individual. [Nab03]

Learning is defined as an interaction between new knowledge and knowledge already present in the brain.

In behaviorism teaching and learning is simply a task of repeatedly presenting information until the student remembers it. In cognitivism learning is not thought of as information transfer but as information processing. Hence, the student has to process the presented information actively in order to learn.

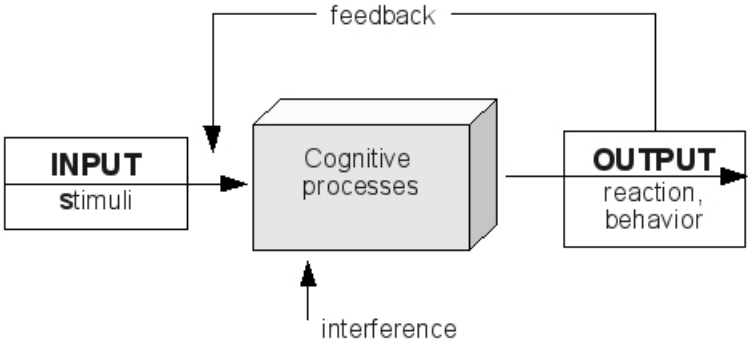

Figure 5.4: According to cognitivism new knowledge is generated through cognitive processes in the brain. [Brä06]

Figure 5.4 displays a model of the learning process according to cognitivism. Knowledge is generated through cognitive processes where new (external) information is combined with existing (internal, already learned) knowledge in order to create new knowledge.

According to cognitivism it is not enough for a teacher or trainer to present new information, because the student has not learned anything before this information has been processed by the brain. Hence, the challenge of cognitivism is to influence the student to process new information presented. [Var07]

5.4.1 Different Types of Knowledge

Cognitivism differentiates between three types of knowledge: [Jud05]

- Declarative knowledge - knowing facts. (E.g. Vienna is the capital of Austria.)
- Procedural knowledge - knowing how to do things. (E.g. how to drive a car.)
- Contextual knowledge - ability to understand the context of information (E.g. for the performance of a certain task.)

According to cognitivism each of the three types of knowledge represents a different cognitive process, and a teacher should take this into account when developing training programs. [Jud05]

5.4.2 Cognitivism and Didactics

The implications of cognitivism on didactics are quite different from the didactical implications of behaviorism. First of all the student has to be more involved and is required to take an active part in the learning process.

The role of the teacher is changed from being solely a presenter of information to being someone who manages to start a cognitive process in the mind of the students. For this the teacher might use different methods and techniques as listed below.

- Problem solving[3] - The teacher presents a problem for the student or a group of students. The problem presented should allow for alternative solutions. The goal of the process is not to teach the students a possible answer, but to train the students in methods and processes for problem solving in addition to obtaining subject specific knowledge. [Brä06]
- Learning through discovery - The students are to a certain degree in control of the learning process, and information has to be discovered without a teacher lecturing/presenting. The teacher is reduced to a guide that helps if necessary. This method should create curious and interested students, and the result would be increased motivation and better conditions for learning. [Brä06] It is however a paradox that learning through discovery seems to be a method of learning that requires interested and motivated students in the first place.
- Self-regulated learning - In this method the student is expected to organize the learning matter autonomously and to select a method of learning. Depending on the situation even the time of learning might be freely selected. Self-regulated learning requires that the student has a high degree of motivation and interest for the subject.

In the case of E-learning or so called blended learning the following methods are examples of methods inspired by cognitivism:

- Intelligent tutoring system (ITS) - a software that adapts to the student's level and progress with the material. The system does not only know about the material to teach, but also how this material is presented in the best didactical way to a student on a certain level. ITSs are usually found for assisting deterministic subjects like mathematics. [Nab03]
- Hypermedia / hypertext - forces the student to select the next step in the learning process on his/her own. This could lead to increased motivation, but could also cause a feeling of being lost. [Nab03]
- Simulation software - enables a student to "play" with the knowledge acquired and test it in a close-to-reality situation. Simulations can be a powerful tool for learning, but need to be developed by experts - hence tend to be costly.

[3] Also known as Problem Based Learning (PBL).

5.5 Constructivism

The essence of constructivism is that each person perceives the reality in their own subjective way. This personal perception of the reality is represented by a mental model which is influenced by e.g. what kind of experience a person has had. Hence, each person has a unique perception of the world. It is not possible for one person to claim that his or her perception of the reality represents the objective and true reality.

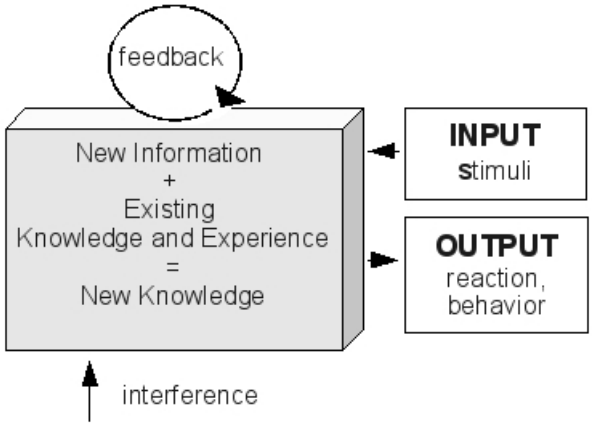

Figure 5.5: Model of the constructivistic theory of learning. Model based upon [Brä06].

In constructivism learning is an active process in which new information is combined with and reflected upon using existing knowledge and experience in order to create new knowledge. In contrast to cognitivism problem solving is not the focus of constructivism. Instead a student should independently develop own questions and problems, that again are used for creating new knowledge and raise new questions. In constructivism the teacher acts as coach or moderator. [Brä06]

5.5.1 Principles of Constructivism

To summarize, some of the most the most important principles of constructivism are listed below:

- Learning is actually the process of looking for *meaning* in new information. As a result of this, learning should always start with issues that the student can use in order to actively construct meaning. [Nab03]
- In order to be able to construct meaning of new information, a student needs to *understand* the context as well as the details. Hence, the process of learning should concentrate on the concepts. Details which can not be put into context by the student should be avoided. [Nab03]

- As each person has his/her own individual perception of the world, it is important for teachers to understand the *mental models* and associated assumptions of the students. [Nab03]
- The purpose of learning is not to memorize facts or to recite somebody else's meaning but to construct new meaning within the mental model of the student. Therefore, the quality of the learning process itself is regarded equally important to the knowledge acquired. Hence, the assessment of the students should include a validation of the quality of the learning process. [Nab03]

5.5.2 Constructivism and Didactics

Constructivism focuses on connecting facts with existing knowledge. The effect on didactical methods is that teachers should try to customize their teaching to the responses from a student or a group of students.

Constructivistic teaching methods usable in an E-learning context include:

- Open questions that enable the student to demonstrate that the new knowledge has relevance to existing knowledge or experience. [Nab03]
- Dialog or discussion between students. [Nab03]
- Hypertext, hypermedia and simulations. (Due to the same reasons as listed for didactical methods for cognitivism on page 81.) [Nab03]
- Micro-worlds that are quite similar to a simulation, but enable the students to change how the simulation works, not only the input parameters. [Nab03]

Chapter 6

A Combined Model for IT Governance

In this chapter a model for supporting the learning process of the IT governance supporting standards ISO 20000, ISO 27001 and COBIT is developed. In addition the developed model should assist in the process of checking an organization's compliance with the standards. The model could also serve as the theoretical basis for a software tool.

The focus of the model lies on the processes and associated requirements defined by the three standards. Less focus is put on control requirements as listed in e.g. ISO 27001 appendix A.

Context and Target Group

The primary intended target group for the model is operative managers in small and medium-sized IT organizations.

The model is not supposed to cover 100% of the requirements in the three standards, instead it should focus on the core areas of each standard. In this way organizations working with the model should be able to either learn about the content of or test the compliance of own organization in respect to the three standards in a relatively short time.

6.1 Outline of the Development Process

The development of a didactical model for supporting learning and assessment processes in organizations can probably be done in numerous different ways. The approach selected for this work is intended to take into account that the model has to find a balance between content and ease of use.

In general the development can be divided into five steps. Each step of the development process is represented with an own section in this chapter. (From chapter 6.2 to 6.6.)

In the following listing the process of developing the model is briefly explained.

1. Selection and identification of requirements, chapter 6.2

   The first step in developing the model is to select which content and level of granularity to include from the three standards. In addition a system for identification of content across all standards is developed.

2. Identify overlapping areas of content, chapter 6.3

   Next step in developing the model is to identify overlapping areas of content for the three standards. Hence, a detailed mapping between overlapping requirements is done.

3. Didactical implications on the developed model, chapter 6.4

   The intended use of the model is to support learning and assessing the compliance of an organization in respect of ISO 20000, ISO 27001 and COBIT. Both learning and assessing require a didactical foundation in order to support the target group optimally. Hence, before building the structure of the model a didactical concept has to be investigated. The didactical concept presented in this part is derived from the theories and concepts presented in chapter 5.

4. Structure of the model, chapter 6.5

   When requirements and overlapping areas of content are identified, the model itself can be developed. This is the main part of the development process and includes a system for organizing requirements and information, collect answers from assessments and aggregate results in order to determine the maturity level of processes.

5. Implementing the model in a software based tool, chapter 6.6

   The last step of the development process is not mandatory, because implementation or planning of a software tool built on the developed model are outside the scope of this work.

   However, the didactical concept developed for the model is built on learning theories that would have an effect on the implementation of the model in a software tool. Hence, a summary of these elements are presented in this last step of the development process.

6.2 Selection and Identification of Requirements

The scope of the model is not to cover all material in the standards, but to enable a small or medium-sized IT organization to quickly learn about the requirements needed. In addition the model should be able to approximately measure the quality of the IT governance system in respect of the three standards.

The model should not be a tool for a 100% accurate assessment of the quality of the IT governance systems, or cover all of the requirements in the standards. Due to this not all parts of all three standards are used in the model.

In this chapter a selection of content to be include in the model is performed. The selection tries to find a balance between detailedness and simplicity in order to find the correct scope and granularity of the model.

6.2.1 The Need for an Unique Identification

All three standards are described and organized in an own custom document structure. Without a common system for identification of content it will be hard and confusing to build a model and refer to content in the different standards.

An example of this would be how the three standards refer to the process of "assess and manage risks." COBIT handles this in the "control objective" part of the documentation with the conceptual identification P09.[1] ISO 20000 and ISO 27001 do not operate with identifications in the way COBIT does, hence one has to refer to the content by using the document structure. ISO 20000 covers assessment and management of risks in the parts 6.6.3[2] and 6.6.4[3] of the documentation, and ISO 27001 in the parts 4.2.1c to 4.2.1h[4] and in 4.2.2a,b[5].

In order to simplify how content is referred to the model needs

- a) a unique identification of content across all of the three standards,
- and b) a unique identification for content organized in the model.

It is important to make a distinction between a) and b) due to how content is used in the model. a) is used for referring to the original content in the three standards, and b) is used for referring to the aggregated structure created based on the overlapping areas of content between the three standards. (Presented in the next section - section 6.3.)

[1] COBIT PO9 is named "Assess and Manage IT Risks."
[2] Security risk assessment practices
[3] Risks to information assets
[4] Part of "Establish the ISMS."
[5] Part of "Implement and operate the ISMS."

Moreover a) is used for mapping the data collected by an internal audit back to the relevant sections in the standards. The internal audit itself is performed with the content organized in the model - b).

6.2.2 Naming Scheme for Identification of Content

In the following chapters lists of requirements that are defined in the documentation of COBIT, ISO 20000 and ISO 27001 and selected for use in the model are presented.

The unique identification assigned is built up as following:

- First letter = Identifies the type of requirements.
  - S = The requirement refers to the documentation in either COBIT, ISO 20000 or ISO 27001. [6]
  - M = The requirement refers to the model. [7]
- Second number = Identifies the standard
  - 1 = COBIT
  - 2 = ISO 20000
  - 3 = ISO 27001
  - If the first letter is "M" a second number is omitted.
- Third number(s) = Identifies a group of requirements within the standard.
- Fourth number(s) = Identifies the requirement.

Example of use:

- S1.2.3 is a reference to content in the COBIT standard, second group of requirements, third requirement.
- M2.3 is a reference to content in the model, second group of requirements, third requirement.

In some cases the group of requirements correspond to the group processes defined in the documentation of the standards. This is the case for e.g. all the groups listed for COBIT. However for e.g. ISO 27001 there are no logical groups of processes, hence they are custom developed for the development of this model. The same applies to some of the requirements as well.

[6] As a) described in chapter 6.2.1
[7] As b) described in chapter 6.2.1

In the following tables the field "ID" refers to the identification assigned in this work, and "Ref." is a reference to the COBIT, ISO 20000 or ISO 27001 documentation. In COBIT "Ref." refers to the conceptual process identification. In case of ISO 20000 and ISO 27001 it refers to the document structure.

6.2.3 COBIT Requirements Selected

The COBIT documentation is divided into a general part and a part containing control objectives. The general part of the documentation describes how to operate an IT governance system based on COBIT and puts the control objectives into context. The control objectives are designed for measure distinct business processes in an IT organization. [COB07]

Trade-off COBIT

For this work the general part is considered to be less important and will not be included in the model. All the 34 processes defined in the "control objective" part of COBIT will be included.

Each COBIT process is associated with a set of control objectives. For the development of the model details of the control objectives are of less importance, although they might be included as a reference in the implementation of the model in a software tool.

Group	ID	Requirement	Ref.
Plan and Organize	S1.1.1	Define a strategic IT Plan	P01
	S1.1.2	Define the Information Architecture	P02
	S1.1.3	Determine technological direction	P03
	S1.1.4	Define the IT processes, organization and relationships	P04
	S1.1.5	Manage the IT investment	P05
	S1.1.6	Communicate management aims and direction	P06
	S1.1.7	Manage IT human resources	P07
	S1.1.8	Manage quality	P08
	S1.1.9	Assess and manage IT risks	P09
	S1.1.10	Manage projects	P10
Acquire and Implement	S1.2.1	Identify automated solutions	AI1
	S1.2.2	Acquire and maintain application software	AI2
	S1.2.3	Acquire and maintain technology infrastructure	AI3
	S1.2.4	Enable operation and use	AI4
	S1.2.5	Procure IT resources	AI5
	S1.2.6	Manage changes	AI6
	S1.2.7	Install and accredit solutions and changes	AI7
Deliver and Support	S1.3.1	Define and manage service levels	DS1
	S1.3.2	Manage third-party services	DS2
	S1.3.3	Manage performance and capacity	DS3
	S1.3.4	Ensure continuous service	DS4
	S1.3.5	Ensure systems security	DS5
	S1.3.6	Identify and allocate costs	DS6
	S1.3.7	Educate and train users	DS7
	S1.3.8	Manage service desk and incidents	DS8
	S1.3.9	Manage the configuration	DS9
	S1.3.10	Manage problems	DS10
	S1.3.11	Manage data	DS11
	S1.3.12	Manage the physical environment	DS12
	S1.3.13	Manage operations	DS13
Monitor and Evaluate	S1.4.1	Monitor and evaluate IT performance	ME1
	S1.4.2	Monitor and evaluate internal control	ME2
	S1.4.3	Ensure compliance with external requirements	ME3
	S1.4.4	Provide IT governance	ME4

Table 6.1: Requirements selected from the COBIT documentation for use in the model.

6.2.4 ISO 20000 Requirements Selected

Group	ID	Requirement	Ref.
Management System	S2.1.1	Management Responsibility	3.1
	S2.1.2	Documentation Requirements	3.2
	S2.1.3	Competence, Awareness and Training	3.3
Service Delivery Process	S2.2.1	Capacity management	6.5
	S2.2.2	Service Level Management	6.1
	S2.2.3	Information Security Management	6.6
	S2.2.4	Service Continuity and Availability Management	6.3
	S2.2.5	Service Reporting	6.2
	S2.2.6	Budgeting and Accounting for IT Services	6.4
Relationship Process	S2.3.1	Business Relationship Management	7.2
	S2.3.2	Supplier Management	7.3
Resolution Process	S2.4.1	Incident Management	8.2
	S2.4.2	Problem Management	8.3
Release Process	S2.5.1	Release Management	10.1
Control Process	S2.6.1	Configuration Management	9.1
	S2.6.2	Change Management	9.2

Table 6.2: Requirements selected from the ISO 20000 documentation for use in the model.

Trade-off ISO 20000

The ISO 20000 documentation describes 13 business processes in five categories. In addition the documentation lists other general requirements not directly linked to any of the 13 business processes. Some of those requirements are valid for this model and are summarized in three additional requirements.[8]

Part four of the ISO 20000 standard contains general requirements for the PDCA cycle. This work focuses on the 13 processes of ISO 20000, hence part four is deliberately omitted.

[8]The group containing the additional requirements is called “Management System”.

6.2.5 ISO 27001 Requirements Selected

Group	ID	Requirement	Ref.
Operate an ISMS	S3.1.1	Establish the ISMS	4.2.1
	S3.1.2	Implement and Operate the ISMS	4.2.2
	S3.1.3	Monitor and review the ISMS	4.2.3
	S3.1.4	Maintain and Improve the ISMS	4.2.4
	S3.1.5	Documentations requirements	4.3
Management	S3.2.1	Management Responsibility	5
Review and Improvement	S3.3.1	Internal ISMS audits	6
	S3.3.2	Management Review	7
	S3.3.3	ISMS Improvement	8

Table 6.3: Requirements selected from the ISO 27001 documentation for use in the model.

Trade-off ISO 27001

Unlike ISO 20000 and COBIT, ISO 27001 is not centered around a set of business processes. Due to this the selection and grouping of requirements for ISO 27001 is not that obvious.

For this work it seemed most suitable to focus the requirements of ISO 27001 around the PDCA cycle. Part four of the ISO 27001 documentation is built around the PDCA cycle, and this part also describes the core of implementing and operating an ISMS.

Due to this it was self-evident to use a more fine-grained description for the requirements in part four than for the other parts.

Appendix A of ISO 27001 contains control objectives for an ISO 27001 system. They are not selected to be part of this model, due to the fact that they go quite into detail and that this would not harmonize with the two other standards.

Instead focus will be put on the normative parts of ISO 27001 - parts 4 to 8. [105c]

6.3 Identify Overlapping Areas of Content

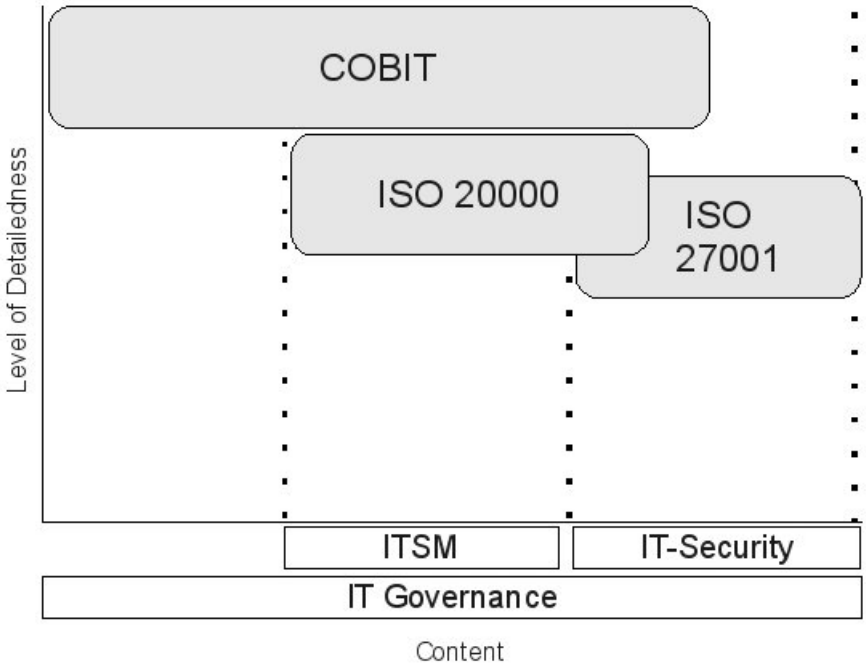

Figure 6.1: Simplified visualization of content in COBIT, ISO 20000 and ISO 27001.

IT governance systems are supposed to manage all aspects of IT in an organization. COBIT aims at being a complete framework for IT governance management systems and is regarded as being quite extensive. It covers a broad spectrum of IT related processes.

The implementation of an IT governance management system based on COBIT does not exclude the implementation of an ISO 20000 and ISO 27001 system. They are all compatible and if combined would most likely have strong synergetic effects.

As figure 6.1 visualizes all of the three standards cover much of the same material.

COBIT covers a broad scope and includes virtually all of the material covered by ISO 20000, but on a more abstract level. In addition COBIT also covers major parts of IT-Security, but is not as specialized as ISO 27001.

ISO 27001 has quite concrete control objectives, and of the three standards seems to be the one going most into details.

6.3.1 The Need for Mapping of Content

The model should utilize the fact that the three standards share much of the same scope of content.

This is primarily due to two reasons:

1. A model that takes into account that the three standards have overlapping content would probably require less effort by a learner wanting to learn about the scope and content of all three standards.

2. An internal audit based on a shared model of the three standards would most likely require less time by the auditor than if the audit was based on three different models.

6.3.2 Aggregate and Grouping Requirements

In total 59[9] requirements are selected from the three standards to be included in the model.

From those 59 requirements a common scope has to be derived, but still without losing much of the detailedness of the requirements.

COBIT covers almost all of the content of the two other standards, but on a more abstract level. Hence it is self-evident to use the COBIT processes and grouping of processes as a foundation.

As a result of this insight the following strategy for mapping the content between the three standards was selected:

1. All COBIT processes and groups of processes were listed in a table.

2. The parts of ISO 20000 and ISO 27001 that were selected to be included in the model were investigated in detail and mapped to the most suitable COBIT process.

3. The ISO 20000 and ISO 27001 requirements that did not have overlapping content with any of the COBIT processes were listed in an own process group.

The result was a list of 38 requirements in five groups. Of the 38 requirement 34 are named after the COBIT processes and four are given a name based on the content of the requirements they represent.

Four requirement groups are named after the process groups in COBIT and one is named “Information Security”.

The reason for this naming is that ISO 27001 was the only standard that listed requirements that did not fit 100% into the content of COBIT. Hence an own process group for the requirements that did not fit had to be inserted. This represents the third step in the listing above.

[9] As listed in chapter 6.2.2

6.3.3 Listing Overlapping Areas of Content

The following table lists overlapping areas of content between the parts of the standards selected for use in the model. The groups and requirements equal the groups and process names in COBIT, except for the last group and the requirements within.
The field "ID" refers to the identification scheme developed for this work, as presented in chapter 6.2.2. The fields "COBIT", "ISO 20000" and "ISO 27001" refer to the corresponding parts in the standards.

Group	ID	Requirement	COBIT	ISO 20000	ISO 27001
Operate an ISMS	M1.1	Define a strategic IT plan	P01	-	-
	M1.2	Define the information architecture	P02	-	-
	M1.3	Determine technological direction	P03	-	-
	M1.4	Define the IT processes, organization and relationships	P04	3.1	-
	M1.5	Manage the IT investment	P05	6.4	-
	M1.6	Communicate management aims and direction	P06	3.1	-
	M1.7	Manage IT human resources	P07	-	-
	M1.8	Manage quality	P08	7.2	-
	M1.9	Assess and manage IT risks	P09	3.1f	4.2.1c-h, 4.2.2a-b
	M1.10	Manage projects	P10	-	-
Acquire and Implement	M2.1	Identify automated solutions	AI1	-	-
	M2.2	Acquire and maintain application software	AI2	-	-
	M2.3	Acquire and maintain technology infrastructure	AI3	-	-
	M2.4	Enable operation and use	AI4	10.1	-
	M2.5	Procure IT resources	AI5	7.3	-
	M2.6	Manage changes	AI6	10.1, 9.2	-
	M2.7	Install and accredit solutions and changes	AI7	10.1	-

Table 6.4: Part 1 of 2: Overlapping areas of content between COBIT, ISO 20000 and ISO 27001.

Group	ID	Requirement	COBIT	ISO 20000	ISO 27001
Deliver and Support	M3.1	Define and manage service levels	DS1	6.1, 3.1, 3.2	-
	M3.2	Manage third-party services	DS2	7.3	-
	M3.3	Manage performance and capacity	DS3	6.5	-
	M3.4	Ensure continuous service	DS4	6.3	-
	M3.5	Ensure systems security	DS5	6.6	4.2.1a,b,i,j, 4.2.2f,g, 6
	M3.6	Identify and allocate costs	DS6	6.4	-
	M3.7	Educate and train users	DS7	3.3	-
	M3.8	Manage service desk and incidents	DS8	7.2, 8.2	-
	M3.9	Manage the configuration	DS9	9.1	-
	M3.10	Manage problems	DS10	8.3	-
	M3.11	Manage data	DS11	-	-
	M3.12	Manage the physical environment	DS12	-	-
	M3.13	Manage operations	DS13	-	-
Monitor and Evaluate	M4.1	Monitor and evaluate IT performance	ME1	6.2, 7.2	4.2.3b-h, 4.2.4
	M4.2	Monitor and evaluate internal control	ME2	6.2	4.2.3a
	M4.3	Ensure compliance with external requirements	ME3	-	-
	M4.4	Provide IT governance	ME4	-	-
Information Security	M5.1	ISMS – Manage documentation	-	-	4.3
	M5.2	ISMS – Management responsibility	-	-	5
	M5.3	ISMS – Management review	-	-	7
	M5.4	ISMS – Improvement	-	-	8

Table 6.5: Part 2 of 2: Overlapping areas of content between COBIT, ISO 20000 and ISO 27001.

6.3.4 Comments on Mapping the Content

While mapping the requirements in the three standards to each other several challenges arose. The major challenges are documented below.

COBIT Requirements not mapped to ISO 27001 or ISO 20000 Requirements

Due to the fact that COBIT covers a broader scope than ISO 27001 and ISO 20000 several COBIT requirements do not have a mapping to the other standards. This is the case for e.g. the requirement "Define a strategic IT Plan" or "Provide IT Governance."

Mapping of a ISO 27001 or ISO 20000 Requirement to more than one COBIT Requirement

Another challenge is that the processes do not completely overlap each other. The result is that some requirements from ISO 27001 and ISO 20000 are mapped to more than one COBIT requirement.

An example of this is the process of "Service Reporting" in ISO 20000. This process is only concerned with the reporting itself - not the monitoring of systems or the collection of the data used in the reports.

The closest match to the ISO 20000 "Service Reporting" process in COBIT are the two processes "Monitor and Evaluate IT- Performance" and "Monitor and Evaluate Internal Controls". Both COBIT processes do have a different primary focus than the "Service Reporting" process in ISO 20000, but include reporting itself as one of several tasks. Hence the ISO 20000 process does not really match either of the COBIT processes. However, in order to be able to make the mapping between the standards compromises are necessary.

6.4 Didactical Implications on the Developed Model

In order to design a didactical model for learning and assessing successfully the requirements of COBIT, ISO 20000 and ISO 27001 the context of learning has to be taken into account.

The model is supposed to support self learning of individuals in small and medium sized organizations that want to or are in the process of improving the quality of its IT operations with the use of standards.

Hence, one can assume a high degree of motivation to learn and a desire to quickly find the essence or core of the material. Moreover it is likely that the users of the model are concerned with practical solutions and implementation strategies.

6.4.1 Underlying Learning Theories Supporting the Model

A modern teaching concept is most likely influenced by several strategies of learning. For the development of the model the theories of cognitivism and constructivism are considered to be especially important.

Behavioristic learning theories are considered to be less important for this work. The reason for this is that behaviorism is focused solely on stimulus (input) and response (output) by the learner, and does not consider the fact that the student has to start a cognitive process in order to work with the material.

A standard can be viewed as a collection of requirements. A requirement is ideally an indisputable fact of type: "It is required that X is performed at least annually." Behavioristic methods are well suited for memorizing facts, and one could easily be misled to think that such methods would fit well for supporting the learning in relation to a standard.

However, the case is that it is far more important to understand the concept of a standard and the implication of this concept on the own organization than to learn the individual requirements by heart.

6.4.2 Types of Knowledge Relevant for the Model

In cognitivism at least three types of knowledge are distinguished. Declarative knowledge is about facts, procedural knowledge is about knowing how to do things, and contextual knowledge is about understanding the background or specific circumstances of information.[10]

The model developed in this work is supposed to support the learning of declarative and contextual knowledge. The learning of procedural knowledge lies not within the scope of this model. The model is supposed to help the learner to start a cognitive process that will lead to new procedural knowledge.

[10] As described on page 81.

In other words, the model is supposed to support the learning of facts in the three standards and the context of those facts. It is not supposed to teach the learner the best way to fulfill requirements of a specific standard. It is regarded as more important that the model could be used to initiate a cognitive process, resulting in the learner developing his/her own strategies for implementations of systems that fulfill the requirements.

6.4.3 Didactical Requirements for the Developed Model

Based on the theories of cognitivism and constructivism four didactical requirements for the developed model have been developed:

1. The model should be structured in such a way that the individual facts are put into context.

2. The model should support "self-regulated learning", and not force a learner into a predefined scheme. Modules in the model should be autonomous, so that the learner can select which part to specialize in without being constrained by dependencies between modules.

3. Modules and requirements should be organized in such a way that it is easy to find a specific requirement and browse through requirements to quickly get an overview. This would support the concept of "Learning through discovery."

4. Each conceptual module should include a set of open questions and example answers. According to cognitivism this should start an internal learning process for the learner and new knowledge should be generated. This is based on the concept of "Problem Solving."

The didactical requirements are independent of an implementation of the model in a software tool. Nevertheless, the practical use of the model would definitely be simplified if realized in a software tool instead of e.g. in form of a book.

Chapter 6.6 contains more thoughts on didactical extensions to the model if implemented in a software tool.

6.5 Structure of the Model

In the task of developing the model several requirements had to be taken into account.

First the model should fulfill the requirements defined in the introduction to this work. In specific this means that the model should be usable in a self learning context as well as a tool for assessing the compliance of internal processes. In addition the model should utilize the fact that the three standards have areas of overlapping content.

Secondly the didactical requirements to the model as listed on page 99 had to influence the development of the model as well.

Summarized the requirements to the model pointed in the direction of a hierarchical structure where specific subject areas are grouped into modules.

6.5.1 Learning vs. Assessing

The model should be able to operate in two modes. In the **learning mode** it should be able to support the learner in quickly gathering information and get an overview of the selected subject area. According to cognitivistic learning theory it should emphasize on context of information and focus less on details.

As the didactical requirements state each module should be independent of each other, so that the learner could start specializing in a specific subject area without being forced into a predefined sequence of modules. References to the relevant parts of the standards should always be present and if necessary hint on how to find more information on the subject.

The learning mode should not prescribe solutions for how the requirements of the standards should be fulfilled. Instead it should help the learner to ask the right questions in order to start a thinking process.

In the **assessing mode** the model should force the learner/auditor to run through a predefined sequence of modules and questions. This should however be done in a semi intelligent way, so that the auditor does not have to answer the same question in more than one way. E.g. if the auditor has already answered the question “Are incidents recorded?” in the negative, he or she should later in the model not be asked questions like “Does a system for reporting of recorded incidents exist?”.

In addition a system for recording the answers from the auditor should be able to map the answer from one question to the relevant part(s) in the standards. The recorded answers enable the model to investigate the maturity level of the processes defined in COBIT and ISO 20000 in addition to the custom developed requirements groups developed for ISO 27001 in this work. (ISO 27001 does not define processes in the same way as the two other standards do. Hence, a custom grouping of requirements had to be developed as described in chapter 6.3.3.)

6.5.2 Structure

The developed model tries to incorporate a balance between requirements to the model on one hand with simplicity and a concept easy to understand on the other hand.

One decision that had to be made was whether to develop two separate models - one for assessing and one for learning - or to try to fit the requirements of both use cases into one model.

It was considered to be most important that the model should be easy to understand and implement in a possible software based solution. Hence, one common model for both use cases was developed.

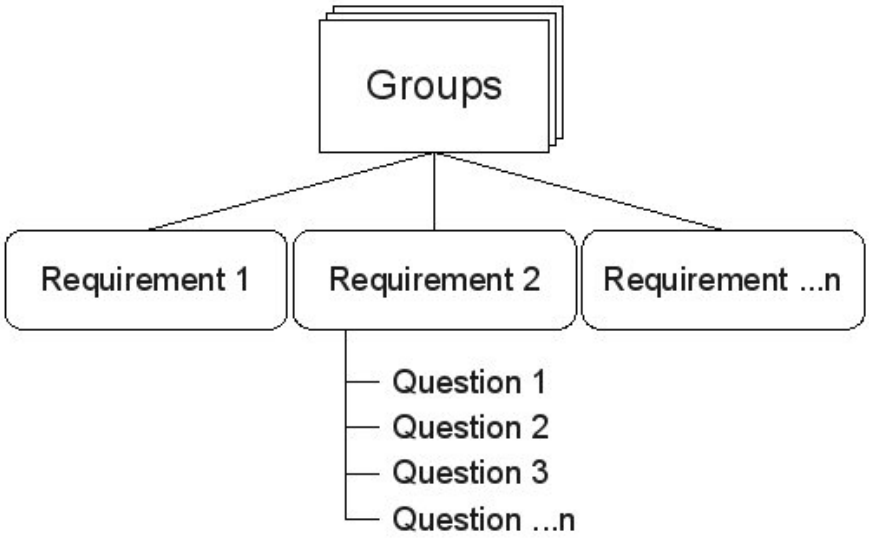

Figure 6.2: Visualization of the structure of the model.

The model is built as a hierarchical structure of groups, requirements and questions.

Groups and Requirements

In the model groups and requirements are identical to the structure of groups and requirements identified in the areas of overlapping content as listed in chapter 6.3.3 on page 95. In total five groups and 38 requirements are used in the model.

The reasons and discussions about why especially those groups and requirements were selected have been done in chapter 6.2 and chapter 6.3. Hence, the focus of this section is on the question parts of the model.

Questions

As the list of didactical requirements to the model suggested questions should be used in order to start a thinking process. Hence questions - and not statements - are used as the smallest part in the hierarchical structure.

This also fits well with the use case of assessing an organization's compliance with the standards. Such assessment has to operate with questions, and by basing the learning mode on the same questions one model can be used for both use cases.

However, questions alone would not be enough for the learning mode, it should be accompanied by extra information presented to the learner. This extra information should describe shortly what is meant by the question, how this is required by the three standards and a reference to where more information can be found.

Moreover, questions developed have to take into account that a requirement might cover the scope of more than one standard. E.g. The requirement with ID M.4.1 (Monitor and evaluate IT performance) is supposed to comprise elements from all three standards. Hence, questions have to be developed to grasp the essence of several standards as well as contain a linkage to the standards it relates to.

For simplicity all questions should be formulated as yes/no questions. This enables easy analysis of the answers given if in assessment mode, and would make the aggregation and presentation of the results more comprehensive.

Example Question

The following table - table 6.6 on page 103 - shows an example of a complete set of questions for a requirement. In general it is expected that three to six questions per requirement should be enough to explain or measure the most important aspects of the requirement.

The "ID" field in the table identifies the question. E.g. "M1.2(3)" is a reference to the third question of the second requirement in the first group of requirements in the model. The list of requirements and groups of requirements used in the model is listed on page 95.

The "Question" field in the table contains three pieces of information. First a question is presented. If in assessment mode, this question has to be answered with yes or no. If in learning mode, the question serves as a heading, and should make the learner think about how this subject applies to his/her organization. Secondly a description of the subject is given. This is supposed to help the learner/auditor to understand the question better.

The third and last piece of information contained in the question field, is a reference to more information about the subject. This could include references to the documentations of the three standards, but could also be

a reference to other sources like books etc. The reference given in this field is simply an information to the user and does not have the same purpose as the "Ref." field in the table.

The "Dep." field in the table contains a reference to another question this question is dependent on. This field is only valid if in assessment mode, and can be empty. If the field contains a reference to another question, it means that the referenced questions had to be answered with "yes". If answered with "no", all questions depending on that question will be skipped. The result is that an auditor will not be asked follow-up questions to a question already answered "no" to.

The last field in the table - the "Ref." field - is a reference to the corresponding parts in the original documentation. This field is used for mapping the answers from an assessment to the corresponding parts in the documentations of the standards. The reference is on the form S1.2.3 as described in chapter 6.2.

If the model was to be implemented in a software tool only the "Question" field and possible the "ID" field of the table should be visible to the user. The "Dep." and "Ref." fields are meta data and should not be displayed to the user.

ID	Question	Dep.	Ref.
M1.9(1)	Question: Are risks to the organization caused by IT documented? Description: An organization certified according to COBIT, ISO 20000 and ISO 27001 is required to have an operating risk management process for information technology. A functional risk management system requires risks to the organization to be documented. This documentation should be reviewed on regular intervals. References: COBIT: P09 ISO 20000: 3.1f, 4.1f, 4.2d, 6.3(2nd para.), 6.6b, 9.2(3rd para.) ISO 27001: 0.2b, 3,14, 4.2.1, 4.2.2, 4.2.3d, 4.3.1, 5.1f, 7.3b-c, 8.3(7th para.)	-	S1.1.9 S2.1.1 S3.1.1 S3.1.2

Table 6.6: Part 1 of 3, questions for requirement M1.9 - "Assess and manage IT risks."

ID	Question	Dep.	Ref.
M1.9(2)	Question: Are treatments for IT risks identified and evaluated? Description: A risk management system does not only require risks to be documented, but also to identify possible solutions for how to reduce or avoid risks. This includes transferring risks to other parties like suppliers, insurers etc, or to avoid the risk completely. All identified risks should be documented with possible solutions or actions. References: COBIT: P09 ISO 20000: 3.1f, 4.1f, 4.2d, 6.3(2nd para.), 6.6b, 9.2(3rd para.) ISO 27001: 0.2b, 3,14, 4.2.1, 4.2.2, 4.2.3d, 4.3.1, 5.1f, 7.3b-c, 8.3(7th para.)	M1.9(1)	S1.1.9 S2.1.1 S3.1.1 S3.1.2
M1.9(3)	Question: Are management and process owners informed about residual risks? Description: Identified risks are required to be documented. The documentation should include descriptions of how to avoid or transfer the risk. Risks that are not avoided or transferred are called residual risks, and should be approved by the management. The risk management process is required to inform relevant process owners and parts of the management of residual risk. References: COBIT: P09 ISO 20000: 3.1f, 4.1f, 4.2d, 6.3(2nd para.), 6.6b, 9.2(3rd para.) ISO 27001: 0.2b, 3,14, 4.2.1, 4.2.2, 4.2.3d, 4.3.1, 5.1f, 7.3b-c, 8.3(7th para.)	M1.9(2)	S1.1.9 S2.1.1 S3.1.1 S3.1.2

Table 6.7: Part 2 of 3, questions for requirement M1.9 - “Assess and manage IT risks.“

ID	Question	Dep.	Ref.
M1.9(4)	Question:Are control objectives and controls for treatments of risks selected? Description: Control objectives and controls are used for ensuring the quality or effectiveness of a system or process. COBIT and ISO 27001 require controls objectives and controls to be implemented for treatment of risks. Both COBIT and ISO 27001 provide a set of control objectives usable in the context of treatments of risks. References: COBIT: P09 ISO 27001: 4.2.1g, Annex A	M1.9.(2)	S1.1.9 S3.1.1

Table 6.8: Part 3 of 3, questions for requirement M1.9 - “Assess and manage IT risks.“

In assessment mode questions should be asked in such a way that they minimize the total number of total questions. E.g. for the question M1.9.(1) - ”Are risks to the organization caused by IT documented?“ - covers actually at least to questions. A positive answer to this question does not only confirm that risks are documented, but also that risks are actually thought of as an issue in the organization. Hence, it is unnecessary to ask if a risk management process exists because one can assume that if risks are documented at least a simple risk management process must be in place.

Furthermore the numbers of questions in assessment mode are reduced due to dependencies between questions. If e.g. question M1.9(1) - ”Are risks to the organization caused by IT documented?“ - answered with ”no“, all the other questions for this requirement will be skipped due to dependencies. If risks are not documented, one can assume that e.g. treatments of risks are not identified and evaluated either.

A map of dependencies of the example above is listed under:

- M1.9(1) - Are risks to the organization caused by IT documented?
  - M1.9(2) - Are treatments for IT risks identified and evaluated?
    - M1.9.(3) - Are management and process owners informed about residual risks?
    - M1.9.(4) - Are control objectives and controls for treatments of risks selected?

In assessment mode the questions M1.9(3) and M1.9(4) are only asked if question M1.9(2) is answered with ”yes“. The same relationship exists between question M1.9(2) and M1.9(1).

6.5.3 Defining Suitable Process Capability Levels

Operating in assessment mode the model should be usable for estimation of the maturity of processes. In this context processes are defined as the processes/requirements identified for use in this model as described in chapter 6.2.

Hence, the output of the model if used in assessment mode should be a report of the maturity levels of the 34 processes defined in COBIT, the 16 processes defined in ISO 20000 and the nine ISO 27001 processes custom designed for this work.

CMMI are using the continuous representation for measurement of single processes. In continuous representation six capability levels are defined.

A capability level of zero means that the process is not, or not well enough performed for a classification on level one. If a process is measured to be on capability level five it means that the process is optimally performed. The names of the capability levels in CMMI are: incomplete(0), performed(1), managed(2),defined(3),quantitatively managed(4) and optimizing(5).

The model developed in this work is deliberately kept simple in order to be a practical tool for organizations wanting to assess their own compliance with the three standards. Due to this each requirement in the model should only be measured with three to six questions each.

The result of this is that the model should be so simple to use, that anyone with knowledge of the operation of the organization should be able to assess the compliance.

The downside of this simplicity is the model's lack of details. Asking three to six questions about each process would probably not acquire enough information for determination of the correct capability level on a CMMI like scale.

Hence the need for using an own custom capability scale for this model. Based on the CMMI capability levels one to three are the following capability levels for the model proposed:

- **Level 0 - not performed**, the process is non existent in the organization.
- **Level 1 - performed**, the process exists and supports the operation of the organization on a basic level.
- **Level 2 - managed**, the process is to a certain degree formalized. In times of stress shortcuts are taken, and this destroys the continuity and quality of the process.
- **Level 3 - defined**, the process is formalized, and could be a candidate for a formal COBIT, ISO 20000 or ISO 27001 compliance review by an external party.

6.5.4 Aggregating Results in Assessment Mode

If used in assessment mode the model should report capability levels of processes and process groups in COBIT, ISO 20000 and ISO 27001 as listed in chapter 6.2.

Processes in the Standards vs. Requirements in the Model

The model itself is organized around a structure of groups and requirements representing the overlapping content between the three standards as defined in chapter 6.3.

Hence, one can not simply calculate the results of all questions for a requirement in the model to identify the capability level of processes. Such method would lead to capability levels of the requirements according to the list of overlapping content as listed in chapter 6.3 and not of the capability levels of processes in the three standards as listed in chapter 6.2.

Aggregating Results

Questions	Requirements					
	:	S1.1.9	S2.1.1	S3.1.1	S3.1.2	:
..						
M1.9(1)		1	1	1	1	
M1.9(2)		1	1	1	1	
M1.9(3)		0	0	0	0	
M1.9(4)		0	-	0	-	
..						
Relative		0,50	0,67	0,50	0,67	
Capability Level		2	3	2	3	

Legend
1 = answered with yes
0= answered with no
- = not valid

Figure 6.3: Schema for calculating the capability level of processes.

Figure 6.3 presents a method for aggregating the results of the data collected from the model in assessment mode in order to determine the capability level of processes.

In the table all processes in the three standards should be listed horizontally. These are the processes identified in chapter 6.2. For simplicity

only the processes referenced in the example on page 102 are inserted in the table.

In the table all questions of the model should be listed vertically. In this example we limit the questions to the four questions developed in chapter 6.5.2.

The answers recorded from the model are represented in the table as either "1" or "0". The first indicates that the user has answered the question with "yes", and the latter that the question was answered with "no".

Most questions in the model would only be relevant for some processes in the standard. The rest of the processes would then be marked with "-" as an indication of an invalid choice.

E.g. question M1.9(4)[11] is only referenced to process S1.1.9[12] and S3.1.1[13] as described on page 105. Only cells where question M1.9(4) and valid processes meet are allowed to contain "1" or "0" - all other cells in the row of M1.9(4) are given the value "-".

In order to calculate the capability level of a process, one has to find the relative number of questions positive answered for the standard in question.

$$\frac{\text{sum of positive answers}}{\text{sum of possible answers}} = \text{relative sum}$$

Determine Capability Levels

Using the data for process S2.1.1 from table 6.3 we calculate the relative number of positive answers like this: $\frac{1+1+0}{3} \approx 0,67$

In order to find the correct process capability level the following rules are applied:

- If **relative sum = 0** then capability level is 0.
- If $\frac{1}{3} >$ **relative sum** > 0 then capability level is 1.
- If $\frac{2}{3} >$ **relative sum** $\geq \frac{1}{3}$ then capability level is 2.
- If **relative sum** $\geq \frac{2}{3}$ then capability level is 3.

The example in figure 6.3 contains only four processes and questions and is extremely simplified. In a real life scenario all the processes and questions in the model should be used and numbers in the formula above would be quite different. Nevertheless, the number of positive to possible answers ratio could still be $\frac{2}{3}$ as in the example, and this would result in process capability level 3.

[11] M1.9(4) - "Are control objectives and controls for treatments of risks selected?"
[12] S1.1.9 - "Assess and manage IT risks"
[13] S3.1.1 - "Establish the ISMS"

6.6 Implementing the Model in a Software Tool

The concept of the model is not very complex and it would be possible to use it without software support. However, the use of the model would be simplified if managed by a software tool.

Especially the case of using the model in assessment mode would be more practical if supported by relevant software. This would enable the automatic management of dependencies between questions and aggregation and presentation of results.

In addition to supporting the model, a software implementation would provide new possibilities not possible without the use of technology. E.g. the implementation of the model as a web based application would enable users to connect and share information and knowledge in new ways.

The following list summarizes some ideas for supporting the model in a web based online tool:

- If used in learning mode, the software could provide the users with two alternative views. Both views should be built around a hierarchical structure.
  - The first view is used for organizing the content of three standards in process groups and processes. If possible from a legal point of view, the relevant text passages from the three standards could be included as a reference. This view represents the core structure of the standards itself as listed in chapter 6.2.
  - The second view displays the model in a structure of groups and requirements. When selecting a requirement, the user is presented - in addition to the text for the requirement itself - a link to relevant parts in the first view. This view represents the structure and content of the model as described in the chapters 6.3 and 6.5.
- Forum functionality would enable users to discuss different aspects of the model or the implementation of an IT governance system in general. For distinct elements in the model like groups, requirements and questions, a link to the relevant discussion forum could be provided. Discussion threads in forums should contain meta data for which objects in the model this thread is relevant for.
- Users should have the possibility to participate in the quality of the documentation. This could e.g. be done by connecting each element in the model to a wiki page, enabling user generated content to extend the standard documentation of the model.
- The results from assessments could be visualized and compared with other companies in the same industry. If an assessment is performed on

regular intervals as parts of a continual improvement program towards a certification, results from previous assessments could be compared with the latest assessment in order to visualize historical trends.

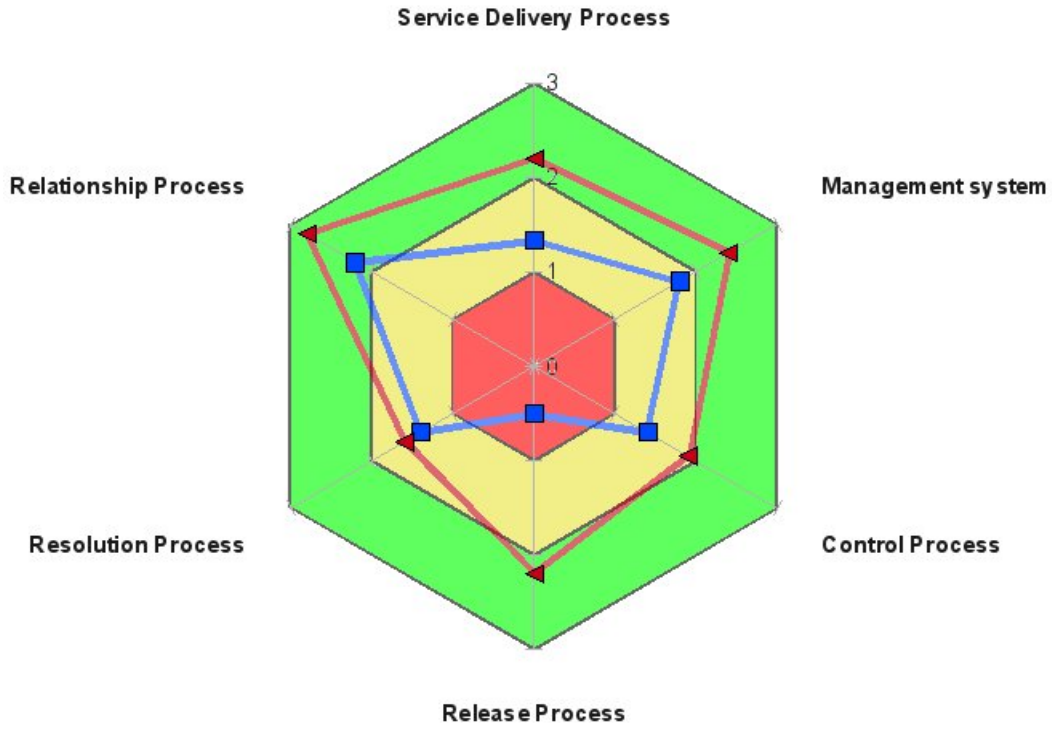

Figure 6.4: Possible graphical representations of the results of an assessment.

The figure above shows a possible graphical representation of the results of the model in assessment mode.

In specific it displays the process groups in ISO 20000 as defined in chapter 6.2.4. The colored areas represent the process capability levels - red for level one, yellow for level 2 and green for level 3.

The blue line (squares) represents the result of the organization's results of the assessment, and the red line (triangles) represents the benchmark value. The benchmark value is used for comparison and could be e.g. the average value of all assessments recorded by the system.

Chapter 7

Conclusion

The main goal of this work is to solve some of the challenges small and medium sized IT organizations face in the process of implementing an IT governance system based upon COBIT, ISO 20000 or ISO 27001.

Small and medium sized IT organizations do normally not have the required level of knowledge about the three standards and this would have to be solved either by using external consultants or by educating own employees.

In any case costs will occur. It is assumed that these costs of acquiring the basic level of knowledge will be a larger obstacle for smaller IT organizations starting the work of improving the quality of organizational processes than for larger organizations.

7.1 Hypotheses vs. Results

The core of this work is the development of a conceptual model that makes it easier for small and medium sized organizations to obtain a basic level of knowledge about COBIT, ISO 20000 and ISO 27001.

In the introduction to this work four hypotheses about the model were presented. In the following sections these hypotheses are compared with the actual result of the work.

Hypothesis 1 - Confirmed

> *One combined model can be developed for assisting the learning process of COBIT, ISO 20000 and ISO 27001 in a self training context.*

A detailed analysis of the structure and content of the three standards showed that the three standards can be combined in one model.

COBIT and ISO 20000 have contents that fit well together, and both are built around a set of defined business processes. ISO 27001 has a different

structure and is not organized around processes in the same way COBIT and ISO 20000 are. Hence, the structure of ISO 27001 had to be partly reorganized in order to make it fit into the logical scheme of the two other standards. This is described in chapter 6.2.5.

Another challenge in relation to this hypothesis was to determine the required level of detailedness of the model. On the one hand if 100% of the content of the three standards should be included it would be very hard to create one model for all three standards. On the other hand should the model at least have a certain level of detailedness in order to fulfill its purpose.

Due to this the model focuses only on the core parts of the standards.

Hypothesis 2 - Partly Confirmed

> *One combined model requires less time of the learner than it would be the case if learning programs for the standards were developed independently of each other.*

This hypothesis relies on the assumption that the contents of the three standards overlap each other to a certain degree. E.g. how the three standards describe basic risk management is the same, hence a learner does only have to learn about this once.

As described in chapter 6.3, this assumption proved to be true for COBIT and ISO 20000 but only partly true for ISO 27001.

Due to the use of overlapping content as a foundation for the model it is likely that this hypothesis can be confirmed. However, to be absolutely positive a study that compares learners using the model with learners using learning programs developed independently of each other has to be conducted.

Hypothesis 3 - Confirmed

> *The same model can be applied in the context of a combined internal audit of the implementation of COBIT, ISO 20000 and ISO 27001.*

The main task of this work was to develop a model to support the learning of requirements in COBIT, ISO 20000 and ISO 27001. Due to didactical considerations - specifically the learning theories of cognitivism and constructivism - a hierarchical structure that puts individual facts into context was selected. The design organizes questions as the smallest part into requirements, and requirements are again organized into groups.

This structure does also fit well in the context of assessing an organization's compliance with the three standards. Hence the model was developed

to operate in two modes - one for assessing the compliance and one for supporting the learning process.

The assessment mode forces the user of the model into a predefined structure of content and provides methods for how to calculate the results of the assessment. The learning mode enables a user to freely select content to specialize in.

Hypothesis 4 - Confirmed

> *In the context of internal compliance audit of the three standards the maturity of the organizational IT processes can be investigated.*

In the course of the development of the model a custom maturity model based on the CMMI capability levels was developed.

The maturity model defined in this work - as described in chapter 6.5.3 - contains only four levels ranging from non existing (level one) to defined (level three). The model is not able to determine higher maturity levels equal to e.g. level four or five in CMMI.

The model can only determine the maturity level of processes if used in assessment mode.

The processes being referred to are the processes identified for use in the model as defined in chapter 6.2. For COBIT and ISO 20000 this includes the processes as defined in the standards. For ISO 27001 the standard does not define business processes as such, hence the maturity levels refer to the requirements and groups of requirements identified to be included in the model as described in chapter 6.2.5.

7.2 Future Research Implications

As confirmed in hypotheses one and three a combined model can be used for learning and assessing the requirements of COBIT, ISO 20000 and ISO 27001. The developed model does not cover the full level of detailedness in the three standards, and due to this can only be used to measure maturity of business process equal to CMMI level three.

In order to measure maturity levels equal to CMMI level four and five a significant higher level of detailedness has to be incorporated into the model. If this can be done in a practical way is something future research could investigate.

Hypothesis two in this work could only be partly confirmed. In order to definitively confirm or disapprove the hypothesis the conceptual model developed in this work has to be developed to a full extent - meaning completing the model with questions for all groups identified in chapter 6.3.3 as demonstrated in chapter 6.5.2. The fully developed model is then to be

tested in a relevant real life scenario and compared with alternative learning and assessment programs.

The model would be optimally supported by a custom developed software tool. Possible future studies could focus on designing the optimal usability of such a tool based on the didactical concept developed in this work.

Bibliography

[105a] ISO/IEC JTC 1. *ISO/IEC 20000-1:2005 Information technology - Service management - Part 1 - Specification*. International Organization for Standardization, 2005.

[105b] ISO/IEC JTC 1. *ISO/IEC 20000-2:2005 Information technology - Service management - Part 2 - Code of practice*. International Organization for Standardization, 2005.

[105c] ISO/IEC JTC 1. *ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements*. International Organization for Standardization, 2005.

[2705] ISO/IEC JTC 1/SC 27. *ISO-IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management*. International Organization for Standardization, 2005.

[APZ07] Alessandro, Piatti, and Zaffalon. *Credal Networks for Operational Risk*, volume 4693 of *Knowledge-Based Intelligent Information and Engineering Systems*, pages 604–611. Springer Berlin / Heidelberg, 2007.

[BH02] Biberoglu and Haddad. A survey of industrial experiences with CMM and the teaching of CMM practices. *J. Comput. Small Coll.*, 18(2):143–152, 2002.

[BMOP06] Bock, Macek, Oberdorfer, and Pumsenberger. *ITIL : Zertifizierung nach BS 15000/ISO 20000*. Galileo Press, Bonn, 1 edition, 2006.

[Brä06] Bräunig. *Konzeption und Realisierung einer webbasierten Lernumgebung für die Signal- und Mustererkennung*. PhD thesis, Technischen Universität Ilmenau, Fakultät für Elektrotechnik und Informationstechnik, 10 2006.

[Brü03] Brühwiler. *Risk-Management als Führungsaufgabe : Methoden und Prozesse der Risikobewältigung für Unternehmen, Organisationen, Produkte und Projekte.* Haupt Verlag, 2 edition, 2003.

[CJ07] Clacy and Jennings. Service Management: Driving the Future of IT. *Computer*, 40(5):98–100, May 2007.

[CMU06] Software Engineering Institute Carnegie Mellon University. Appraisal Requirements for CMMI Version 1.2. http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tr011.pdf, 08 2006. Accessed on 28.04.2009.

[COB07] *Control Objectives for Information and Related Technology.* IT Governance Institute, 4.1 edition, 2007.

[CVDV06] Cumps, Viaene, Dedene, and Vandenbulcke. An Empirical Study on Business/ICT Alignment in European Organisations. *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, 8:195–195, Jan. 2006.

[Deb06] Debreceny. Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls. *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, 8:196–196, Jan. 2006.

[DK06] Dahlberg and Kivijarvi. An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, 8:194–194, Jan. 2006.

[DT08] Dugmore and Taylor. White Paper: ITIL V3 and ISO/IEC 20000. http://www.best-management-practice.com/gempdf/ITIL_and_ISO_20000_March08.pdf, 2008. Office of Governance and Commerce(OGC) and British Standards Institution (BSI).

[Eck08] Eckhardt. Rechliche Grundlagen der IT-Sicherheit. *Datenschutz und Datensicherheit*, (5):300–336, 2008.

[EDBS05] Ebert, Dumke, Bundschuh, and Schmietendorf. *Best Practices in Software Measurement.* Springer-Verlag Berlin Heidelberg, 2005.

[EE03] Eloff and Eloff. Information security management: a new paradigm. In *SAICSIT '03: Proceedings of the 2003 annual research conference of the South African institute of computer*

scientists and information technologists on Enablement through technology, pages 130–136, , Republic of South Africa, 2003. South African Institute for Computer Scientists and Information Technologists.

[FH96] Falconer and Hodgett. A survey of strategic information systems planning in Australian companies. *Information Systems Conference of New Zealand, 1996. Proceedings*, pages 85–95, Oct 1996.

[Fle07] Fleisch. Das IT Security - ISAT Model. NLP powered IT Security Awareness Training und Management. Master's thesis, Technische Universität Wien, 10 2007.

[FSR08] Foegen, Solbach, and Raak. *Der Weg zur professionellen IT*. Springer-Verlag Berlin Heidelberg, 1 edition, 2008.

[FSUJ] Lehrstuhl für Schulpädagogik/Didaktik Friedrich-Schiller-Universität Jena. Didaktik. `http://www.didaktik.uni-jena.de/did_01/index.htm`. Accessed on 20.11.2008.

[Ger06] Gerdenitsch. Einsatz von ISO 17799 und IT-Grundschutz in kleinen und mittleren Unernehmen. Master's thesis, Technische Universität Wien, 03 2006.

[Ger08] Gerber. Information security requirements – Interpreting the legal aspects. *Computers & Security*, 27(5-6):124, 2008.

[Gmb07] Materna GmbH. IT-Service-Management Executive-Studie 2007. `http://www.materna.com/lang_de/nn_101910/DE/Presse/de/BUI/2007/MATERNA_20ver_C3_B6ffentlicht_20IT-Service-Management_20Executive-Studie_202007.html`, 09 2007.

[Gol06] Goltsche. *COBIT kompakt und verständlich*. Vieweg, 2006.

[GQDC07] Galup, Quan, Dattero, and Conger. Information technology service management: an emerging area for academic research and pedagogical development. In *SIGMIS-CPR '07: Proceedings of the 2007 ACM SIGMIS CPR conference on Computer personnel research*, pages 46–52, New York, NY, USA, 2007. ACM.

[Gre07] Greiner. ITIL: the international repository of IT wisdom. *netWorker*, 11(4):9–11, 2007.

[HBS00] Hevner, Bernt, and Studnicki. Strategic information systems planning with box structures. *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, pages 11–1, Jan. 2000.

[Hei08] Heinz. Optimierung des Business Continuity Management von klein- und Mittelunternehmen mittels ITIL V3. Master's thesis, Vienna University of Technology, 05 2008.

[HG08] De Haes and Grembergen. Analysing the Relationship between IT Governance and Business/IT Alignment Maturity. *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, pages 428–428, Jan. 2008.

[HV93] Henderson and Venkaraman. Strategic Alignment, Levearging Informations Technology for transforming Organization. *IBM Systems Journal*, 32(1), 1993.

[Ins08] Computer Security Institute. CSI Computer Crime & Security Survey 2008. `http://www.gocsi.com/forms/csi_survey.jhtml`, 2008. Accessed on 17.10.2008.

[ISA08] ISACS. ISACA Overview and History. `http://www.isaca.org/Content/NavigationMenu/About_ISACA/Overview_and_History/Overview_and_History.htm`, 08 2008. Accessed on 2008.08.30.

[IT08] Fox IT. BS15000 and ISO20000 Frequently Asked Questions (FAQs). `http://www.foxit.net/asp/Frames_Set.asp?go2=bs15000%20/%20ISO20000%20faqs`, 09 2008.

[ITI08] The ITIL Core Framework. `http://www.itil.org/osMedia/pic/22gr-the-core-framework_2142_or.jpg`, 09 2008.

[itS07] *An Introductory Overview of ITIL V3*. The UK Chapter of the IT Service Management Forums(itSMF), 1 edition, 2007.

[JPKS+98] Jarvinen, Perklen, Kaila-Stenberg, Hyvarinen, Hyytiainen, and Tornqvist. PDCA-cycle in implementing design for environment in an R&D unit of Nokia Telecommunications. *Electronics and the Environment, 1998. ISEE-1998. Proceedings of the 1998 IEEE International Symposium on*, pages 237–242, May 1998.

[Jud05] Judmaier. *Konzept und Umsetzung eines eLearning-Kurses für die berufsbegleitende Erwachsenenbildung*. PhD thesis, Technische Universität Wien, Fakultät für Informatik, Institut für Gestaltungs- und Wirkungsforschung, 2005.

[Kne06] Kneuper. *CMMI - Verbesserung von Softwareprozessen mit Capability Maturity Model Integration.* dpunkt.verkag GmbH, 2 edition, 2006.

[Köh07] Köhler. *ITIL.* Springer-Verlag Berlin Heidelberg, 2 edition, 2007.

[KRS08] Kersten, Reuter, and Schröder. *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Der Weg zur Zertifitierung.* Friedr. Vieweg & Sohn Verlag, 1 edition, 2008.

[LV95] Loh and Venkatraman. Diffusion of information technology outsourcing: influence sources and the Kodak effect. pages 292–325, 1995.

[May06] Mayrhofer. IT Governance im KMU. Master's thesis, Technische Universität Wien, Institute for software Technology and Interaktive Systems, 09 2006.

[MD07] McLaughlin and Damiano. American ITIL. In *SIGUCCS '07: Proceedings of the 35th annual ACM SIGUCCS conference on User services*, pages 251–254, New York, NY, USA, 2007. ACM.

[Mül06] Müller. *Die Bedeutung neuer Medien in der Fachdidaktik für den Unterrichtsgegenstand Darstellende Geometrie.* PhD thesis, Technische Universität Wien, Fakultät für Mathematik und Geoinformation, Institut für Diskrete Mathematik und Geometrie, 12 2006.

[Nab03] Naber. *e-ULE - e-usable learning environment.* PhD thesis, Technischen Universität Wien, Fakultät für Technische Naturwissenschaften und Informatik, Institut für Rechnergestützte Automation, 06 2003.

[oBS04] Basel Committee on Banking Supervision. Basel II - International Convergence of Capital Measurement and Capital Standards. Technical report, Bank for International Settlements, 2004.

[OEC04] OECD. OECD Principles of corporate Governance. Technical report, Organisation for Economic Co-operation and Development(OECD), 2004.

[OEC06] OECD. Corporate Governance of Non-Listed companies in emerging markets. Technical report, Organisation for Economic Co-operation and Development(OECD), 2006.

[oGC07a] Office of Governance and Commerce. *Continual Service Improvement*. ITIL V3. TSO (The Stationaty Office), 1 edition, 2007.

[oGC07b] Office of Governance and Commerce. *Service Design*. ITIL V3. TSO (The Stationaty Office), 1 edition, 2007.

[oGC07c] Office of Governance and Commerce. *Service Operation*. ITIL V3. TSO (The Stationaty Office), 1 edition, 2007.

[oGC07d] Office of Governance and Commerce. *Service Strategy*. ITIL V3. TSO (The Stationaty Office), 1 edition, 2007.

[oGC07e] Office of Governmence and Commerce. *Service Transition*. ITIL V3. TSO (The Stationaty Office), 1 edition, 2007.

[oGC07f] Office of Government and Commerece. *The Official Introduction to the ITIL Service Lifecycle*. ITIL V3. TSO (The Stationaty Office), 1 edition, 2007.

[oGCU05] IT Governance Institute. Office of Government Commerce UK. Aligning COBIT, ITIL and ISO 17799 for business benefit: management summary. 2005.

[Pop07] Popp. IT-Governance Modelle. Master's thesis, Vienna University of Technology, 10 2007.

[Pre08] Prein. Didaktische Entwürfe zum Pflichtgegenstand Angewandte Programmierung des ersten Jahrganges einer HTL für Informationstechnologie. Master's thesis, Technische Universität Wien, 08 2008.

[Pri06] PricewaterhouseCoopers. *IT Governance Global Status Report - 2006*. IT Governance Institute, 2006.

[PWCC95] Paulk, Weber, Curtis, and Chrissis. *The Capability Maturity Model: Guidelines for Improving the Software Process*. Software Engineering Institute, Carnegie Mellon University, Addison Wesley Longman, Inc., SEI series in software emgineering, 11 edition, 1995.

[RSG06] Rüter, Schröder, and Göldner. *IT-Governance in der Praxis*. Springer-Verlag Berlin Heidelbarg, 2006.

[RW04] Ross and Weill. Recipes for Good Governance. *CIO: Australia's Magazine for Information Executives*, 12 July, 2004.

[RYC04] Ridley, Young, and Carroll. COBIT and its utilization: a framework from the literature. *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, page 8, Jan. 2004.

[SE06] Simonsson and Ekstedt. Getting the Priorities Right: Literature vs Practice on IT Governance. *Technology Management for the Global Future, 2006. PICMET 2006*, 1:18–26, July 2006.

[SEI07] Carnegie Mellon University Software Engineering Institute. Capability Maturity Model Integration (CMMI) Version 1.2 Overview. `http://www.sei.cmu.edu/cmmi/adoption/pdf/cmmi-overview07.pdf`, 2007.

[SJW07] Simonsson, Johnson, and Wijkström. Model-based IT Governance maturity assessments with Cobit. In *European Conference on Information Systems*, jun 2007.

[SSA08] Sahibudin, Sharifi, and Ayat. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, pages 749–753, May 2008.

[Sur05] Sury. IT-Governance. *Informatik-Spektrum*, 28(1):69, 2005.

[SVFMP06] Sanchez, Villafranca, Fernandez-Medina, and Piattini. Practical approach of a secure management system based on ISO/IEC 17799. *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, page 8, April 2006.

[Sys07] Gamma Secure Systems. History of 27000. `http://www.gammassl.co.uk/bs7799/history.html`, 06 2007. Accessed on 17.10.2008.

[SZ99] Sambamurthy and Zmud. Arrangements for information technology governance: a theory of multiple contingencies. *MIS Q.*, 23(2):261–290, 1999.

[SZ07] Sen and Zheng. The Relation of CMM and Software Lifecycle Model. *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on*, 3:864–869, 30 2007-Aug. 1 2007.

[SZ08] Stych and Zeppenfeld. *ITIL*. Informatik im Fokus. Springer-Verlag Berlin Heidelberg, 1 edition, 2008.

[SZK08] Spremic, Zmirak, and Kraljevic. IT and business process performance management: Case study of ITIL implementation in finance service industry. *Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on*, pages 243–250, June 2008.

[Tat08] Tat. Analyse der Erreichbarkeit von Capability Maturity Model Integration Levels in Extrem Programming. Master's thesis, Technische Universität Wien, 02 2008.

[Tho04] Thornburgh. Social engineering: the "Dark Art". In *InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development*, pages 133–135, New York, NY, USA, 2004. ACM.

[TK05] Tjoa and Karagiannis. IT Governance Definition, Standards & Zertifizierung. *Österreichische Computer-Gesellschaft: OCG-Journal*, 30(4):18–19, 2005.

[Tur08] Turbitt. *White Paper, ISO 20000: What's an organization to Do?* www.techrepublic.com, 2008.

[Uni06a] Carnegie Mellon University. CMMI for Services: Initial Draft. `https://bscw.sei.cmu.edu/pub/bscw.cgi/d537712/CMMI-SVC%20baseline%20for%20review%20v0.5c.doc`, 09 2006. Accessed on 29.09.2008.

[Uni06b] CMMI Product Team Carnegie Mellon University. CMMI for Development, Version 1.2. `http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tr008.pdf`, 08 2006. Accessed on 27.09.2008.

[Uni07] CMMI Product Team Carnegie Mellon University. CMMI for Acquisition, Version 1.2. `http://www.sei.cmu.edu/pub/documents/07.reports/07tr017.pdf`, 11 2007. Accessed on 27.09.2008.

[Uni08] Software Engineering Institute Carnegie Mellon University. Sunset of the Software Acquisition Capability Maturity Model (SA-CMM). `http://www.sei.cmu.edu/cmmi/models/SA-CMM-sunset-announce.html`, 02 2008. Accessed on 27.09.2008.

[Var07] Varol. Evaluation von E-Learning-Systemen am Beispiel des Kurses Ecodesign. Master's thesis, Technische Universität Wien, 03 2007.

[Von05] Vonsolms. Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2):99, 2005.

[Wec07] Weck. Messbare IT-Security. *DuD - Datenschutz und Datensicherheit*, (31):84–86, 2007.

[Wol06] Wolf. IT-Governance mit ITIL, CObIT und der Balance Scorecard. Master's thesis, Hochschule Niederrhein, 2006.

[WPR06] Webb, Pollard, and Ridley. Attempting to Define IT Governance: Wisdom or Folly? *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, 8:194–194, Jan. 2006.

[WS06] Johannes Kepler Universität Linz Werner Stangl, Institut für Pädagogik und Psychologie. Psychologische Begriffsbestimmungen, Didaktik. `http://www.stangl.eu/psychologie/definition/Didaktik.shtml`, 08 2006. Accessed on 20.11.2008.

[You07] Ernst & Young. 10th Global Information Security Survey. 2007.