Positioning the roles, interfaces and processes in the information security scene.

Dimitrios Papadopoulos

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2013

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Positioning the roles, interfaces and processes in the information security scene.

Dimitrios Papadopoulos

2013/06/02

Keywords

Information Security Management, Information Security Governance, Organizational structure, Information Security in a company's environment. Information security procedures, Roles and Responsibilities.

Abstract

All information security professionals around the globe acknowledge that "everyone is responsible for information security" in a company. This trivial statement looks clever but hides core challenges, "Who is everyone? How does everyone contribute or challenge information security?" In our researched project we researched in-depth roles, processes and interaction in the corporate information security, by creating a framework for crystal clear defined roles and its associated security obligations and responsibilities. 20 corporate roles are analysed from management and security perspective; classical interactions between information security roles leveraging and turning down security are given in case studies. Furthermore we generated structured tasks descriptions of the roles and open the road to the fulfilment of an information security consultants dream by creating Job descriptions including its security responsibilities! We justified the necessity of defining roles and by introducing benefits of this approach:

1. Avoiding unnecessary conflicts and internal politics by establishing security organization with inclusion of all employee's duties.
2. Increasing security-level, efficiency and productivity by assigning clearly responsibilities.
3. Achieving good information security governance by encouraging coordinated team effort and mutual control.

Illustrative corporate examples demonstrate the need to supplement traditional corporate information security governance frameworks with roles and responsibilities for all positions. Templates for both security obligations and task description are provided for being used in corporations.

Acknowledgements

"***One man may hit the mark, another blunder; but heed not these distinctions. Only from the alliance of the one, working with and through the other, are great things born.***" [1]

This master thesis is the culmination of a long studying path started in the beginning of my B.Sc. in Greece and ending today in Norway. Many people contributed either directly or indirectly in my journey to my Master's degree. I thank and remember all of them.

Foremost, I express my sincere gratitude to my advisor, Professor Dr. Bernhard M. Hämmerli for his patience motivation, enthusiasm, support and continuous guidance through the research and writing of this thesis. I could not have imagined having a better advisor and mentor during my master studies. With his great contribution to the development of this thesis, as well as myself personally, with the valuable insight, advice and life experience he shared and coached me through my studies, first to become a better man and a good professional.

Besides my advisor, I would like to thank Professor Stewart Kowalski and Professor Siv Hilde Houmb for their encouragement, insightful comments and hard questions which improved the quality of this dissertation.

My sincere thanks also goes to my collogues for the stimulating discussions and support during the writing of this thesis, as well as for the sleepless nights we were working together before deadlines and for all the fun we have had in the last two years of my studies.

I would also like to take the time to thank my close friends that life spread around the globe for their spiritual support and friendship during all this years of my life. Special thanks to one of them, Savvas Bellis, for his valuable contribution of proofreading this thesis as a native English speaker.

Last but not least I would like to thank my family for their support, guidance and my character shaping during my life journey.

Dimitrios Papadopoulos

[1] Antoine de Saint-Exupery

Copyright

Contents

List of Figures

List of Tables

1 Introduction

In the beginning of this thesis we would like to quote a phrase from Paulo Coelho.[1] In an interview a reporter asked him whether he could describe the aim of his book in one sentence. "If I could do that, there is no need for me to write a whole book." Thus said, the results of this thesis can't be expressed in one sentence without entirely describing the thesis itself.

During the last decade the rapid advance of Information technology created a solid need for information security. Thus, made information security a priority and an area of significant importance for companies around the globe. Information security became a part of the business innovation process. That happened due to the fact that the information scene realised that security is way more than security controls but rather personnel management and employee behaviour and culture. In fact, a study regarding information security conducted by AT&T [1] showed that an estimate of 30% associates with technology and 70% with people and security practices. This is also something that was confirmed by a foreign high ranking government security officer who described the government security policy, where the basic principals as followed: " *a) organizational security measures regarding the roles and responsibilities of staff and any external partners processing, the definition and responsibilities of the security officer, training staff, managing security incidents and the destruction of personal data b) the technical security measures regarding the management of the users of the information system, the identification and authentication of users, the communications security, the security of the operation logs and the security of the exported backup, c) physical security measures.* " Also, the security policy should clearly define the roles of each stakeholder in the company or organization, powers, responsibilities and duties as to the procedures relating to security.
Thus said, it is rhetorical to ask whether you find roles and responsibilities a matter of importance in the information Security Theatre? [2]
In our research we identified the most significant roles inside a company and performed an analysis over them resulting to their responsibilities, tasks and daily activities as well as proposing the security culture those roles have to inherit on the road to a good security governance.

[1] Paulo Coelho born on August 24, 1947 is a Brazilian lyricist and novelist. He has become one of the most widely read authors in the world today. He is the recipient of numerous prestigious international awards, amongst them the Crystal Award by the World Economic Forum and France's Legion d'honneur.

[2] 'Security Theatre' was a term coined by Bruce Scheiner in his book Beyond Fear and basically describes a situation, where a security countermeasure offers little or no protection from a real threat, but is simply applied in order to increase the feeling of being secure. However, this approach is often being used by organisations in an attempt to secure corporate information assets.

1.1 Report Outline

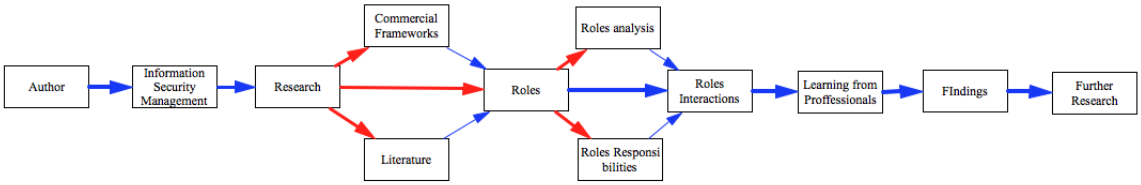


Figure 1: **Visual Report Outline and Research Structure**

1.2 Information Security

We believe that before going any further and also to conduct research, it is wise to define what information security means actually. Since it's common knowledge to us that most of the people have a misconception of the term information security and always relate it to either a) the protection of electronic data or b) computer security. Hence, even though there are many different definitions of information security available we selected two of them which we believe will give you a clear understanding of what actually is information security and clear any doubts you might have regarding the term. In addition to the textual definitions you can see in figure 2 the visual representation of information security.

1. Information Security is a discipline governing the framework for the continuous cycle of safeguarding information and ensuring related regulatory compliance.[2]
   Where:
   - Discipline is a branch of instruction and learning such as history, finance, and economics.
   - Framework is a frame or structure composed of parts fitted together documenting the methodology of incident identification, mitigation, and resolution much like the scientific method.
   - Cycle is a series of processes that are repeated in a precise and deliberate manner.
   - Information is electronic, printed, audible, visual, memorized.
   - Compliance is ensuring that the institution is in compliance with applicable laws, regulations, and contractual agreements.

2. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [3]
   where:
   -integrity, means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
   -confidentiality, means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
   -availability, means ensuring timely and reliable access to and use of information.

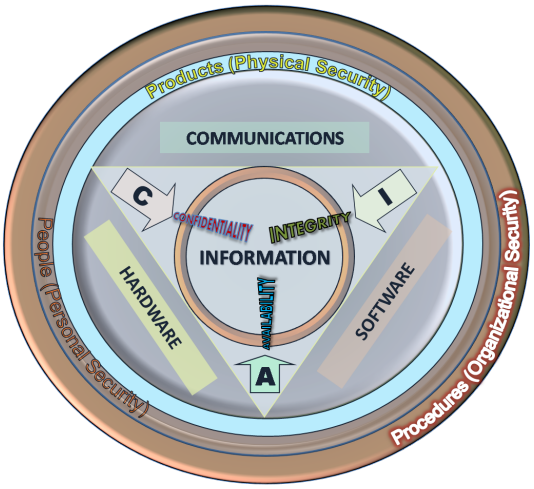


Figure 2: **Visual representation of Information Security**

1.3 Research Problem, motivation and aim

Before we discuss the research problem we would like to tell a short story behind the idea of this thesis. The preliminary thoughts the author had on the thesis started in the first weeks of his presence in the information security master's program at GUC. Back then we had to choose a track for our studies. Hence to choose a career path. That is where the author first met Prof. Hämmerli, in a discussion we had he analysed and explained the scope of tracks and career paths. The authors interests lie in management and luckily for him Prof. Hämmerli specialises in this field among others. The author chose his track and got from the professor some master thesis proposals for that year just to take a taste of what lies ahead. We agreed with the professor to come back to this when the time was right. The time came and a year passed of the authors study. At that time being, the author realised both the career path he wants to follow and the things he is most interested in. Thus, no secret, he is to become an information security management consultant and hence his interests lie on the management field. Now it was the question to combine the author's interests and knowledge with a topic derived from management that would serve a double purpose. Firstly, lead his path to graduation and secondly to coach him and provide valuable insight from the consulting world. We spent a lot of time discussing various proposals and topics. It was a very hard and time consuming process since it had to satisfy many factors. The university, the professor and the author. In the lecture of organisational and human aspects conducted by Prof. Hämmerli in GUC he taught us that everyone in a company is responsible for security. And that there is a need that all the stakeholders of a company acknowledge and follow it in their companies. However, from the authors life experience he knew that, it wasn't followed, at the companies he once worked at. Therefore, he had a discussion with the professor stating that it is usually the case that companies nowadays have a tendency to associate their information security with the information security officer. He is considered

responsible for the overall information security of the company. This approach generates problems between departments inside a company since everyone believes that security is just the responsibility of the CISO and his department and therefore they neglect its concern as something that is not of their interest. But the CISO and his department aren't magicians and don't have a magic stick that will solve all the security threats and this is something that they cant accomplish on their own. That discussion generated the idea for the author to investigate and identify literature that would analyse all the involved stakeholders and their role in information security. He was surprised to find that very little is done in this area; you will read more about this in the literature overview in a following section. Hence, we discussed this issue with the professor and this is how we got to the topic of this thesis "Positioning the roles, interfaces and processes in the information security scene." A topic that comes to investigate the live field of information security. Identifying the stakeholders that are involved with information security within a company's environment and placing them in the information security scene of a company defining their responsibilities towards information security as well as the responsibilities of information security towards them. We provide examples on how a security office runs in a company; How information security management should be conducted; How various roles benefit and contribute to information security; As well as fulfilling an information security consultants dream by summarizing the security responsibilities and generating job descriptions with them attached. This is a hot topic for research and a base for future scientific work and reference. The dual nature of the analysis of roles with the purpose to provide a holistic overview of a role serves both educational and industrial purposes. A general reader of this thesis will not only learn about information security but will get an overview of concepts such as organisational structure, company's governance and stakeholders. He will have a modern view of the roles and how they contribute to a company. While at the same time he will familiarise himself with many different aspects of information security and how it protects, develops and drives forward a company. An academic reader of this thesis will get a valuable insight on how information security is interpreted and applied in the industrial market seeing the difference between theory and practice. A professional can use it as a map and use the findings for consulting purposes and brighten his horizons on the topics covered by this thesis. As for how it benefits the author on a personal level. He wouldn't expect a better topic for research to serve his purpose to familiarise himself with the industrial world and the way it places and interprets information security. By conducting this thesis the author gained a huge amount of knowledge both from an information security perspective and a management perspective that will serve as a great tool-kit in his career as an information security professional. With this thesis we opened Pandora's box on an area that clearly lacks research. Thus, of roles and responsibilities. It is essential for companies to understand that everyone within a company is responsible for information security. There can't and shouldn't be only one person to blame if something goes wrong. Security is an overall process and everyone, one way or another, has to contribute in order to make it work. Any control measures can collapse in seconds if people don't understand that they also play a role in the information scene. These roles and their responsibilities is something that we want to make crystal clear and easily understandable. We raised a hot topic for research and covered it as much as we could. However, we expect others to follow our example and take it to a higher level with more resources and workforce.

1.4 Research Objectives

As already defined, our study is about the roles & responsibilities and we aim to achieve the following:

1. Provide roles global definition.
2. Provide roles analysis from a management perspective.
3. Provide roles analysis from a security perspective.
4. Generate the overall Roles responsibilities.
5. Propose some generalized job description's of roles.

Furthermore, present typical use cases/scenarios of those role interaction.
Finally, the goal is to provide to you (the reader) a solid, state of the art, overview of security organizations, and the roles, interfaces and processes of it.

1.5 Research Methodology and Limitations

This thesis is about roles, responsibilities and their interactions in the information security scene of a company. The first question that derives is where do the roles we analyse come from and which is the method of their selection? Before we give a clear answer to this question we have to discuss about an organizational structure. There are many different ways to look at an organization. There is the socio-technical approach and the psychological approach. In other words there is the organisational structure and organizational behaviour. Information security management inherits many characteristics from both concepts and is placed somewhere in the middle. Since our research is an industrial study of how information security looks like in the live field of industry we had to analyse and see how companies are structured. However due to the limitations in resources and the many millions of companies, conducting such a survey to derive statistical data and to see how organizations are structured and how information security is in them was unrealistic for us. Therefore we used a different approach. That of a naïve inductivist where we use primary and secondary data to observe the real industry and create generalisations. A visualised representation of this approach is listed in figure 17 (page 39). Our primary data came from discussions with professors that are actively involved with the industry and interviews with people from the industry. We used a case study of a gas and oil company which shared with us its organizational structure where we could observe and derive some roles for our research. In addition we use secondary data such as interviews, surveys, job descriptions, consulting papers, information security frameworks/standards and industrial analysis conducted by others to finalize the last piece of the puzzle. The same methodology applies also to the analysis of the roles. Another challenge of the research methodology and validity comes from a socio technical analysis of a company where the question is how do we compare the roles we identified in different companies. Since in a Small-medium enterprise (SME) company the role of the CEO for instance is totally different than in a large company. Therefore, for the reason of resources as well as other factors you will read about it in the eyes of industry section of the thesis, we acknowledge this obstacle and study the roles with the perspective of large companies which have more then 1500 employees and a comparison of roles is doable. Another major limitation of this thesis is that we cant provide accurate description about

the interactions of the roles with respect to authority (meaning the person who has the budget), the responsibility and the competence. Thus, because in every company depending on the persons and its structure these three factors are distributed differently. However, we provide our analysis estimating that they cover a portion of companies in the industry. The same approach is used in the scenarios and use cases we developed. We would like to also acknowledge that we understand how scientific research is conducted by generating a hypothesis and trying to prove it wrong or right. However, management, hence information security management in our understanding is more an art then science. And in fact, management came from industry and the scientific community spent decades analysing it due to its attractive and appealing nature. The nature of our study is an industrial research based on scientific principles as they where taught in the scientific methodology course of Gjovik University College.

1.6 Literature Overview

Nowadays, there are long and drastic discussions held over the subject: " Should security be part of the business process ?" The experts answer to that with a well defined yes [4]. In the digitized ear of computer processes and remarkable technological advantages, security investments should have a direct line to business priorities and building security into business innovation processes drives bottom line results.[4] Security strategies and practices now have the power to make or break business goals. [4] A lot of people fail to realise that security is not a single process and that a security officer is not a policeman chasing bad guys. Security is a matter that concerns everyone within a company, starting from the cleaning crew ending at the CEO of the company. Everyone is responsible for security. [5] Organizations are facing various threats to information security and try to deal with them using various ways. In this processes of defending themselves they have to meet different legal and regulatory requirements. The lack of security compliance will lead to serious problems for the organisation, starting with profit loss ending into criminal charges at the top management. We are living in a digitised world and therefore things as availability, integrity, confidentiality as well as regulation compliance are essential for every company. There are various ways to achieve these requirements. A lot of companies are implementing an ISMS, Information Security Management System, in order to achieve there business goals and comply with legal aspects. Such ISMS systems are frequently deployed according to the ISO/IEC [6] and we have encountered the three most popular ones during our studies which are COBIT [7], ITIL [8] and NIST [9]. But why are we writing the above information how is it relevant to our topic? Information Security management, [10] business management and on the other hand software security and network security engineering have been handled for a longer period as separate areas. In the security process of a company there are many different stakeholders involved and each one of them has his role to play and contribution to make in the overall security. Thus, the involvement of many different people derives a problem of responsibilities. It is axiomatic [11] that those things for which no one is explicitly accountable are often ignored. Therefore we need to have different roles and responsibilities assigned to everyone involved. There will be people responsible and someone to take the blame in case something goes wrong and an incident happens. A thing we learned is that the higher management prefers to have a persons "beheaded" rather than statistics or unclear situations. In addition, an important thing of having responsibilities and roles assigned is

a key factor in successful governance. There are a variety of approaches that these roles are described and categorised in different related works [6], [7], [9] one conclusion that we can derive from all those different frameworks is that management has to identify clear roles and assign responsibilities for the protection of assets and for all security processes and controls.
The purpose of this chapter is to give to the reader a small overview on what is already researched by the literature and what our contribution will be. There are a lot of ways to approach roles and responsibilities some of the roles are really well defined and analysed already such as the CIO, CEO and the Audit Investigators but as you will find out in the next chapters that there are many roles for us to explore, specify and analyse. At the current point, it is sufficient to say that we have a clear picture of different roles functioning inside of a company, out of which some are defined by the literature and others coming from the commercial sector.
The second and major part of our research is how all these different stakeholders (people involved) interact regarding information security. This is a field not explored in detail, however there is a certain point of literature but specified on customised study cases. This domain is something that we are looking forward to explore ourselves based on our gained knowledge from our studies and different work environments over the years combining those two parameters and adding the interviews of the experts in the field, we believe we will have the appropriate materials to derive good and solid findings. For the last part regarding the use cases and scenarios the situation is more likely the same as with the roles, some use cases are undefined and others well defined, for instance a case study of information audit which is a well defined process and there is plenty of literature available on this aspect, one of the most interesting is the Auditor's Guide to Information Systems Auditing [12] but our purpose is not to investigate the internal audit process but rather how a finding of this process is communicated within an organisation and how it affects the different stakeholders and the security of the enterprise. Thus, also the purpose of all the use cases and scenarios we are about to use in this thesis. This interaction is something we will have to investigate and search since the literature only provides the usual steps of this process but not the affects of each step of the communication plan towards security.

2 Roles

2.1 Introduction

The previous chapters have given an overview of what is to come in this thesis. As we clearly stated a huge part of this thesis is about roles and their responsibilities. But before we can proceed any further we have to understand and identify those roles and their origin. Unfortunately in the available literature and most noted such as ISO/IEC [6], COBIT [7], ITIL [8], NIST [9] and CISSP [13] clear definitions of roles and responsibilities are not available but rather a generalized approach is taken in some of them. Thus, lead the author to apply the inverse innovation model [1] where the lack of academic literature in the area of applied corporate information security is covered by the business industry which is far more developed then the academia. The author turning to the industrial market realised that there is plenty of information available but this information doesn't come cheap and there are many "obstacles" for the author to face in order to obtain it, but we will come back to this at a later stage. Now it is time to go back to the start and our primary concern which is the roles and the responsibilities that come with them. In the industrial market big companies (defined for us as companies that employee 1500+ employees) but also small and medium companies usually use a hierarchical model of governance where clear roles are defined and a chain of command is developed and structured. Such kind of governance is conducted with the help of organizational charts. Where the chain of command, the infrastructure and as well as the operations and process of a company are shown. Thus, something that the author knows from his working experience and in order to give the reader a clear view of how this scene is set up and of course clearly show where the different roles that we will analyse, in later section, come from making the task of obtaining such organizational charts a priority and a necessity for this thesis. Realizing that at this point the author began his quest to obtain such documents. We refer to this as a quest since at first look it appears to be "a piece of cake" to obtain such a simple document but when it comes to industry, things are unpredictable and this task became a mission impossible but yet accomplished by the author. In this process we interacted with various industrial giants and the answer we had to face was always the same "We apologise but such information is classified and available for internal use only". Many of you would raise a question: "why is that information regarded as classified?" which is totally justified thing to ask. Therefore, we recall an off the record conversation of the author with a C.O.O. [2](Chief Operating Officer) of a well known security company where he said: " In the era of vast technological development, the era of industrial espionage and competitors where companies would do anything to increase revenue, a disclosure of key personal in key positions would pose an immediate threat for any company. Since if one is to cause damage to a company he would try to compromise the people in high positions. Therefore, such information is classified and sensitive." We were surprised to hear such a statement, but yet come to realise that he is absolutely

[1]The term is proposed by Prof.Dr. Bernhard M. Hämmerli to describe the phenomenon
[2]The credentials of this person will remain unknown since the conversation was off the record

correct and furthermore history proved this to us in various occasions during the years. In all the great wars the strategy was the same to eliminate the opponents commanders since an army without a commander is not an army that can stand in battle. We recall a documentary film "The battle for Stalingrad" where in the famous battle of Stalingrad the elite brigade of Russian snipers was instructed to eliminate only commanding officers of the German Army. History always teaches us good lessons and even though we aren't in a war condition/situation with the literature meaning of the word there is an ongoing technological war of industrial espionage between many companies. And unfortunately for us, we are in the middle of it trying to collect useful information for our research which in most occasions is classified and sensitive. In such a situation a lot of people would recall the golden rule of the three F's [3] where F's stand for family, friends and so called "fools" who would reveal classified information and become ones sources. Although at some point this approach might have a dose of reality the situation is a bit better in the industry but yet more pragmatic. The industry is willing to cooperate with "researchers" but under their own conditions. Those conditions are specified and are as follow: The author is responsible to anonymize and sanitise the information he obtains in such way that it will be impossible for one to trace back to its origin before he is allowed to put such information in written form in the thesis. Thus, might not look very academic to many of you but that is the way things are done when it comes to actual research in the industrial market. The phenomenon of inverse innovation model is letting the author with limited choices, to accept the conditions posed to him by the industrial market experts. At this point you probably understand why we called it a quest in the first place and why most of the obtained information which is yet to come into the thesis will be a quest of itself. A quest which was successfully accomplished by obtaining the organizational charts of a globally known oil and gas company to serve our purpose and help us proceed with our research.

2.2 Organizational Charts

Finally we have them! But what makes them that important and us so happy to have them in our hands? Although a small answer to this question is given in the above section we haven't yet revealed the true power of such documents. In today's modern world if we attend a company's presentation the first thing they will show us is an organigram which is the general model of a company most people would recognise it as a picture with hierarchical lines which show the structure of the company and the departments that it has. The structure is one of the most important things when it comes to a company. [14] It defines the effectiveness and the efficiency of the company. The structure is defined as a set of rules on how a company operates. [15] It defines the responsibilities and the powers within the company.

[3] A "joke" but yet reality told to the author by Prof.Dr. Bernhard M. Hämmerli

In terms of questions [14] a structure defines:

1. "*who did that?*"

2. "*who gets the blame?*"

3. "*who is accountable for that*"

Furthermore a structure is a set of relations between the roles of a company [14]. There is ongoing research in this area such as [14], [15], which shows the benefits of organizational structures but we won't go deeper into it but rather pinpoint you to those papers if you find this topic interesting. We believe that you have already shaped a clear view and understanding of what an organizational structure is and does and it is time that we present you our organizational charts which show the organizational structure of the oil and gas company that we from now on will refer as company A.

2.2.1 Overall Organizational Chart

Analysing an organizational chart is not an easy process but rather a whole science itself. We will give an brief analysis of the organizational charts we obtain from the industrial company but before we proceed on that we would like to dive a bit deeper in the security perspective of the charts. Having an organisational chart in hand you can easily paralyse a companies business since you can attack/recruit the key personal of a company. A simple example of such a situation can be a bidding auction where an attacker can recruit a person with the relative information about the companies bid and by knowing that they can outbid that company which in terms of money could be for instance a contract of a potential worth of a 100 million $. Thus, the attacked company loses the opportunity to win that amount of money which is most likely to be a huge loss for them. Hence you understand how important such a document can be. But who and how such a chart is developed? In the industrial market the common policy in developing such documents is conducted by the stakeholders or the executive board members. Where actually they agree on the distribution of responsibilities. There are various of forms of how such a structure is formed and there are many factors that play a role in this process, but it is not a topic for analysis in this current thesis. What is of our interest is to see how such a chart would be developed from a security perspective and how a security chart is developed. Thus, how the security responsibilities are distributed within a company. In a discussion with Prof. Siv Hilde Houmb we generated an opinion presented in figure 3 where you can see the roles which have to interact and communicate in order to achieve an excellent security governance. This figure illustrates the ideal occasion, assuming that the company would allocate a lot of resources towards security in order to have the best possible security infrastructure and where security poses as a priority and a must for the company.

Thus of course is the ideal solution but according to various security experts in the real industry things are somewhat different but close to this basis. We will describe in a more detailed way these interactions and roles later on in the security chart analysis and roles descriptions.

Figure 3: **Ideal Security Infrastructure developers**

In figure 4 you can see the overall infrastructure of company A. Looking at this chart we can see the various departments and role distributions. Nowadays, people believe that security is just an IT function but as you can see in the organizational chart, security has its own department since the role of the CISO (Chief information Security Officer) or how it is stated in the current diagram as Security Manager shows that it is an independent process of the company and not under the information management which is the IT department of the company. We can see that the security department is connected to the commercial department that is because the physical security is being outsourced to other companies but more about that in the detailed security section. We can see the direct connection of the Security department with the Managing Director or also known as the CEO of the company which is then connected with the rest of the departments of the company. We can also see that various roles such as the Legal department, the operations department and so on, most of these important roles will be identified and analysed in detail in the next sections of this thesis. The organizational chart will be used as a map to navigate between the roles and it will serve as a visualisation of the roles and their interaction.

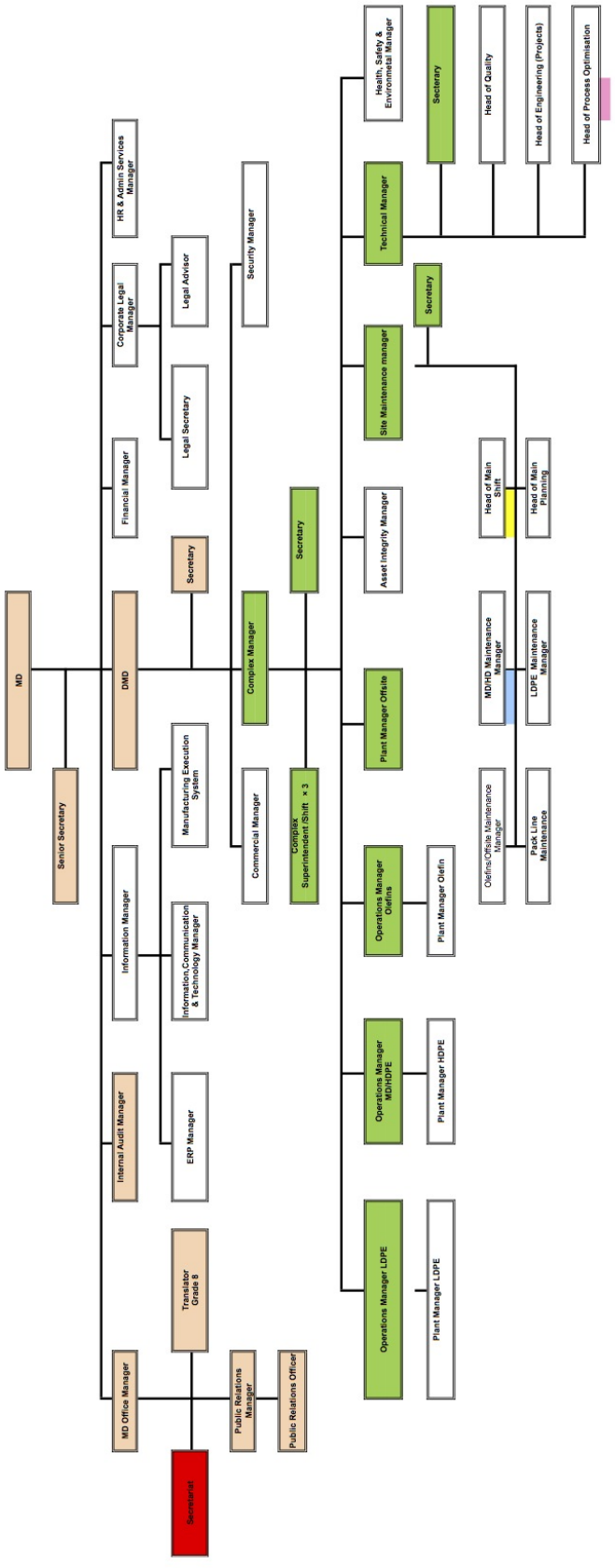


Figure 4: **Overall Organizational Chart of Company A**

2.2.2 IT Organizational Chart

In figure 5 you can see the IT chart. By reviewing this chart we can understand that the CIO (Chief Information Officer) also known as Information Manager also identified like that in this chart is more of a Technical person since the ICT (Information and Communication Technology) officer is below him which in different companies can be found at the same level as the information officer. The information manager is responsible for the information that flows inside and outside of the company. The information manager looks at information as an asset. He has to define what is classified, what is internal, what is external and how all this information is treated. He has to concentrate on the information inside the documents. He is responsible for the different information systems that the company uses. Another interesting thing that we can identify by viewing this IT chart is that a lot of processes of the IT department are outsourced to third party companies, you can see those functions that are outsourced are marked as red boxes. In addition we can see that they have an expert in security and risk management in the IT department that is the person who will perform the risk assessments of the information tools. If we go back to figure 4 we can see that the Information Management is also responsible for ERP Management, the ICT and the Manufacturing Execution System. In other words the IT department is responsible for every section that uses IT technology. Thus, something that is affiliated directly with the security and the security department. Therefore it is time to see what is going on in the security office and how these two departments interact.

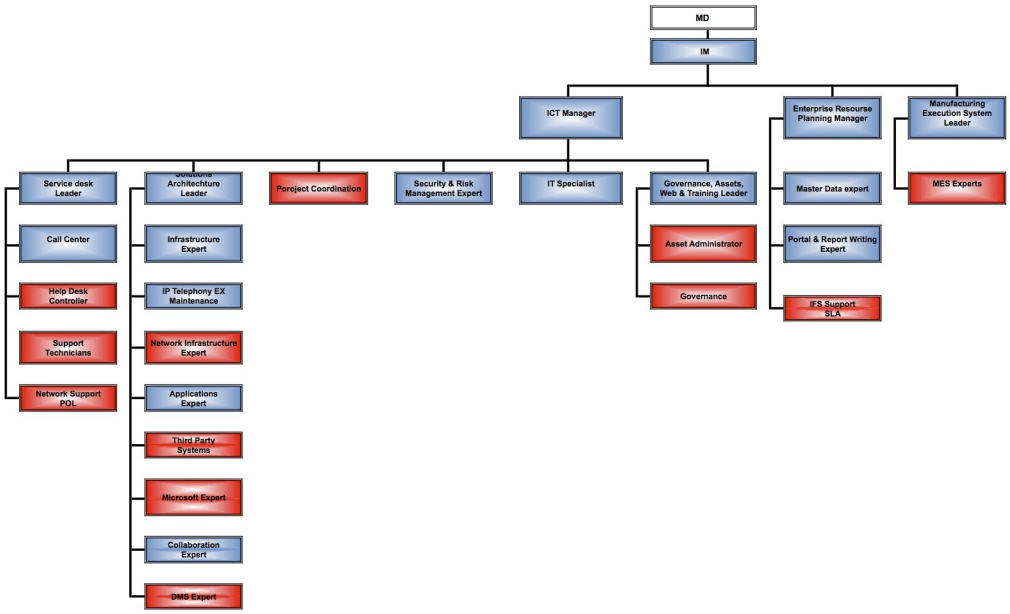


Figure 5: **IT Department Infrastructure**

2.2.3 Security Organizational Chart

In figure 6 you can see the Security Department infrastructure. As we already mentioned

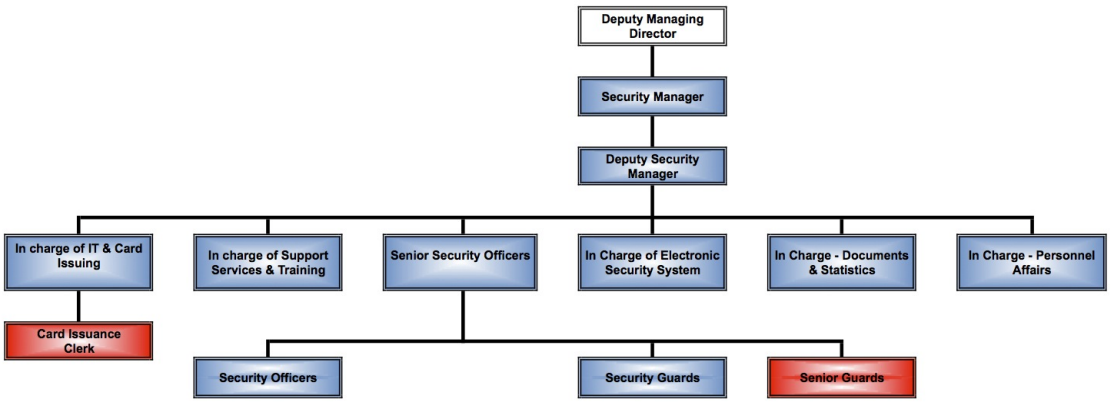


Figure 6: **Security Department Infrastructure**

security is regarded as an IT function but that is fiction that belongs to history. In modern industry security is understood as a process, a journey and not a destination[16]. In security there is not and there will never be a point that we can say "we have arrived and there is nothing else to do " [16] perfect security is just a vision of the academia and a pure theory which in practice never can be achieved that is what industry proves us. Security is a continuous improvement process. Security is not just the electronic part and the IT systems it is the way we treat everything starting with documents ending with APIS. Information is just the asset that we want to protect and security is just a sub part of this process. The security manager also known as CISO is responsible for a security attack or a security event that takes place or if somebody does something that should be covered by the security policy. His tools are the security policies but not just the ICT policies but everything related to the information using technical or procedural means. The security officer doesn't care about the information itself but the way to protect it using access controls mechanisms and various other techniques available to him. His role is to implement the local security policies. If we take a closer look at the chart we can see that the above described procedures are identified in the chart. In addition we can see that the CISO is responsible for the awareness campaigns and the training of the staff about security procedures. It is also easy to understand that he (in the terms of he actually reflects the whole department) is responsible for the physical security of the company as well as the background checks and the security clearance of the potential employees identified by the Human Resources department. Also we can see that he is responsible for the technical security and also the overall implementation of security measures. There are many different structures and responsibilities of departments varying from company to company the structure of each department could be different. The described above responsibilities are specific for this department's structure but nevertheless is somewhat similar in other big companies. We have briefly described these organizational charts but what we find of most interest is to describe the interaction of security and IT within a company and how do other departments interact with them.

2.2.4 Interactions

In the previous sections we describe the charts but now it is time to take a glance on how all this is combined. In company A and also in many various other companies in the industrial market you will usually find four people cooperating when it comes to security. These are the CEO, CISO, CIO and the CHRO where of course the final call goes to the CEO. These roles with addition of the CLO need to collaborate in order to cover all the information security aspects. The CISO and the CIO are the people responsible for the control of information and how to protect it. Thus, exposing their job stability and defines their job as a risky one. Thus, because these two people interact with the CEO of the company and are dependant on each other for an effective security governance. Usually the CIO and CISO are the people to take the blame if a security incident occurs but it is the CEO who has to go out there and face the media and take the blame on behalf of the company. A well known example is the Saudi Arabian oil company where a security incident took down the system for 11 days. As a result both the CIO and CISO where fired since somebody has to take the blame and of course the CEO is also out of favour because of the loss of the money, but the stakeholders usually wont fire all three since then they will remain without anyone in the chain of command therefore the CEO will fire the other two to save his position. There is a famous joke that is known to the security community where both the CISO and the CEO are going to the bathroom but they never meet. There is a big sense of truth in this joke since the CEO is occupied with so many responsibilities and burdens to carry, but more to that in the CEO analysis later on, that he cant interact with every single problem that the CISO will come up with every-time he meets him. Since the CISO will always have a different problem to address too. Nevertheless, in the real industry people in those three departments build a mutual trust relationship and the CEO places his trust to the CISO and CIO to run the business smoothly, usually in the cases of emergencies where decisions must be taken fast and effectively. The CIO and CISO are people with authority and the relationship between them is something that affects every system in the company. They have to communicate, respect and trust each other. On the other hand problems, will occur and it is most likely that the one causing them will have to face the consequences. It is very hard to speak of different affiliations and the distribution of responsibilities between these two roles since as in our research we ought to leave the personalities outside and describe the role. But when it comes to industry and industrial processes, it is the personality that creates the role. If you have a bright CISO and an average CIO it is logical that the CISO will take more and more responsibilities and his opinion will wage more than the others of course this applies vice versa too. In the ideal situation that both CISO and CIO are extremely good then the CEO will have to interact between them and play the role of a mediator in their arguments. In company A we see a Human Resources interaction with the security department where the security department has to run the background checks and obtain the security clearance for the potential employees. This is something that is different from company to company, in some you can find the HR runs these by its own. In the whole process we should never forget the legal aspects that have a major affect on every project or system the company runs since legal compliance is a must for every company. Closing this chapter we want to emphasize that there are three key people that actually run the security office but after all security is not just a three person job but everyone affects security and is responsible for it. All are responsible for the security inside a company!

How and on what extent is something that we will discuss when analysing the various roles individually. Furthermore, we would like to forecast that security governance and overall demands in security of a company will grow, over the coming years. Thus, in addition to the fact that security is such a specialized process it will require that someone supports you in it. That means, we expect a lot of outsourcing of security, leading the security to become an industrialized process.

2.3 Roles Analysis

Before we continue any further in our analysis and development of the individual roles we have to describe a little bit about the role analysis. When we look to a job we usually see it within the company. We think of different tasks, duties and activities of the job. Thus, because our primary understanding of a job is a company concept standing no meaning outside the company environment [17]. Looking at the job outside a company we understand that the job role is the way that someone contributes to the company. That makes the tasks and activities the means that the job holder uses in order to get the job done [17]. To understand what we are going to do in the coming chapters we would like to introduce you to the concept of job analysis. According to [17] "*Job Analysis is the process of understanding a job and presenting this information in a format which will enable others to understand the job.*" Furthermore, they [17] introduce four main principles that a job Analyst must adhere and which we endorse and follow in our research. Those are: "

1. ***Analysis not lists.*** *The Job Analyst separates jobs into their important constituent parts, examines them, and reassembles them in a way which facilitates understanding. Without analysis, the job description or role profile is likely to become a wearying check-list of small and unrelated tasks.*
2. ***Jobs not people.*** *Analysis is not concerned with performance, style, character, career history or anything else about the job holder. It is concerned with the job, and the present job holder is only involved because he/she usually knows most about it.*
3. ***Facts not judgements.*** *It is not the role of the Analyst to make judgements about jobs; rather the task is to communicate factual information as clearly as possible. The distinction is analogous to that between the news itself and the editorial comment in a paper. It is for the eventual users of the job description or role profile to form whatever kind of judgements are necessary for their purpose, on the evidence the Analyst has presented.*
4. ***The job as it is now.*** *The Analyst's role is to capture jobs as they are at a particular point in time. The job description or role profile should not be clouded by references to historic roles or future aspirations, although information on such aspects may well be gathered during the course of discussions about a job, or group of jobs.*"

Taking those principles into account we are going to proceed with our analysis of the roles to the best of our knowledge and understanding. Furthermore, we believe that in order to get a better understanding of corporate discussions it is important to analyse a job from a management point of view. However, due to the fact that analysing a job from a management point of view is a very broad topic we will leave that delicate task to more appropriate experts by taking a holistic view of a job and focusing on our expertise, which lie on the security related tasks.

2.4 CEO

2.4.1 Role Global definition

There are various definitions of the Chief Executive Officer and they are depending on the nature of the company. This is affiliated with the existence of a board of directors or their absence. When there is a board of directors, the CEO is the person who will carry out the goals set by the board. On the other hand when there is no board in place the CEO is the person will set those goals and sees them through. Below you can find three well known definitions of the CEO role.

Investopedia [4] defines the CEO as "*The highest ranking executive in a company whose main responsibilities include developing and implementing high-level strategies, making major corporate decisions, managing the overall operations and resources of a company, and acting as the main point of communication between the board of directors and the corporate operations. The CEO will often have a position on the board, and in some cases is even the chair.* "

The Business Dictionary[5] defines the CEO as " *Top executive responsible for a firm's overall operations and performance. He or she is the leader of the firm, serves as the main link between the board of directors (the board) and the firm's various parts or levels, and is held solely responsible for the firm's success or failure. One of the major duties of a CEO is to maintain and implement corporate policy, as established by the board. Also called President or managing director, he or she may also be the chairman (or chairperson) of the board.*"

Business Glossary [6] defines the CEO as "officer who has ultimate management responsibility for an organization. The CEO reports directly to a board of directors , which is accountable to the company's owners. The CEO appoints other managers, including a president, to assist in carrying out the responsibilities of the organization."

2.4.2 Role analysis from a management perspective.

It is common knowledge that people are the one species upon this earth that consider themselves to be on the top of the food chain. That is a statement that can be used from the CEO as his role places him at the top of the hierarchical chain but instead of the earth we have a company. He is the person who is "superior" to the others always metaphorically speaking. What are the first thoughts that come to a person mind hearing the term CEO? The human brain is a very complex organ. Usually a persons thoughts are divided into two parts the fast thinking and the slow thinking. The brain works differently when it comes to solve or associate somewhere where the solution is simple and easy for example, if five is bigger then three but it will react differently when it comes to a complex multiplication problem or complex problem. You can learn more about this in the video that ASAP science created "This is how your brain works".[7] But what was our purpose why did we introduced this concept? Thus, because Hollywood, has presented us for many years the CEO as an old person playing golf, going for fishing, living in a penthouse in a nice area and is far from the office and has others to do the job for him and is only there when crucial decision have to be taken. Well, we might be accused of watching too many films but that is the first thought that crosses a persons mind when

[4] http://www.investopedia.com/terms/c/ceo.asp#axzz2LMa3OKFa (10.02.2013)
[5] http://www.businessdictionary.com/definition/chief-executive-officer-CEO.html (10.02.2013)
[6] http://www.allbusiness.com/glossaries/chief-executive-officer-ceo/4957142-1.html#axzz2LN88X5mn (10.02.2013)
[7] http://www.youtube.com/watch?feature=player_embedded&v=JiTz2i4VHFw

he hears the term CEO and that's because it is the fast thinking process that takes place in our brain. Of course this description is far away from reality, but as always behind any story there is a part of it that is true. Therefore, lets take a look on what is going on in the real world. But, before we go any further we would like to clarify a certain authors view on the current thesis and his belief of science. We do acknowledge that this is an academic research and work and we do take this approach seriously and respectfully but we recall a quote of one of the greatest minds that ever walked this earth Albert Einstein where he stated " You don't really understand something unless you can explain it to your grandparents". Thus, said and in addition to our belief that academia is not only for academia, our goal is to conduct a thesis which is easy to read with a lot of "science" yet meaningful in an extent to various other readers. We have already introduced three different definitions of the CEO. They pretty much describe the same concept to make a long story short, CEO is the boss of a company responsible for its "well being" and "proper function". What do we mean by these terms and how they are interpreted in the real industry? Before we go there and answer this question we would like to go a bit back to the Hollywood description of the CEO, where it is always an "old person". We asked ourselves why is that? Does it come from reality? In our modern world where "*It Takes a B.A. to Find a Job as a File Clerk*" [8] a persons education takes at least up to his 26th birthday, and even more time for men if we attach his military service. A person's career starts towards the end of his third decade of his life. A relevant study [18] shows that it takes at least twelve years for a person to mature in his career in order to become suitable for the position of CEO and that in addition to the fact that in most cases a CEO will come from within the company [18] and grow until that position means that this process can be even more timely. Thus, leads us to the conclusion that usually a CEO will be at his 40's or 50's when he will step forward to the position. You can find many more interesting schematics about this in the [18] relevant research. We will not go down that road analysing how to become a CEO there are many good books in the market about that.[9] But rather we will try to explain what it means to be a CEO what is this role and provide an answer to the question we posted earlier in this section. A CEO is a manager, in fact he is the head of the managers, he is a person who has to build and supervise a very effective management team to support him in the governance of the organization. This is his hardest challenge to face! Since in most occasions he cannot build an entire team on his own due to budget limitations (cant hire more people or better professionals) or due to the fact that when he was appointed some of the key positions where already filled. That means that he has to find a way to inspire and motivate the staff he has in hand and try to get the most of them if his goal is to be successful. We name this as his hardest challenge and the reason lies in the fact that if a CEO can manage and coordinate his team in working effectively and achieving the goals he could focus only on the critical needs of the certain company and of course allocate all his resources on his strongest asset which is the thing(s) he knows best and do(es) best which will be very beneficial for the company. Our research draws us to the conclusion, always from a management perspective, that a CEO's top priority and job is to lead and direct the company in order to achieve the company's mission, settled goals,objectives and strategy as well as assuring

[8] http://www.nytimes.com/2013/02/20/business/college-degree-required-by-increasing-number-of-companies.html?_r=0

[9] We wont be recommending any cause promoting any book would be a contradiction with our ethics

that the company will comply with its philosophy. Which in the first place is defined by the board of directors or by the stakeholders of the company. Understanding this we describe the CEO in few words: "Decision maker, Manager, Leader, Visionary and Board Developer" but where do these descriptions rise of is something we will describe in the following chapter of the CEO responsibilities.

2.4.3 Role analysis from a security perspective.

There is a famous joke about the CEO and the CISO. "They are going towards the same bathroom and they never meet". There is truth in this joke since a lot of times the CEO doesn't have the time or isn't willing to listen to security issues since every time he sees the CISO he comes in with a new problem. But that doesn't mean that a CEO should neglect security. Either he likes it or not his destiny is tied up with security in the modern world. There is a dependency between the CEO and security . The first thing is that the first task of a CISO is to make sure that the CEO doesn't go to jail. Therefore a CEO should pay a lot of attention to security because he might face legal charges if something is not legitimate or goes down on a wrong path. But that of course is not the only reason why they are connected. Nor is the fact that in any security incident the CEO is the person who has to go out there and face the media taking the blame on behalf of the company. In addition to facing the furious board of directors or stakeholders asking why such thing happened? What connects the CEO to security? We will do the hard work and connect the dots. Starting with the statement: Neglecting Security will cost you! If a security incident occurs it will cost you a lot of money regardless of what it will be, a data breach or compliance issues they both result in paying a lot of money on compensation to the customers, third parties, paying fines to the government for compliance issues, spending money on forensics investigations, losing profit because of the business is put on hold. Additionally losing reputation and business opportunities and eventually investing the money you should have in the first place in order to develop your security and in the meanwhile dealing with the extra money loss and headaches of the different problems you have to face and covering the losses are things that could be avoided if you had taken security seriously in first place. Here of course we ought to say that there is no bullet proof system but investing in security increases your chances and minimizes exposure and mitigates the risk that is in stake. As an example we would like to refer to the well known incident of the Saudi Arabian Oil company which is the worlds leader in Oil which suffered a security incident and was out of business for eleven days and led to loss of millions of dollars. Data security is no longer a concern only for the CEO of Banks or CEO of governments (presidents after all are the world biggest CEO's) it is a concern for every company and its CEO. Think about the various data a company handles on a daily basis,data such as contracts, customer lists, auctions, suppliers, etc. information is an asset and the way that modern companies operate. Information is the strongest asset in a company's goal to achieve its objectives which when it comes to industry is revenue. If a CEO neglects informations security he is throwing a dice and gambling with his companies well being and revenue[19]. Without proper attention to security and the CISO suggestions a CEO will end up in the unpleasant for him position to wish that he had listened to all those technical or risk factors and issues the CISO was describing. But now it is unfortunately too late, he is [19] learning the hard way and seeing at best a breach in his financials and in the worst case seeing his name and his company's name

in the headlines of newspapers and media with bad consequences both for him as a CEO and the company itself. The CEO has to understand that security is no longer a technical game it is business related and a topic that should be addressed at the board of directors and the person who should address it shouldn't be the CISO but the CEO because he is the one who leads and the others follow. Security is a boardroom issue [19]! Furthermore, a CEO should acknowledge the fact that attackers are real and very sophisticated regardless of their motivation (Hackers, Hactivists, Insiders etc) and their reasons they will come for you and when they do they will do it hard. Best to be prepared. Understanding that technology evolves rapidly and gives tremendous opportunities and help for any business is a great asset for a CEO to have, but as always great things come with greater risks. That risk is security! The more technology advances the more the demand for security increases. This is an analogy, thus what history teaches us. The sooner a CEO realises that security is a continuous process the better it is for him and the well being of his company. A serious misconception that a CEO faces is that security equals with Compliance[19]. Regulations are made to be followed and kept but compliance is just a part of the overall Security process. We would like to close this section with a concluding sentence: A CEO that handles security properly will ensure the well being of his company (always from a security perspective) and his company will be distinguished from the crowd. A good security reputation brings business opportunities.

2.4.4 Role Responsibilities

In the previous sections we speak about the role of the CEO and that he is responsible on the well being and proper function of a company. We have described what these things mean but now it is time to go deeper and see how a CEO can accomplish them. What are his responsibilities. We described a CEO as a leader. Thus, because he is the head, he is the boss, he is the person to set an example for others to follow, he is the one that others will seek advice and guidance from. He is responsible in providing this guidance and advice. A CEO is responsible to advise the board, propose changes and motivate the staff into achieving the goals of a company. We named him as manager this is because he has to supervise the operations of a company. A CEO is responsible to manage the financial resources and invest them properly in order to achieve the desired outcome. He is accountable into dealing with the Human Resources drawing the policies and allocating the appropriate resources to the departments in need. Furthermore he has to conduct or approve plans which have to be implemented by his supervision. He is a Decision maker! It is his responsibility to pull the strings, make the final call, sort out the problems, balance the arguments, accept, reject or improve suggestions. In the end he is the one responsible and the one to take the blame if things go wrong. A CEO's nature requires him to be a visionary. Otherwise he cant compete in that position. He has to visualise the future of the company, forecast the opportunities that will come and seal them. As a CEO he is responsible for the connection of the board of directors and the staff he must ensure that they both are getting up to date information and assure that they will maintain a good relationship. A CEO has to be good with media handling. He is the public figure of a company and he connects the company to the community. Whether he will be a fund raiser or a donator on behalf of the company he is the one person who will be mentioned and addressed to. He is the public face of the company. Finally he is a board developer he is responsible to recommend people for the board of directors. He has

to provide support, recommendations and guidance to the board of directors and support it in the governance of the company. In his long list of accountabilities he has to add the annual self evaluation performance of both himself, the board's and also the company's. In addition to all these management oriented tasks, he has to de facto deal with security. He has to bring the security topic to the board and the whole company. He has to allocate the appropriate resources towards security. He is obligated to listen to the CISO demands and recommendations and proceed with them reasonably. As a CEO he has to adopt to the new modern world of security demands and change the way of thinking. Security is no longer just a part of the IT it is part of the whole company. He is responsible to oversees this vision to become a clear picture to everyone in the company. Thus, everyone is responsible for security. It is his primary responsibility to assure that proper plans on how to deal with incidents such as contingency plans, disaster recovery plans, business continuity plans are conducted and he is well informed on the procedures. Furthermore he has to keep up with the evolution of technology and support the evolution of security. After all security is a continuous process and he should make sure everyone realises this. Finally he has to be sure that the defensive mechanisms exist and are ready to defend in depth and with all means available, the companies well being.

2.5 CIO

2.5.1 Role Global definition

Chief Information Officer is defined as "*a senior executive responsible for establishing corporate information policy, standards and management control over all information resources.*"[20]

A modern definition of CIO given by Investopedia[10] is "*A company executive who is responsible for the management, implementation and usability of information and computer technologies. The CIO will analyse how these technologies can benefit the company or improve an existing business process and will then integrate a system to realize that benefit or improvement.* "

2.5.2 Role analysis from a management perspective.

Chief information officer (CIO) also known as Chief Technology officer (CTO) is a very complex but yet very well researched role. The role of CIO carries a long history, of more than half a century and is a constantly evolving role. Originally we find the CIO role back in 1950s known as data processing manager [21] which evolved to today's globally known CIO. As people we are admires of history and we believe history leads the way to future and is a powerful asset when it comes to learning. But, it is not our purpose to review the evolution of the CIO role, thus something many other fellow researchers did in relative studies [21], [22], [23], [24] , but to analyse how this role presents itself in modern industrial society. The chief information officer as the name reveals itself deals with information, using information in this concept we don't only include information systems but any kind of information needed for a company to operate on a daily basis. Starting with simple contracts ending to sensitive and critical information systems. In the modern world, information has become the strongest asset of a company. In fact it is a part of the revenue process by either generating revenue or by financial savvy with cut of costs inside a company. Thus, described we have primarily emphasize on the importance of

[10] http://www.investopedia.com/terms/ c/cio.asp#ixzz2LvovSTxp (20.02.2013)

dealing with information which is a very complex process. A CIO is a manager, regarded to be a technical manager,[22], [23] supervising IT departments, running company's servers dealing with hardware equipment and performing IT administrative duties, but nowadays he is a business manager [23], [21] integral to every department in a company and capable of speaking and understanding technical terms. Looking at the above description we can somewhat start to see the natural complexity of this role, but what is the "true" hidden challenge of this role? The fact is, this is a combo of two different roles opposing as one creating a very complex and demanding position. Where on one side of the coin, we have the technical part which covers the operational requirements of a company, ensuring proper function of data centres, systems, applications and overall IT functions/assets. On the other, we have the business manager who has to discover strategic opportunities [23], bring changes to the information flow infrastructure in order to benefit the companies operations and generate business opportunities or create cost effective solutions for the company. Either way, he produces revenue for the company and places himself as equal member of the C-level executives. The CIO are no longer a part of the support group rather they are key personnel for business innovation and partners in driving the business forward [23]. Thus, something also confirmed by another relative study [21] where there findings claim that "*The CIO has settled into one of two distinctive roles: (1) an executive that focuses on invigorating the firm's IT infrastructure to achieve an ROI*[11] *on the company's IT investments, and (2) another that is tasked with increasing revenue generation and the visioning and implementation of new IS throughout the corporation for business innovation.*". Furthermore the same research [21] concludes that the roles and responsibilities of CIOs fall into four natural categories: (figure 7)

1. *Triage nurse/firefighter: These are IS managers or executives whose main goal is to fix urgent IS-related problems (e.g., technical bugs, failed systems and disrupted processing).*
2. *Landscape cultivator: These CIOs have the primary responsibility for technical improvement and rationalization of the firm's data by maintaining and integrating existing applications and processes.*
3. *Opportunity seeker: The CIOs in this category are opportunity seekers whose main goal was to improve business processes within and outside the firm.*
4. Innovator/creator: These CIOs primarily focused on innovation and new opportunities, implementing new IS across the corporation.

Summarizing our management review of the CIO role and our deductive review of related literature with the most noticeable to be [25], [21], [22], [23], [24] which leads us to accept and inherit the forecast and description of the CIO role by Modis [23] " *The role of the CIO will become increasingly important in distilling changes in the technology/marketplace, translating those changes into opportunities and then taking a lead role in transforming those opportunities into actions.*" which is a reality nowadays in the modern industry.

[11] Return on investment (ROI) is a performance measure used to evaluate the efficiency of an investment or to compare the efficiency of a number of different investments

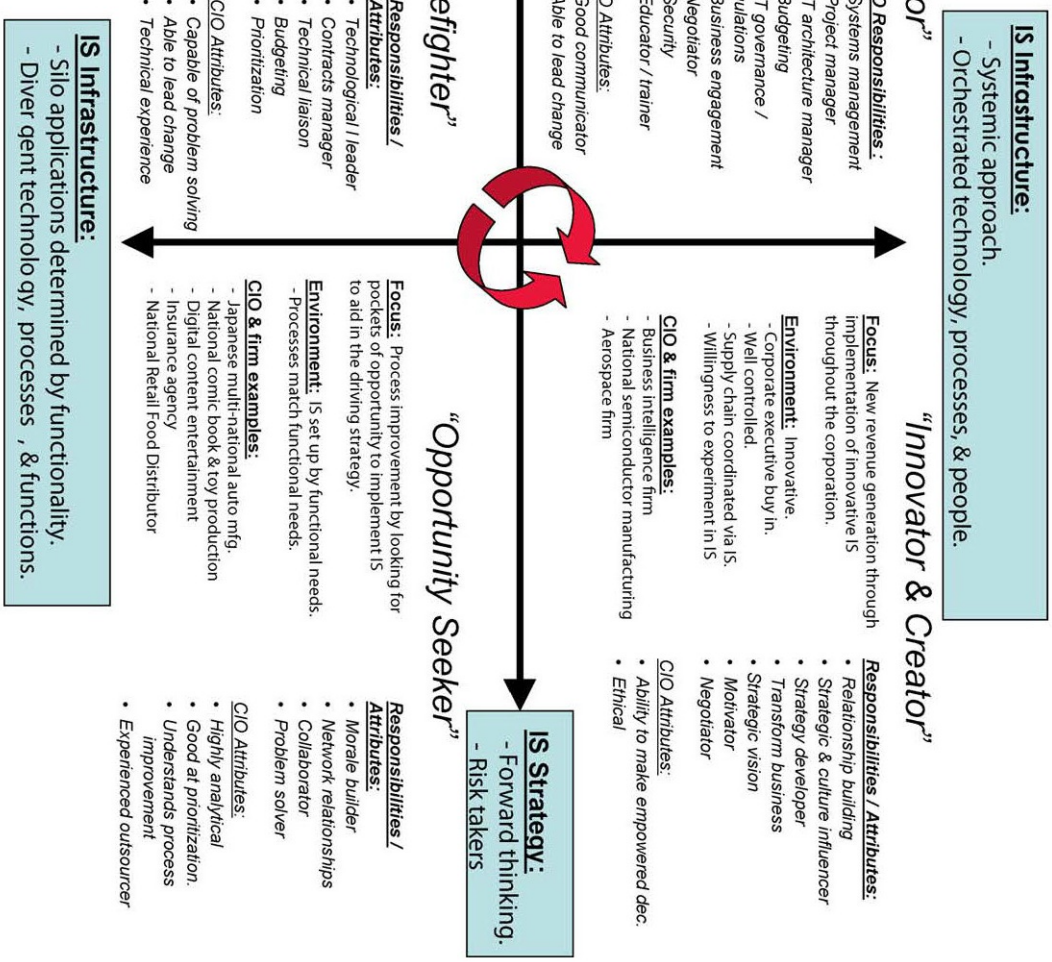


Figure 7: **Four CIO role types. M. Chun, J. Mooney / Information & Management 46 (2009) 323-334**

2.5.3 Role analysis from a security perspective.

We live in a digitised era where information is the alpha and the omega of a company. We read-hear in the headlines daily about security breaches which cost millions of dollars for companies. Something even stated by the President of United States of America Barack Obama in his 2009 cybersecurity speech, where he repeated McAfee's [12] $1 trillion annual cybercrime cost claim, exact quote: " *It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion.*" Whether this figure is accurate or not it serves our purpose to emphasize in the value of information. Thus, makes information a curse and a blessing, its a target and a prize for those who posses it. Who can deal better with information than the CIO of a company. We find that it is essential for the CIO to collaborate with the CISO and assure that information is safe. This is something that has to be done from day one since recovering from an incident will cost far more for a company. In addition, on a personal level as the recent case of the Saudi Arabian oil giant, an information security incident costs both their jobs. The CIO is the person who has to determine what is regarded as information for the company and of course its value. We speak of the value of the information but how do you determine the value of information? Thus, a huge challenge for the CIO, the value is measured by an audit process that the CIO has to lead. Furthermore it is affected and exposed by other factors, such as threats exposure, risk exposure and various cost benefits approaches. Those extra factors are key points that cannot be handled by the CIO himself and requires the presence and consultation-collaboration with the CISO of a company. Those two roles by nature are dependant on each other and that makes the CIO role the closest asset of the CISO and security. A CIO priority is to assure that information is audited and valued as any other business asset of the company. Furthermore, the results of those processes should be transferred and explained by him to the board of directors. Thus, because by convincing the leadership of informations value it is assured that the rest of the company will follow and endorse that belief. This will lead to the appreciation of the value of information and change the companies culture towards it. That is the primary goal of every CIO, an awareness of information's value and the need for its protection. Here, we would like to clarify a common misconception, information assurance is affiliated with the proper function of the CIA rule ,confidentiality, integrity and availability, but it is way more when it comes to the protection of information, something we will look into in future sections. We already speak of the connection of the CIO and CISO when it comes to information and its security, they have to collaborate and recruit the correct people to handle and deal with information and its security. There is an illusion that all IT people are suitable for all IT functions but that is just a fiction, having the wrong person for the job might end up even worse then having no person at all. Finally, from our point of view, when it comes to information the strongest asset is trust. Therefore a CIO should inspire a trust culture in the company and provide the tools and motivation for the staff to handle information and its security properly and seriously and this accomplishment is the borderline between a CIOs success or failure.

2.5.4 Role Responsibilities

We have analysed and presented the role of the CIO inside a company and now we will look at his responsibilities. According to [21] we can see in figure 7 specific respons-

[12] McAfee research: "Unsecured Economies: Protecting Vital Information " 2009

ibilities of a CIO based on the nature of the role a CIO tends to have in a company. Furthermore, the same study [21] concludes on six key responsibilities of a CIO:
(1) identifying, promoting, and managing IT-enabled business agility;
(2) innovating and integrating IT in the enterprise;
(3) communicating the impact of business decisions on IT costs;
(4) prioritizing and negotiating IT-enabled business initiatives;
(5) moving beyond managing the IT utility (supply perspective) to managing IT demand and value creation;
(6) demonstrating IT business value while maintaining IT goodwill among corporate executives.
Which the authors of the study claim to have verified with different relative studies. From our side we agree with their findings and is something that we have validated reviewing many different job descriptions and job advertisements from the industrial market where we find those attributes present almost in every document we reviewed. Additionally to these responsibilities we would like to add those with a security nature. A CIO has to identify what is regarded as information for the company, determine and categorize its value and emphasize on what is the critical data that he feels needs to be protected. Additionally he has to develop an awareness of information's value and the need for its protection both to the staff and the board of directors. He has to build and promote trust culture in handling information inside the company. Finally, a CIO with the collaboration of the CISO are responsible for the development of an information security strategy and policy framework that will safeguard the value of information inside a company.

2.6 CISO

2.6.1 Role Global definition

Chief Information Security Officer (CISO) is defined as: A job role that focuses on information security strategy within an organization. This security strategy can vary depending on the needs of an enterprise [26].

2.6.2 A Glance at History

We would like to start this chapter recalling a phrase of Robert M. Pirsig[13]: " Technology presumes there's just one right way to do things and there never is." Thus, the ultimate challenge for a CISO. Is there a correct way to do things in security? Will there ever be a point where we can say we have done everything we are now safe? Those, rhetorical questions have one single obvious answer: "security is a continuous process it will never stop evolving." In a discussion with Prof. Siv Hilde Houmb we asked "when do things change in the security of a company?" she stated: "Things change whenever a major incident occurs." We look back into history and we see that a major incident changed the course of Information Technology. We refer to the disastrous events of 11th September 2001 a date which change the global understanding of Information Security as we know it. The CISO role was introduced soon after the incident, first on a national level where the United States government created a dedicated officer solely responsible for information sdecurity. A trend that was rapidly spread to companies globally. Hence it was a way for many companies to demonstrate a serious commitment to information security, disaster recover planning and business continuity[27]. At that point executives believed

[13]Robert M. Pirsig is an American Writer and Philosopher

that hiring a CISO would be the solution to address the security "problems" [27] and would be reviewed by clients, partners and regulators as a positive sign showing that the company takes security seriously and increases a company's credibility. In the early stages the CISO role was a technical conception, it dealt with information security form a technical perspective implementing software and hardware solutions to protect information and its assets. However, that was the beginning of the information security evolution, the rapid advance of technology and the modern digitised era we live in where information is no longer a static entity that stays where you stored it and is constantly flowing in and out of a company through laptops, tablets, smart phones and various other means, making information protection impossible by simple perimeter-based security[27]. Thus, created huge demands for securing information. Nowadays, security is far more than the technical conception we once knew, of course technology still remains a part of information Security, but companies started to realise that security is not a thing, a product (software or hardware) that can be developed, configured, bought, but it is a continuous process at the very heart of business development and innovation [28]. This is also something stated by Bruce Schneier [14] in Preface to Secrets and Lies (2004) where he writes: "*In the real world, security involves processes. It involves preventative technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty. Security is not a product; it itself is a process. And if we're ever going to make our digital systems secure, we're going to have to start building processes.*" This modern understanding of security creates a very challenging role. Today's CISO faces so many different challenges on a daily basis that it will make little sense to describe them in this thesis since a challenge we might write today will be different tomorrow. Therefore, we will approach and study the nature of the role in an holistic overview.

2.6.3 CISO Role

who is Chief Information Security Officer ? Is he a fire-fighter; Is he the person to blame when things go wrong and a security breach occurs? Is he a risk manager or a regulator always posing obstacles and seeing things from a negative perspective? In an unofficial discussion of the author with Professor Bernhard M. Hämmerli and Professor Stewart Kowalski the author posed the same question " who truly is a CISO ?" Professor Stewart Kowalski replied: " *He is the person who will assure that the CEO of a company doesn't go to jail.*" Furthermore, he shared with us a funny moment of his long career as a CISO, we recall his words: "*When the CEO of Ericsson asked me what I want written in my business card under my name, I replied "Innocent Victim" the CEO said "victim" yes "Innocent" no* ". Although these are quotes from an informal conversation they are just a taste of what lies ahead in the search of the true nature of the CISO role. Questions like the above, can occur in every mind by simple reviewing a job description of a CISO. Thus, is something normal due to the complexity of the role. We would even dare to say that a CISO is the most challenging position that you could find in a company. A lot of people would raise a question: "why is that ? " We will come back to this question in the end of this section, although we believe that by the time we get there you will already have figured out the answer yourselves. A CISO is a person who manages information security in a company. We will try to decode this statement and analyse what it truly means to

[14] Bruce Schneier is an internationally renowned security technologist and author. Described by The Economist as a "security guru," he is best known as a refreshingly candid and lucid security critic and commentator. When people want to know how security really works, they turn to Schneier.

manage information Security. Thus what a CISO does. There are many different studies of the CISO role conducted through the years, We chose to isolate and concentrate on the following four studies [29] , [30], [31], [28], which we believe create a complete description of the CISO role. We will start our review by extracting and presenting the findings from the "Guide for the role and responsibilities of an information security office" [31] where you can see in figures 8-13 they develop 12 key components which they claim to be the components for a CISO to perform for an effective information security program.

Components	CISO Role and Responsibility
Component 1	
Risk Management **Objective:** To identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the agency. • Develop and maintain a risk management program. • Conduct risk assessment/analysis every two years. The resulting strategies should have a direct relationship with the disaster recovery priorities. • Mitigate security risks.	**1.1 Risk Management Program:** Create a formal process to address risk through the coordination and control of activities regarding each risk. **1.2 Risk Assessment:** Conduct formal vulnerability assessments of the agency environment on a regular basis. **1.3 Risk Mitigation:** Create a formal process to mitigate vulnerabilities.
Component 2	
Security Policy Management **Objective**: To provide management direction and support for information security in accordance with business requirements, relevant laws and regulations, and state policy. • Create, issue, and maintain security policies, standards, guidelines, processes, and procedures.	**2.1 Executive Communication:** Provide management advice and recommendations for the agency's information security program. **2.2 Policy Development:** Develop and maintain security policies, standards, guidelines, processes, and procedures. **2.3 Policy Compliance:** Oversee the monitoring and compliance with policies, standards, guidelines, processes, and procedures. **2.4 Employee Acknowledgements:** Create a security policy acknowledgement process.
Component 3	
Organizing Information Security **Objective**: Managing information security within the organization. • Management commitment. • Information Security Program. • Governance structure.	**3.1 Information Security Program:** Establish and implement a security program that aligns with the agency's business, mission, goals, and objectives. Establish a governance framework for communicating and coordinating security activities. **3.2 Independent Reviews:**

Figure 8: **CISO Accountabilities by California Office of Information Security and Privacy protection**

• Security agreements and contract language.	Implement a strategy for independent reviews at planned intervals. **3.3 Confidentiality or Non-Disclosure Agreements:** Oversee the development and process for the implementation of these agreements. **3.4 Third Party Agreements:** Establish security language to be included in the contracts and agreements.
Component 4	
Asset Management **Objective**: To achieve and maintain appropriate protection of agency assets. • Asset inventory, ownership, and acceptable use. • Data classification.	**4.1 Asset Protection:** Develop and maintain internal policies, standards, processes, procedures, and practices that prevent and detect fraud, misuse, and abuse of state assets. **4.2 Data Classification:** Develop categories and definitions that provide guidelines used to determine the appropriate level of protection for information.
Component 5	
Human Resources Security **Objective:** To ensure that employees, contractors, and third party users understand their responsibilities, that they are suitable for the roles they are considered for, and to reduce the risk of theft, fraud, or misuse of facilities by recognizing information security problems and incidents. • Screening. • Management responsibilities. • Security and privacy awareness training and education. • Disciplinary process. • Termination or change of employment. • Return of assets. • Removal of access rights.	**5.1 Personnel Practices:** Ensure activities related to employees include the proper handling of security breaches; and creation of checklists for managers' signoff upon employee termination or change of job duties. **5.2 Awareness Training:** Coordinate training efforts for the appropriate use of information assets, including personal, sensitive, or confidential information and the process to report security and privacy incidents.

Figure 9: **CISO Accountabilities by California Office of Information Security and Privacy protection**

Component 6	
Physical and Environmental Security **Objective:** To prevent unauthorized physical access, damage, and interference to the agency's premises and information. • Physical security perimeter and controls. • Protecting against external and environmental threats. • Working in secure areas. • Equipment security. • Secure disposal or re-use of equipment. • Secure disposal/destruction of confidential and sensitive information (paper and media).	**6.1 Physical and Environmental Security:** Lead or participate in the development and maintenance of internal policies, standards, processes, and procedures that prevent unauthorized physical access to state assets, damage from man-made or natural disasters, and conduct internal and external threat assessments.
Component 7	
Communications and Operations Management **Objective:** To ensure the correct and secure operation of information processing facilities. • Documented operating procedures. • Change management. • Segregation of duties. • Separation of development, test, and operational facilities. • Protection against malicious and mobile code. • Backup functions. • Network security management. • Media handling. • Exchange of information. • Electronic messaging. • Electronic commerce services. • Monitoring. • Protection of logs.	**7.1 Operational Procedures:** Lead in the development and documentation of operating procedures, including change control and separation of duties. **7.2 Protecting Against Malicious Code:** Activities required for the prevention and detection of malicious code, which could cause a disruption in business. **7.3 Backup Functions:** Activities required for the integrity and availability of information and systems. **7.4 Network Security Management:** Activities required for the protection of networks and supporting infrastructure. **7.5 Media Handling:** Activities for the prevention of unauthorized disclosure, modification, removal, or destruction of assets.

Figure 10: **CISO Accountabilities by California Office of Information Security and Privacy protection**

	7.6 Exchange of Information: Lead in the development and implementation of a formal information and application exchange with internal and external entities. **7.7 Electronic Messaging:** Lead in the development of policies and procedures needed to protect electronic messages and systems. **7.8 Electronic Online Services:** Lead in the development and implementation of security measures to ensure the integrity and confidential of information while accessing electronically. **7.9 Monitoring:** Ensure that agency operational policies and procedures are being followed. Periodically, or on request, monitor the controls in place in support of agency policies and procedures.
Component 8	
Access Control **Objective:** To control access to information. • Access control policy. • User access management. • User responsibilities. • Unattended user equipment. • Clear desk/screen policy. • Network access controls. • Operating system access control. • Application and information access control. • Mobile computing and teleworking.	**8.1 Access Control:** Review procedures for applying the appropriate rules and rights for each user or group. **8.2 User Access Management:** Review privilege and passwords rules and processes and user registration and de- registration procedures for granting and revoking access to information systems and services. **8.3 User Responsibilities:** Ensure users are made aware of their responsibilities in accessing, protecting, and using information assets. **8.4 Application and Information Access Control:** Review procedures to prevent unauthorized access to restricted systems, applications, and information. **8.5 Sensitive System Isolation:** Ensure the identification and separation of systems, applications, and information based on criticality and

Figure 11: **CISO Accountabilities by California Office of Information Security and Privacy protection**

	sensitivity.
Component 9	
Information Systems Acquisition, Development, and Maintenance **Objective:** To ensure that security is an integral part of information systems. • Security requirements analysis and specification. • Corrective processing in applications. • Input data validation. • Control of internal processing. • Message integrity. • Output data validation. • Cryptographic (encryption) controls. • Security of system files. • Security in development and support processes. • Technical vulnerability management.	**9.1 Security Requirements:** Participate in the development and maintenance of internal policies, standards, guidelines, processes, and procedures for the collection of security requirements, approval of project-related documents, change control, technical review, independent application testing, developer security testing, and the protection of system test data and program source code.
Component 10	
Information Security Incident Management **Objective:** To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. • Reporting information security events. • Management of information security incidents and improvements.	**10.1 Incident Management:** Establish a formal procedure for internally reporting and tracking security incidents, ensure incident response and escalation procedures are followed, and inform all employees, contractors, and third party users of their responsibility to report security incidents. **10.2 Incident Handling:** Participate and/or oversee in the investigation and management of information security events and policy violations and track to conclusion. **10.3 Incident Notification and Reporting:** Follow state policy for the notification and reporting of incidents immediately upon discovery.

Figure 12: **CISO Accountabilities by California Office of Information Security and Privacy protection**

	10.4 Lessons Learned: Develop and document corrective action plans and implement lessons learned to mitigate recurrence.
Component 11	
Disaster Recovery Management **Objective:** To counteract interruptions to business activities, protect critical business processes from the effects of major failures of information systems or disasters, and ensure their timely resumption. • Disaster Recovery Management – documenting, testing, maintaining, and reassessing recovery plans.	**11.1 Disaster Recovery:** Lead in the planning efforts for the agency's disaster recovery plan and provide oversight to ensure it is maintained. Participate in the testing and management of the plan.
Component 12	
Compliance **Objective:** To avoid breaches of any law, statutory, regulatory, or contractual obligations, and state requirements. • Identify applicable laws, regulations, statutes, and state requirements. • Protect organizational records. • Protect personal, sensitive, and confidential information. • Enforce policy, standards, and technical compliance. • Validate technical compliance. • Conduct information system audits.	**12.1 Internal Compliance:** Implement internal procedures to ensure compliance requirements are met, organizational records are protected and controls are in place. **12.2 External Compliance:** Ensure agency is adhering to all applicable laws, regulations, statutes, and state requirements.

Figure 13: **CISO Accountabilities by California Office of Information Security and Privacy protection**

At this point we will just accept those 12 components for granted and use them as a starting point of our research. Trying to compare them and see whether they complete the whole picture of the CISO role or whether something is missing. Therefore we are starting by reviewing the Business Model for Information Security (BMIS) created by ISACA figure 14 [29].

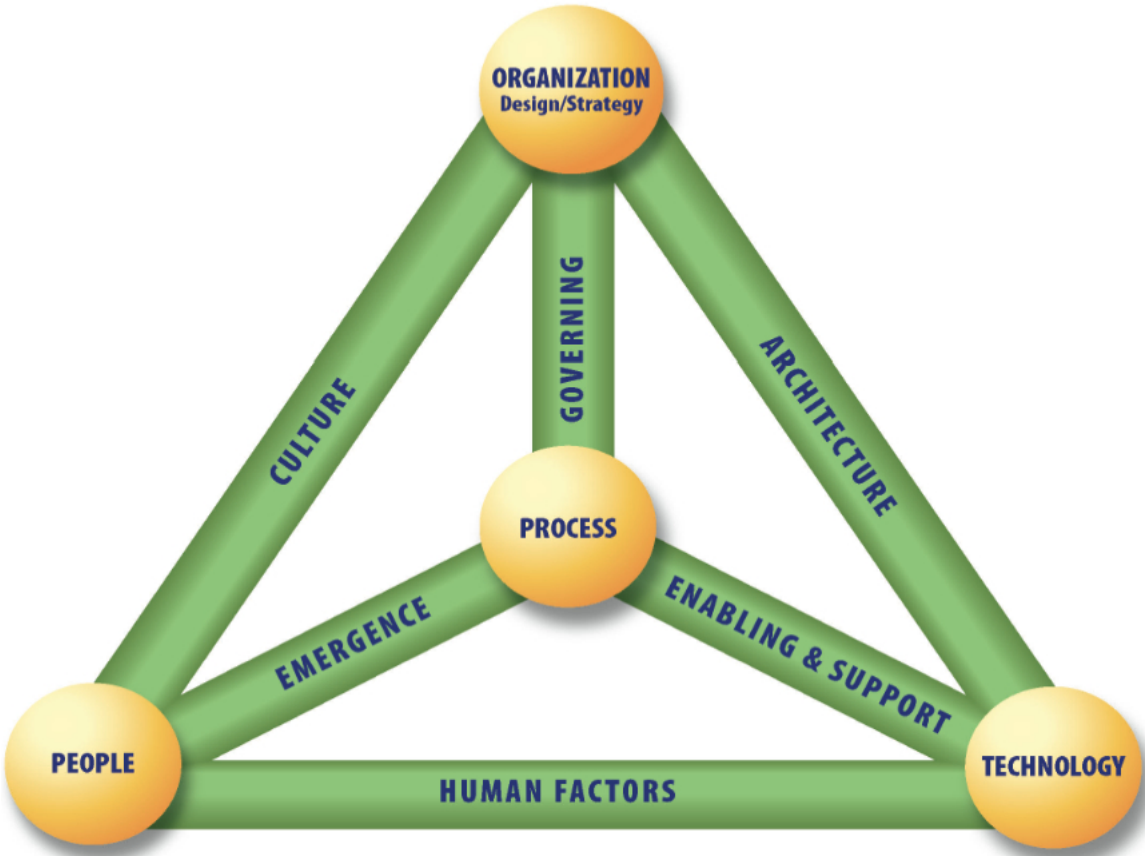


Figure 14: **ISACA's Business Model for Information Security**

We can easily identify the components of the model which is composed from four key components (people, technology, organization, process) and six interconnections between them (culture, governing, architecture, enabling and support, emergence, human factors). By just looking at those components we can identify similarities with some of the 12 key components proposed by the State of California. We studied the BMIS model and its components and found that all of the components are linked and included in the 12 key components proposed by the State of California. As a mater of fact, in both we have human resources identified in the BMIS as people and human factors in addition to that, people in the BMIS model represent also physical security and business assets things also present in components, 4 Asset management, and 6 ,Physical and Environmental Security, of the State of California findings. We also have Technology which is similar to component 9, Information systems Acquisition, Development and Maintenance, advancing further we have governing and culture which are linked to components 3 and 7, Organizing Information Security and Communications and Operations Management, which also includes the process component of the BMIS model. Furthermore,

we have architecture in BMIS which is spread between components 2, 7 and 9 of the State of California findings. In addition to this we have the two last components of the BMIS model which are emergence, which relates to risk management, based on our understanding of the description that ISACA provides for the interconnection which in the case of the twelve is the first component, and enabling and support which by ISACA's description deal with Access controls, policies, user responsibilities, awareness and compliance. Those are also identified in the components 2,5,8 and 12 of the California State accountabilities. By reviewing the BMIS model and the key findings of the State of California we identify similar approaches into managing information security. Between the two proposals we find three differences from those, the two are the components 10 and 11 of the California State guidance, Incident Management and disaster Recovery Management, which ISACA presumes as de-facto responsibilities and don't visually include them in their model, but rather hides them within the general culture needed for the application of this model. Meanwhile, the biggest difference is the exclusion of Information Security Economics which the State of California didn't include. Thus, the responsibility of the CISO to calculate and use an economical security adapted tool/model to validate whether the security investment/solution he proposes is justified. Moreover, security economics deals with proper allocation of existing budget and financial approaches towards security, such as cost benefits approaches and cost cut approaches. Thus, also the conclusion we generated by studying the [30], [28] studies of the CISO role, which align with the 12 proposed key components but add Information Security Economics in order to have a complete overview of CISO role and his responsibilities. Furthermore, we compare the derived findings of the California State guidance with the proposals of different frameworks such as COBIT [7], ITIL [8] and NIST [9] and ISO/IEC [6]. As a result we find that the California State government used ISO/IEC 27002 figure 15 as their basis for the creation of their guideline for the CISO role. Therefore, there are many differences between the proposed guidelines of the State of California and the description of the role from the COBIT, ITIL, and NIST perspective. Thus, of course, because ISO/IEC 27002 is very different from COBIT, ITIL because it is a pure security standard, so it has smaller but deeper domain towards security compared to COBIT and ITIL. But on the other hand it is in line with NIST framework since NIST harmonizes with ISO/IEC 2700x standards. We wont go deeper into the differences but rather refer to related studies such as [32] , [33] but it is important to mention that there is no perfect security and the adoption of a pure security framework such as ISO/IEC 2700x series could be a drawback for business. Therefore, companies usually have a combination of COBIT and ISO/IEC 2700x to achieve the desired result, not just for effective security management, but also for good business integration and proper overall IT infrastructure. It is proper to say that one framework usually completes the other. Such an example of combined framework is the OCIO/F4.1 Information Security Management Framework [34] which is a combined framework for overall IT, business and security governance of a company. But this leads to another interesting topic for research and any further discussion over it will drive us out of our scope which is pure information security management and the role of CISO. Summarizing, we have analysed and reviewed the role of the CISO from different frameworks and we found that the State of California has conducting a very good review of the role which aligns it with other relative research and frameworks and requires the addition of the Information Security Economics part in order to give a complete overview

of the CISO role.

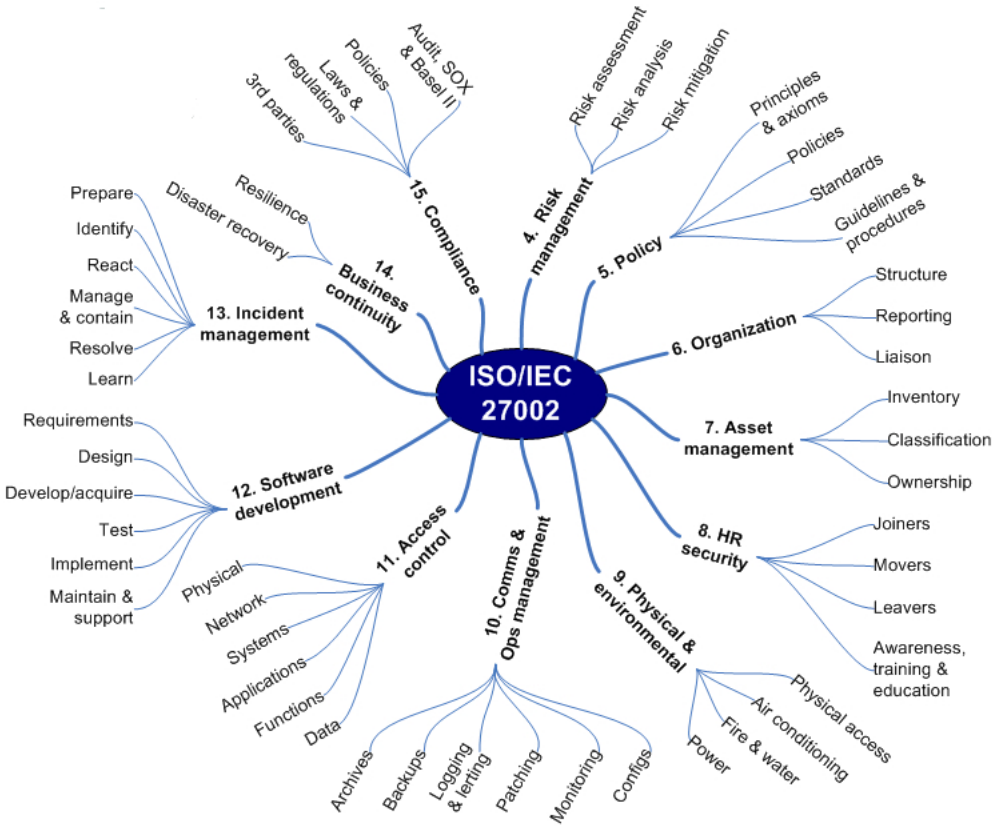


Figure 15: **ISO/IEC 27002**

The inevitable question that is raised here is "how such an important issue (Information Security Economics) was neglected by the State of California?" Our humble opinion is that because the guide was conducted by the State Government of California and there are no "issues" of security investments budgets within the state government especially if that state government is part of the United States of America, but that is not the case when it comes to companies. Companies have to include information Security Economics. Although we strongly believe and recommend that the whole 13 principles are followed by a CISO in a company in order to achieve good information security, it is often the case that most of the components are either neglected or considered not doable/profitable in the industrial market. This is our topic for the next section where we will scale down the growth of companies that have the ability to follow this guidance and which have to outsource or try to identify ways to comply with these key recommendations. In addition we consult industrial experts to identify the situation in the real industrial market.

2.6.4 Eyes of Industry

We now know for a fact that those 12 core principles derive from a government document, nevertheless they are identical to the ones ISACA proposes with the BMIS model. Taking into consideration the fact that the additional 13th component (Information Security Economics) derives from industrial research, makes it a must for every company. Also having in mind that the 12 components are government guidelines and proposals

for government agencies, we would jump to the conclusion that they are not applicable for companies or they should be altered or adjusted for company requirements. Thus, on the one hand true, minor adjustments might be necessary however the general scope remains the same. We used ISACA's model among other literature review's in order to compare those government instructions, but how does this serve our purpose to see whether these instructions are applicable only in a governmental level or in an industrial as well? The answer to that comes from the ISACA's study of the BMIS model[29] where they state that: " *The model can be used regardless of the size of the enterprise or the information security framework (if any) the enterprise currently has in place. The model is independent of any particular technology or technological changes over time. Likewise, it is applicable across industries, geographies, and regulatory and legal systems. It includes not only traditional information security but also privacy, linkages to risk, physical security and compliance.*" Although this statement gives us a partial answer to our question, hence the BMIS is composed from equivalent components with the government recommendations, we could claim that it makes them applicable for all size companies as well. Keeping of course in mind that the 13th added component (Information Security Economics) is included in every company by default and is out of the question. Thus, would be the easy thing to do but we would like to dive deeper into this topic. We should note that we do not doubt ISACA's claim which might be accurate for the BMIS model, rather we want to investigate whether these 13 components that describe the CISO role can be applied in any company regardless of their size. Through our studies in information security management we learned and developed a common understanding that the CISO role is affiliated with large companies with more than 1500 personnel. Thus, reviewing this role we acknowledge that we are expecting such components to suit entirely large companies and not Small-medium enterprises (SME). Thus, for a CISO to perform such duties described in the 13 components he needs a well defined budget and assigned security related personnel things that SME's in most cases cant afford and have other priorities. In a related study by David Lacey [35] his findings shown in figure 16 show that security for SME is approached on a different basis than the one in large/big companies were they choose to follow leading standards and management frameworks for information security which have a strong emphasis on policy, organisation and compliance requirements. Which according to Lacey: " *Are not suitable for SMEs who have a different perspective and attitude, responding primarily to practical drivers such as sales opportunities, rather than policy requirements.*"

Therefore, and based on our literature review we find that those 13 components are solely to be used by large/big companies that can afford to implement such security frameworks. This conclusion is driven entirely based on literature and theoretical research reviews of information security. The question that is raised in our minds at this point is " What about industry, how are things in reality?". One thing we learned in our long career in chess is that theory is always good but doesn't always represent reality and things turn to be way different when you start moving the pieces on the chessboard. Will this be the case here too ? Lets find out! There is no better person to ask than a CISO with a long and bright career with industrial giants. And we were lucky to know such a person. Therefore we ask prof.Kowalski to share his knowledge and experience on how things are in the industrial market. In our discussion the first thing that prof.Kowalski explained was the theory about different information security man-

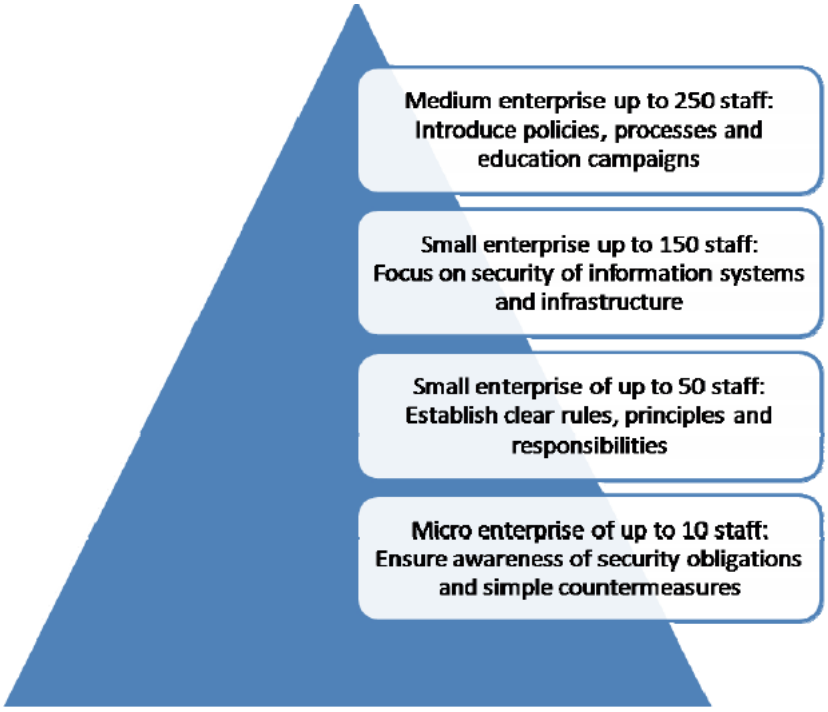


Figure 16: The impact of enterprise size on security priorities

agement models and frameworks. There are many different frameworks and standards out there. They are made by consultants for consultants with the ultimate purpose of earning profit from them. Therefore, the conversation was firstly around models where the professor showed us a quote of Stainslaw Jerzy Lec: " *Some like to understand what they believe in. Others like to believe in what they understand.*" Furthermore, prof. Kowalski shared with us figure 17 which shows the different approaches that we use to validate and verify a model or a framework and explains the Stainslaw statement. But what is the catch in all of this why are the models so relevant to what happens in industry? That, was the question that we asked ourselves and of course stated it to the professor. The answer is pretty simple, in industry, companies use models and frameworks that are proposed and so called globally accepted creating a trend and a must for big companies to follow, but the validity and question of how good they are still remains! That is the know how and understanding on how models work and that you need to have a model to manage it and when you manage it you can measure it. You cant measure it if you don't manage it and you cant manage it if you don't have one. Thus, said the industry uses frameworks that are proposed but every company leaves it to the CISO to choose which model to follow in managing information security. That means that this is personalized to the understanding and capability of the person having the CISO role. The common thing is that big companies use world renowned standards, like the model proposed by the State of California, because they are accepted globally and the change of concept and scope of how these models work happens only when a major incident occurs. Only then will they find out what went wrong with that model and try to improve it. The bottom line is that big companies use globally accepted standards for ISMS and the CISO is the person who will be choosing which of those models they are to follow and justify that

choice to the board of directors or CEO. However, we still owe you an answer on what happens with SME companies and not big industrial giants who have the money and resources to implement such globally accepted standards. We believe that there is no one size fits all when it comes to information security and companies but prof.Kowalski came to prove us wrong proposing his own model of information System management figure 18 which combines the core parts of any information security models which are people, culture, process and technologies. Some of those parts change rapidly, others over time, but it is their connections that reflect on how secure a system is and as prof.Kowalski explained, his idea of perfect information security is based on figure 19 where you can see the factors that affect security one way or another. Concluding, information security is based on many things, in industry it is based on models. What kind of model a company uses lies in the hands of its CISO if it has one. If not it lies in the hands of the board of directors or the CEO that have to make a decision based on the requirement of the industry and the needs for information security in that industry. Therefore, the Suggestion of David Lacey about SME is somewhat true when it comes to the industry. After all, security is based on people, culture, process and technology. That is something that is unlikely to change, hence it is the requirement on how we connect them that changes over time and that is why security is a continuous process.

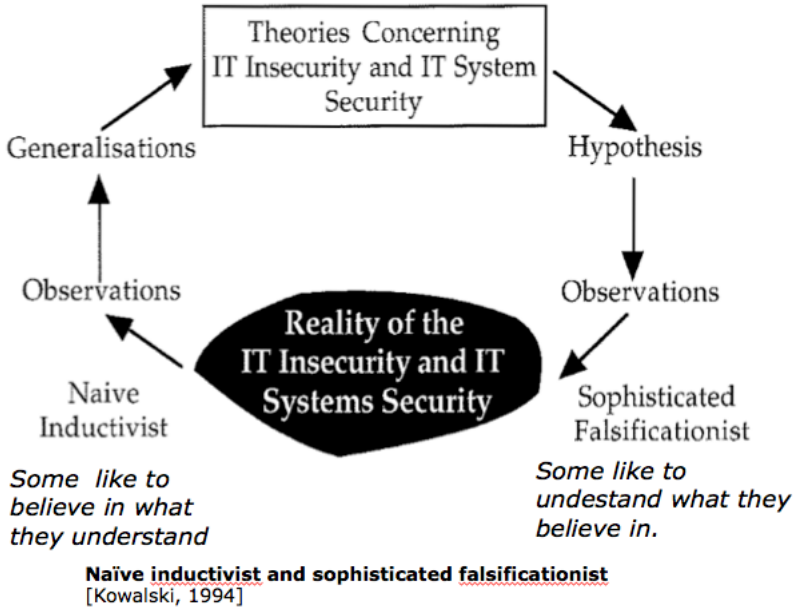


Figure 17: Naïve inductivist and sophisticated falsificationist

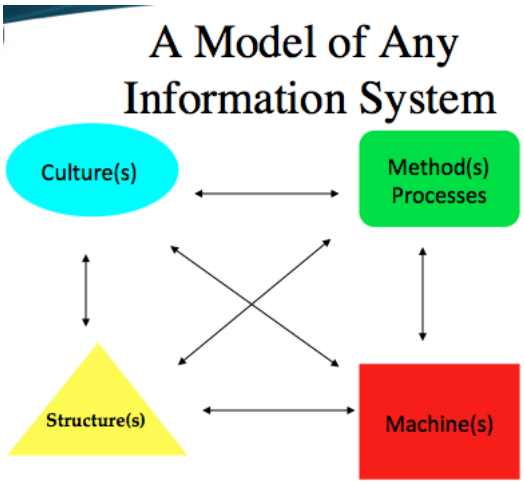


Figure 18: Model of any Information System

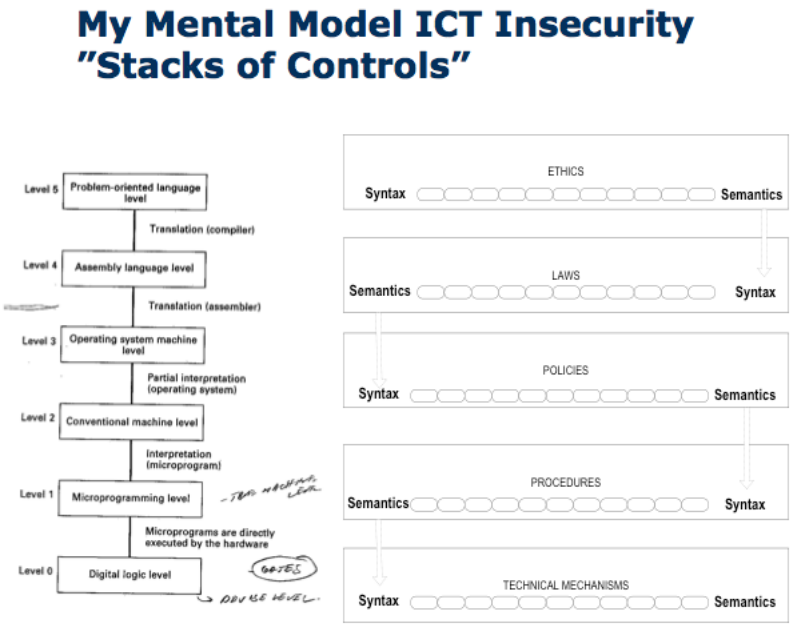


Figure 19: Factors of a Secure system

2.6.5 CISO Interconnections

Now that we have established the CISO role and his nature we would like to see what is needed for the CISO to perform his duties. As we have already stated many times security is not just a CISO responsibility but a concern of every department of a company. Therefore, we have created visual representations based on the findings from [31], [34], figures 20-21, of the roles/departments that need to assist and interact with the CISO in order for him to perform his duties which in our case are the 13 described components in the above sections. We would like to note that these interactions are not just positive interactions but also negative ones, meaning that those roles are involved with the CISO either in assisting him to perform his tasks or creating obstacles in his way and goal to conduct good security governance. We will provide more about the nature of these interactions in our review of each role.

Summarizing we would like to close our review of the CISO role by recalling William O. Douglas[15] about security: " *Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts.*"

[15] US Supreme Court Justice

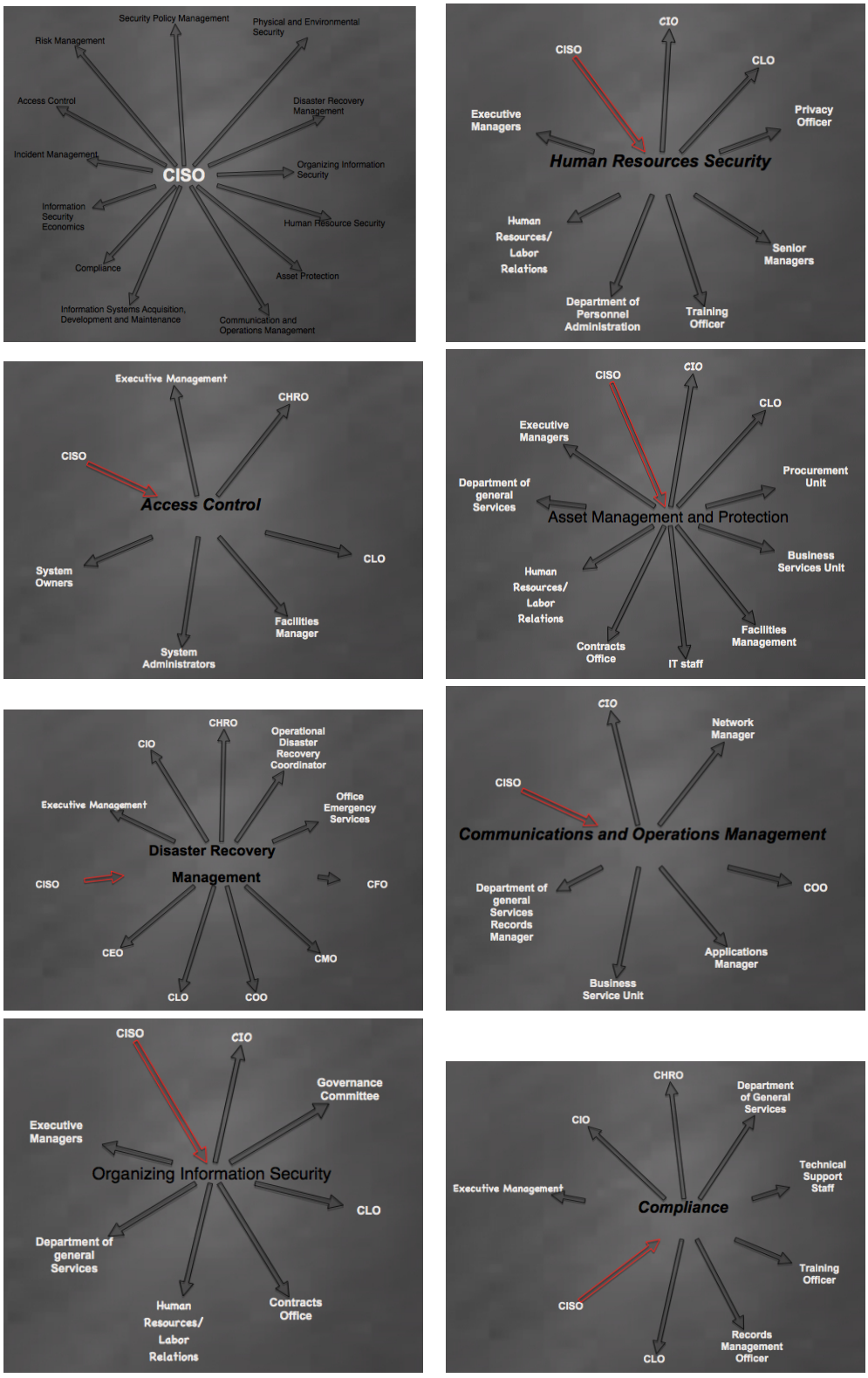


Figure 20: CISO Interconnection With other Roles in a Company

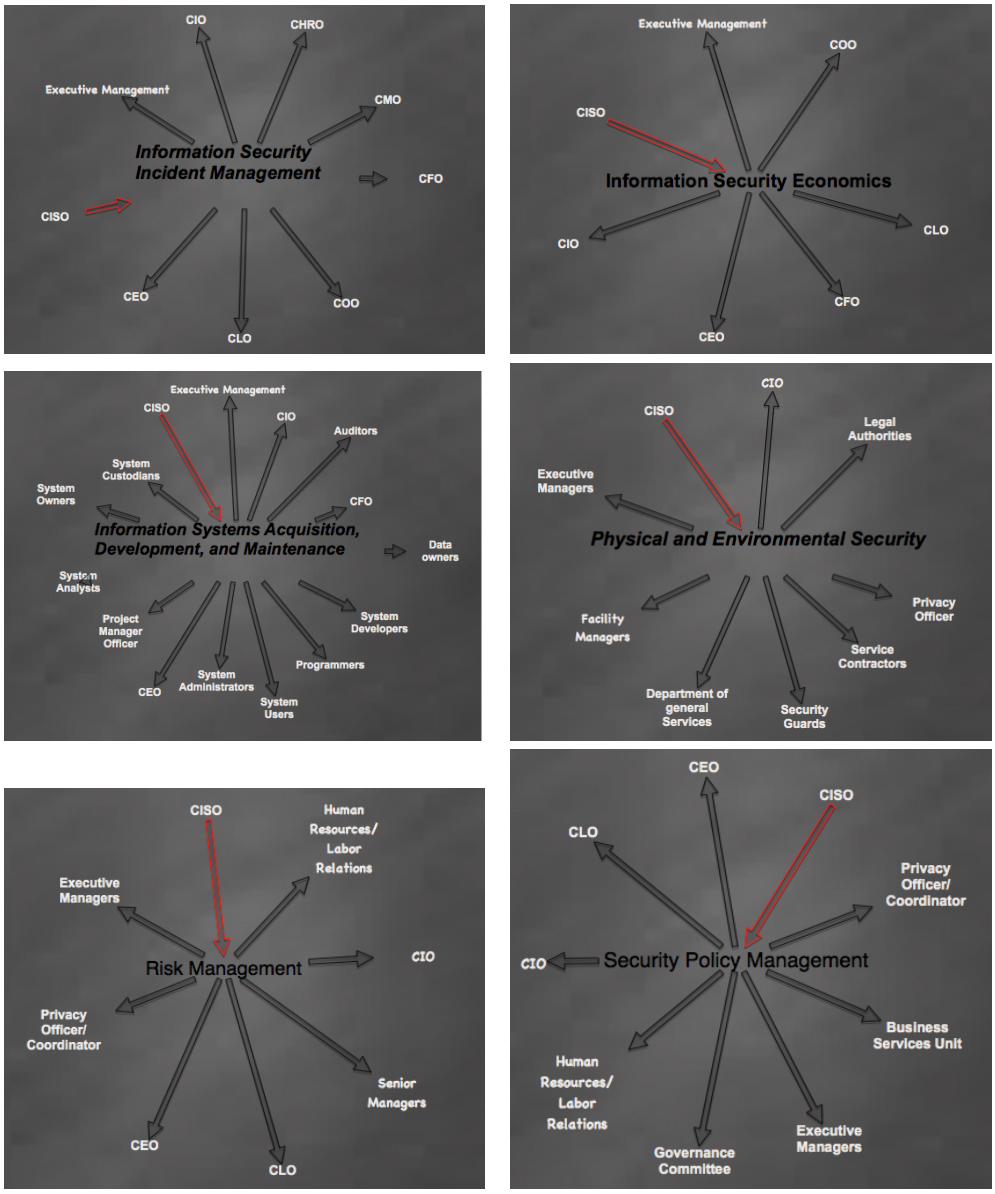


Figure 21: CISO Interconnection With other Roles in a Company

2.7 CFO

2.7.1 Role Global definition

Chief Financial Officer as defined in Investopedia[16] :
The senior manager responsible for overseeing the financial activities of an entire company. The CFO's duties include financial planning and monitoring cash flow. He or she analyses the company's financial strengths and weaknesses and suggests plans for improvement. The CFO is similar to a treasurer or controller in that he or she is responsible for overseeing the accounting and finance departments and for ensuring that the company's financial reports are accurate and completed on time.

2.7.2 Role analysis from a management perspective.

The role of Chief Financial Officer came to life in the late 1970s as a response to a new law the American government introduced [36]. At that period of time, a lot of American companies stocks where valued less than the actual assets and cash the company possessed, therefore a regulatory change in earnings reporting requirements posed a real threat to the companies earnings statements making the reconstruction of the financial department a necessity. Thus, gave birth to the Chief Financial Officer as a solution to firstly, an accounting problem and a response to the new law [36]. During those early years, the CFO was acting as the company's ambassador to it's investors and financial analysts. His primary tasks were to manage relationships between shareholders and to assure that their expectations were met regarding the companies stock value among other things, such as managing sales, acquisitions, divestitures and ultimately generate revenue for the company. Furthermore, as the role evolved more and more responsibilities were added. The development of accounting gimmicks to lower taxes, the participation in strategic and operational decisions, the evaluation of business unit performance and invention of new ways to increase capital in the company as well as its protection from adversaries takeover attempts, became routine things in a CFO's daily-diary. In the modern world and in the year 2013 we find that the CFO's role has changed from that of day-to-day management into that of a strategic thinker, shaping company's value and exit plan strategy, although it still inherits the characteristics of the previous years. The CFO is still responsible for overseeing all the "ancient" functions to come with the name. However, due to the modernisation of the companies financial department is no longer a one man job, rather a responsibility for various people. Therefore many of those "ancient" tasks [37] are delegated to senior officers leaving the old-school definition of the role: "manager of the day-to-day financial risks of a company" to the modern "A key player in building a company's business value to an exit plan." The CFO in his modern understanding is a leader, a strategic thinker, a person who will bring changes to a company and help the entire workforce to adopt a new era of changes. The CFO plays a key role in developing future plans for the company, he is one of the top financial analysts and he forecasts the future outcome of possible paths a company can take, with the ultimate goal of increasing "sales", revenue, and the assurance of the prosperity and future existence of the company. It is important to tell that he is not the person who will make the calls, but he surely is the person to provide the necessary financial data to prove whether an investment is worthy, profitable, or wrong. Thus, [36] makes him a good risk manager which is something that is a must for the position, the ability to mitigate risks and provide

[16] http://www.investopedia.com/terms/c/cfo.asp#ixzz2NFerfrRU

accurate forecasts are still key abilities of a CFO. Among the many and different accountabilities that derive from this position, a CFO should be able to identify the company's strengths, weaknesses, opportunities and threats [37] in order to build up productivity and cash flow always aligning with the board of directors visions and scope of values. Furthermore, as head of the financial department he has to oversee the development of business strategies that will minimize taxes and connect with existing departments to manage their financials with a cost benefit approach to maximise their efficiency and provide the necessary financial data to help them conduct long term plans/projects and operations. Although all the above described give you a broad overview of what a CFO means for a company, we left for last what we believe to be the two most imperative tasks which actually change the nature of the role from what it was to what it appears to be now. Thus, the abilities of the CFO in a) leading merges or acquisition of other companies and b) driving a company to an exit plan. These two "parameters" may appear to be opposite and may rely on the scope and future of a company as the stakeholders forecast it. But they aren't necessary opposite, since there is often a case that a company will first purchase another company in order to increase its business value and increase its stock value just before they enter the exit plan which exit plan is the process of increasing a companies value and in the end selling a part of it or the entire company to other investors. Either way, a CFO is a key player in this process whether it is the process of acquiring new companies or merging with another, he is the person who will forecast and provide a future outcome of such potential and he will be the first person the board will address before they conclude on any final decisions. These abilities of the CFO will make a difference "win or lose" for any company and that is the reason that sometimes the CEO of a company takes the CFO position as well. Summarizing, a CFO is an " all in one " package that will manage the financials of a company, will accept or reject investments, will oversee the well being of a company by being strict about reducing costs and increasing revenue for the company. He is a person who will take part in the shape of business goals, vision and objective of a company and assist the CEO into seeing them accomplished.

2.7.3 Role analysis from a security perspective.

We have introduced in figure 3 the ideal roles that need to interact to achieve good information security governance in a company. We can see the role of CFO highlighted in that figure that he is a key player when it comes to security. We can start our discussion on why the CFO is one of the most important roles when it comes to security by reviewing the industrial market where we can identify companies that choose to appoint the CFO as the reporting person of the CISO. That, might not be the primary case in the industrial market usually as we already mentioned in previous chapters, the CISO reports to the CEO, but this is just a case that highlights the importance of the role. But lets take a deeper look and see why the CFO is so important. The CFO is the person who "sets" budgets, recommends cuts, provides the means for other departments to implement projects and run processes. Thus said, we understand that he/she is the person who will provide the IT budget which usually will include the information security budget. Therefore, his understanding and beliefs about security are things that will either help security develop or become a serious drawback. Lack of security awareness and understanding will lead to costs cutting from the security budget and tie the hands of the CISO into man-

aging the security threats of the company. Therefore, the starting point is the budget. But in order to set a budget for security the CFO has to understand and accept for a fact that security is not just an IT risk but it is a real business risk, therefore it has to be treated as such. It is a CFO's responsibility to deal with business risks and find ways to mitigate. That will put security on the top of the risk list. A CFO has to understand that security is a continues process that means that security is a continuous risk and needs constant investment and improvement in order to be mitigated. Thus, a CFO has to acknowledge and fully understand a philosophy that "The purpose of risk management is to improve the future, not to explain the past." [38] Risk management is just the beginning! Compliance is the second top issue when it comes to the relationship of a CFO and security. Governments around the globe force companies to keep personal data secure according to the Personal Data Acts each government conducts and any failure to comply with the requirements will lead to hefty fines. Therefore, that might look like a task of the CISO but it affects radically the CFO since any failure of compliance [39] has a direct affect on the company's financials and sometimes it might be critical for a company's future. Therefore, it is a top issue for the CFO that could eventually lead him to unemployment if such fines and penalties are issued, since he is the one who will be in the firing line accompanied by the CISO. Thus making the CFO an enforcer when it comes to risk management and compliance. Furthermore, financial deals, contracts, auctions, forecasts, product launch dates and prices are things that are within the information that has to be protected and can affect the financial well being of a company, as well as any financial information that shouldn't be publicly available has to be protected from threats that might appear to be a huge headache for a CISO but in reality it is for both. Thus, because if a security incident occurs the financial losses will be a huge price to pay, the loss of revenue production even if temporary might be fatal for the company. In addition, losing reputation, business opportunities and the business itself and being left with recovery and crisis management costs are things that he has to be concerned and be fully aware of. In order to be prepared to overcome the financial losses and restart the business he must have solutions, like business continuity strategies and disaster recovery plans in place. Things that require his constant interaction with the CISO in order to implement such policies and strategies. These requirements force a CFO to be a security aware person, a failure to do this would mean a failure in business. But is this the end? We speak of business but what really is business for a CFO? We have identified merges and acquisitions as on the top of CFO's agenda therefore lets see how security can affect those delicate processes. In our research we came across an interesting interview of Simon Church [17] [40] by CFO Innovation's [18] Pearl Liu we would like to share with you a small part of that interview in order to highlight the importance that information security plays in merges and acquisitions and let the experts speak for ourselves upon this delicate issue. Below you can find listed the part of the interview.

"***It seems mergers and acquisitions are accelerating in Asia and elsewhere. Is there an information technology and security dimension to M&A that CFOs and their companies need to know?***

I once was told by a wise corporate executive, who is very experienced in M&A, that the

[17] CEO of information security service provider "Integralis"

[18] CFO innovation Asia is the only online publication exclusively for top-level finance managers in the corporate sector in Asia and China.

best thing to do with M&A is not to do M&A. You are inherently bringing risk into your organisation. Often, acquiring a company in a different vertical or a different country will have different risks because you have different cultural imperatives. What we've seen is that companies may not fully understand the nuances [around IT and security] compliance issues in each county. We see this especially in the Asian market. For example, in Japan, if there is a breach [in information security], you have to tell the regulators within 24 hours. Now that's not common across all the Asian markets. In Australia, if somebody makes changes remotely, especially a systems change, you again have to tell the regulator. With large MNCs, often the systems change is done outside the country, remotely. In Indonesia, you have to have data centres, not just the data, but the data centres, installed actually in the country.
Does the information security issue have a significant impact on the M&A process? Will it drive up the cost, for example?
I have definitely seen instances where organisations decided not to acquire a company because of the messy IT system. The acquisition of a large multinational corporation failed recently because [the due diligence] study of their IT systems and processes found they were so significantly out of compliance. The acquiring organisation decided not to acquire that company. In M&A, the acquiring company is looking at all factors of the organisation. They are looking at how efficient the organisation is, what that organisation actually brings to them in terms of market scope and market size. Information security is definitely a deciding factor because it is directly related to the risk and the cost. So those organisations looking to be acquired should make sure their IT infrastructure is tidy, their security policies are compliant and their employees are educated properly [on information security]. "
Reading this part of the interview you understand the importance of both compliance and information security, that literally can be a deal breaker when it comes to acquisitions and merges, which raises security concerns for the CFO.
Last but not least we would like to address a very modern issue and security concern for both the CFOs and the CISOs but one which derives from the CFOs, the mobile computing and bring-your-own-device policies which CFOs tend to accept and promote. In order to achieve an attractive workplace the CFOs let the employees work the way they want. Something that eventually leads to massive productivity advantages, because the employees will be more effective, efficient and happy. Such policies that might be considered at least at the moment as good practice, raises a lot of security concerns and issues, such as data loss, inappropriate usage of devices, unauthorised access to non personal devices of the company and many more yet not fully revealed threats and risks that need to be handled and mitigated. This is a topic with a lot of ongoing research and only time will provide us results and ways to address this issue. For the time being we would like to address the CFOs about this new "security threat/risk" and advice them "If they haven't started to pay attention, now's the time to do it!"

Closing this chapter we would like to state that "Information security is expensive!" but not paying proper attention or not having it at all will cost you way more eventually! And that's a lesson we wouldn't wish a CFO to learn the hard way, therefore if security isn't one of the top things on your list make sure you place it there!

2.7.4 Role Responsibilities

Now that we have given an overview of the CFOs role it is time to generate the role's responsibilities. We summarize them in table 1 listed bellow.

CFO Management Responsibilities	**Task brief description**
1.Business Strategy	Assess annual organizational performance. Assist in establishing yearly objectives and goals. Oversees strategic long-term budgetary planning and costs management in alignment with the board of Directors.
2.Financial Planning and Analysis	Conducts regular financial planning reports. Conducts analysis of financial conditions of the company and forecasts financial expectations. Develop and execute analysis of various business initiatives. Develop and maintain capital budget.
3.Finance and Accounting	Oversee cash flow planning and ensure availability of funds as needed. Oversee cash, investment, and asset management. Ensure legal and regulatory compliance regarding all financial functions. Lead the development of accounting gimmicks to lower taxes and increase revenue.
4.Insurance and Real Estate	Manage company's insurance program. Manage the company's real estate affairs.
5.Merges and Acquisitions	Plan, develop and execute merges and acquisitions. Conduct analysis, forecast and provide future outcome of penitential merges and acquisitions.
6.Business value and Exit plan strategy	Conduct analysis recommend innovations to grow business value and companies stock value. Develop and oversee the exit plan strategy for the company.
Security Related Responsibilities	**Brief Description**
1.Security Culture	A CFO should be a security aware person. Allocate appropriate resources and funding for continuous improvement of security. Treat security as a business risk.
2.DRP and BCM	Participate and assist the CISO in the development of Disaster Recovery, Business Continuity strategies and plans.
3.Compliance	Oversee and enforce compliance with regulations to avoid fines and penalties.
4.Ensure financial assets security	Ensure that financial deals, contracts, auctions, forecasts, product launch dates and prices are things that are within the information that has to be protected and can affect the financial well being of a company.
5.Information Security in M&A	Ensure proper Information security infrastructure exists in the acquired company and compliance with regulations is in place and in order.
6.Bring-your-own-device policies	They raise a lot of security concerns and issues, such as data loss, inappropriate usage of devices, unauthorised access to non personal devices of the company and many more yet not fully revealed threats and risks that need to be handled and mitigated. If the CFOs haven't started to pay attention, now's the time to do it!

Table 1: **CFO Responsibilities**

2.8 COO

2.8.1 Role Global definition

Chief Operating Officer (COO) as defined by Investopedia [19] is: "*The senior manager who is responsible for managing the company's day-to-day operations and reporting them to the chief executive officer (CEO)*."

2.8.2 Role analysis from a management perspective.

Chief Operating Officer (COO) is a role that we could say survived through time, its existence starts a century ago in the railway industry and soon transferred to various companies in various ways. The very nature of the role, that of a corporate chameleon is the reason that this role stand the test of time. Even nowadays, unlike other management roles there are not defined professional standards or expectations of the job in companies across the globe [41]. There is only a set of skills that can be easily identified in the person possessing the COO role in any company. Although the role exists for more than a century now, for many years now it has lost its appealing nature and remains in the shadows. In the beginning of the 21st century we could say the role has "risen from its ashes" and once again became a must for almost every company. The global economic crisis [41] that struck the globe at the beginning of the 21st century created a need for business growth, business transformation, tight cost management in combination with huge efficiency and short product development life cycles for companies. Thus, when the role of the COO gained its lost value, the demand for an operational leader who would lead the companies in the complexed global market was a must. The very fact that it survived for so long and came back more powerful than ever highlights the role of the COO as one of the most demanding and important roles in a company. The importance of this role and the power it processes is demonstrated by the industrial market where we have the example of the ex-COO Timothy Cook appointed as the CEO of Apple in the summer of 2011. That is one of the first characteristics that accompanies this role for such a long time, that of a CEO Successor [42]. An executive that interacts with every department of a company and creates an environment and relationships that would lead the company to success. Furthermore, nowadays a COO is a co-leader, he is a person who often possess opposite skills to the CEO. He covers the CEO weaknesses and together they will lead a company to success. The COO has a a clear understanding of the company's assets and capabilities and will assist the Executive team and the CEO in crafting the strategic objectives of a company, as well as oppose them if he finds that the suggested strategy is too difficult to implement or too costly bringing back the C-suit executives to reality. A COO will be the person who will assist the CEO to implement the decided strategy by managing the people and processes needed to achieve the settled goals [42]. This is very important, since it will allow the CEO to allocate his attention to other corporate domains. Nowadays, operations has become the alpha and the omega of every company. Ones with strategic importance, because by optimizing operations performance a company gains significant cost efficiencies, hence increase of revenue which is the desired outcome of the stakeholders. The COO is the person who can keep the balance between cost cuts, efficiency [41] and flexibility of the company. That means a company will cut costs but yet keep the same quality of its products/services. He is a person who has to identify new technology, innovate, explore new markets and opportunities in order

[19] http://www.investopedia.com/terms/c/coo.asp#ixzz2NXQzbzEC

to optimize performance and grow the company's target audience and market share. We stated that one of the characteristics of this role is that its a chameleon. It is a role that adopts and find his place in any company with various responsibilities and obligations based on the nature of the company. Although the common thing that a COO does is to oversee every aspect and function of the business and interact with internal and external stakeholders. A related research [42] has identified 6 six key areas in which operations leaders play an active role and are common for every company. Due to the fact that we believe that a picture speaks louder and is equal to a thousand words we present you their results in their summarized graph figure 22.

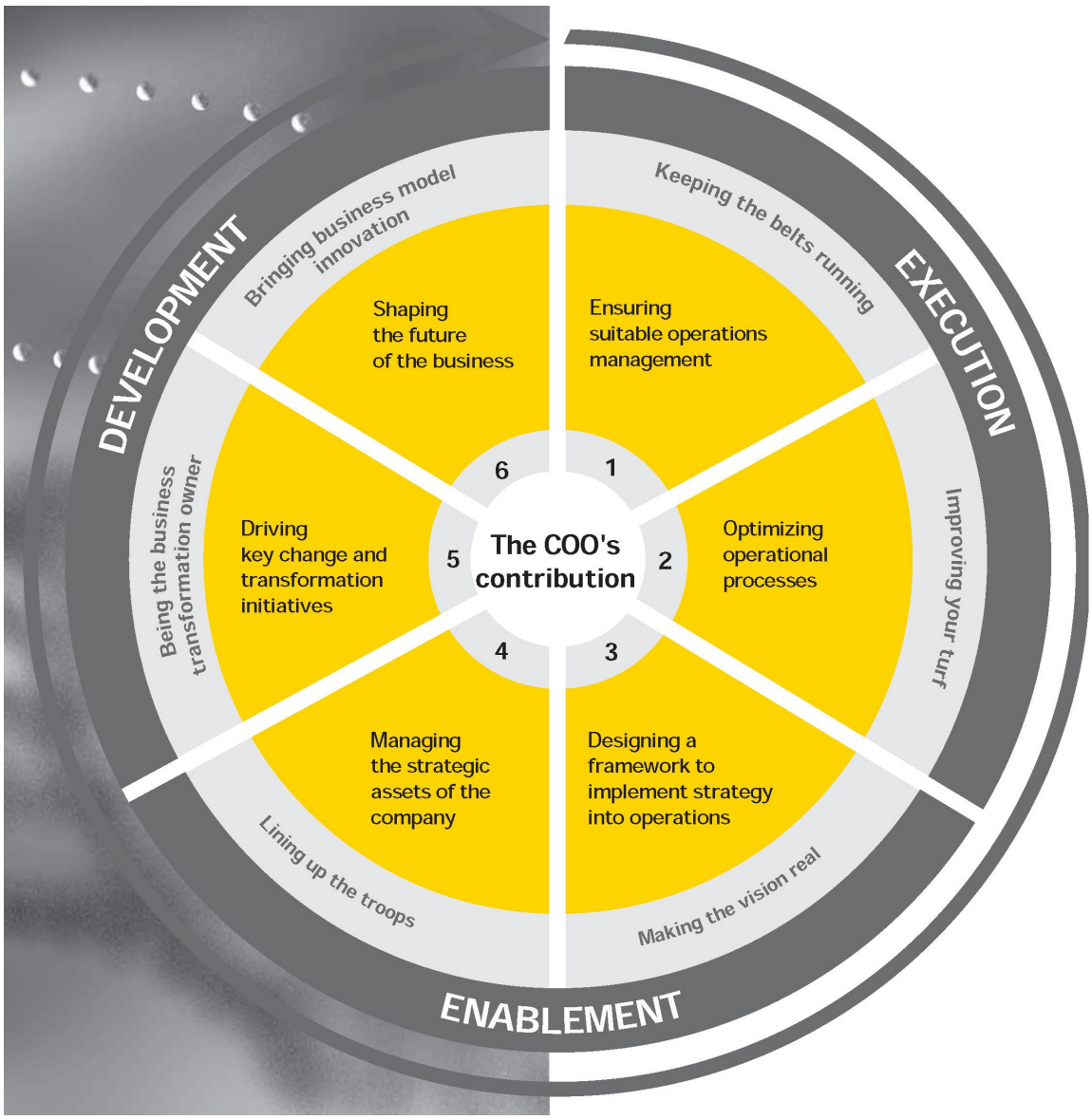


Figure 22: **COO's six key areas. (Picture Extracted from white paper The DNA of the COO [42]**

We wont go into many details of the core aspects because our goal is to give a holistic overview of the roles but if you would like more details we encourage you to refer to the

related study [42]. As you can see in figure 22 there are 3 domains that a COO is primary responsible for. We will give a brief overview of those domains below.

1. **Execution**
   This is the primary reason that a company needs a COO, to free up the CEOs time and deal with day-to-day operations. In addition to this, it includes the oversight of all departments, budgetary issues and company's growth strategies.

2. **Development**
   The COO plays a big role in the establishment of a company's goals, visions, strengths & weaknesses and evaluates future opportunities. He is the person that will bring changes, innovated ideas, leading trends and new technologies that would transform the business according to the market requirements.

3. **Enablement**
   It is the co-leadership with the CEO where the COO brings to life the visions and the appointed strategy by the CEO and the board. He has to find the way to align this strategy with the operations in order to achieve the settled goals.

2.8.3 Role analysis from a security perspective.

The operations of a company is the actual live feed, where all real time events and procedures take place and that's the place where most of security incidents occur. The operational department is usually the first department that will identify security incidents-breaches, since it is the department with the biggest activity in a company. Therefore its contribution to information security and overall security in a company is crucial. According to ITIL [43] there are 6 core areas which a COO has to cooperate and oversee with the CISO in order to ensure proper Information Security governance. Those areas identified in ITIL are:

1. **Policing and reporting**
   The COO has to ensure that the staff of his department are following the tasks and acknowledge the responsibilities assigned to them by the information security policy of the company. Such examples could be checking of system journals, logs, event/monitoring alerts and notifying the Security department of cases of unusual behaviour of the system or a suspicion of information security breaches. Furthermore he has to ensure that physical access to company's areas, equipment and network from third parties either for maintenance, visiting or operational needs is always supervised by trained staff of the operational department to avoid Security breaches.

2. **Training and awareness**
   This is one of the biggest security challenges a company's environment has to face. The "human factor" and human management is one of the hardest challenges towards security. Any security controls will collapse in seconds, by human error or an "insider". Thus is a live threat to any security of any company and the only way to handle it, is creating a security culture. The COO should ensure that the staff receives proper and continuous training and familiarise themselves with the security policy and procedures of the company. Emphasis on security should be promoted and security awareness should be highlighted and rewarded by the COO as well as disciplinary

measures if the staff fails to comply.

3. **Technical assistance**
   The COO has to ensure that the operations department is capable and willing to provide technical assistance to the IT security Department such as forensics evidence, data, time-lines, conditions etc. when an incident occurs. In addition, in an ongoing security investigation the staff cooperation is a must, in some cases interrogation of the staff will be needed. Additionally the COO should conduct and report potential security improvements/requirements, if any. Last but not least the COO should co-operate with the CISO in order to achieve security controls that will ensure efficiency and effectiveness both for the security and operational procedures.

4. **Screening and vetting**
   The COO has to ensure that the security and human resources departments are informed before hiring third-party contractors, in order for them to run the proper background checks and give the proper security level clearance and access to them.

5. **Operational security control**
   The COO has to report to the Security Department a list of people who will have access to critical systems as well as the purpose and the time that this will happen. Systems such as data centres, server rooms, root access to information systems or any other form of access that he is given conditionally. That list should be frequently updated and the personnel who no longer have the required access privileges have to immediately be removed from it. It is essential that the COO keep an audit trail of who has, had and when, access to those systems and the sort of activities he was performing.

6. **Documented policies and procedures**
   The COO has to oversee, the creation and documentation of a user manual regarding information security procedures of the operational department. The document should be generated from the overall security policy of the company and has to explain in more detail the department's policy regarding information security in order to educate the departments staff.

2.8.4 Role Responsibilities

Now that we have given an overview of the COOs role it is time to generate the role's responsibilities. We summarize them in table 2 listed bellow.

CFO Management Responsibilities	**Task brief description**
1.Ensuring suitable operations management.	Managing operating day-to-day processes.
2.Optimizing operational processes.	The COO should find ways to increase operational agility and efficiency.
3.Designing a framework to implement strategy into operations.	The COO has to derive goals for business units from the vision and strategy of a company. Additionally he has to oversee the development of operating systems, operating policies, directives, procedures in order to achieve strategic goals.
4.Managing the strategic assets of the company.	The COO has to protect the intellectual properties of the company. Foster talented employees and create models for rewards and recognition of staff.
5.Driving key change and transformation initiatives.	The COO has to inspire, plan, develop and execute a transformation plan with transparent outline of benefits for the company.
6.Shaping the future of the business	The COO must Challenge C-suite and CEO opinions, when needed and discuss, propose strategic options and business innovation.
Security Related Responsibilities	**Brief Description**
1.Policing and Reporting	The COO has to ensure that the staff of his department are following the tasks and acknowledge the responsibilities assigned to them by the information security policy of the company and report any suspicious activities to the security department.
2.Training and awareness	The COO should ensure that the staff receives proper and continuous training and familiarise themselves with the security policy and procedures of the company.
3.Technical assistance	The COO has to ensure that the operations department is capable and willing to provide technical assistance to the IT security Department.
4.Screening and vetting	The COO has to ensure that Security and Human Resources departments are informed before hiring third-party contractors.
5.Operational security control	The COO has to report to the security department a list of people who have access to critical systems as well as the purpose and time.
6.Documented policies and procedures	The COO has to oversee, the creation and documentation of a user manual regarding information security procedures of the operational department.

Table 2: **COO Responsibilities**

2.9 CLO

2.9.1 Role Global definition

A chief legal officer (CLO) also known as general counsel (GC) as defined in Investopedia[20] is: "*A publicly traded company's most powerful legal executive. The Chief Legal Officer (CLO) is an expert and leader who helps the company minimize its legal risks by advising the company's other officers and board members on any major legal and regulatory issues the company confronts, such as litigation risks. The CLO may also be a member of the company's operating committee and is overseen by the CEO. The CLO oversees the company's in-house attorneys.*"

2.9.2 Role analysis from a management perspective.

Chief legal officer or general counsel is a role of a C-suit Lawyer who's purpose is to defend whatever it is that the company wants to do. Thus, according to Deborah Majoras[21] , as implied in her interview [44] is a common misconception and as she stated: " *Nothing could be further from the truth. Our Job is much broader than defending our company in litigation.* " We accept this statement and will identify the broader concept that accompanies the obvious nature of the role ,that of a lawyer. We would like to quote Laurence Midler [22] where he started his presentation on the Chief Legal Officer Leadership Forum [45] with a series of questions: " *Is today's general counsel in an untenable ethical position? Can we be a trusted business partner and a confidant to the CEO and senior management, but still have a duty to the board of directors and be considered by the government as a guardian of the public interest? Can we have a legal practice with only one client, be at peril constantly of losing our livelihood in the event of a disagreement or worse, and yet have the courage to push back and insist that things are always done the right way at our companies? Can we be the embodiment of the conscience of an entire company, be responsible for ensuring that it complies with the law, and then be expected to be a zealous advocate and defendant when it doesn't*? " he answered these questions with a short answer "*I believe that we can. In fact, we have to. The best of us can walk the balance beam.* " and continued his presentation. These questions depict the very nature of the CLOs role that lies way beyond legal. A relative study of the CLO role [46] also agrees with the experts and in fact categorizes the CLO role into four sub-roles of:

A. Legal Adviser to Corporation and Its Constituents.

B. Corporate Officer and Member of Senior Management Team.

C. Administrator of the Internal Legal Department.

D. Agent of the Corporation in Dealings with Third Parties.

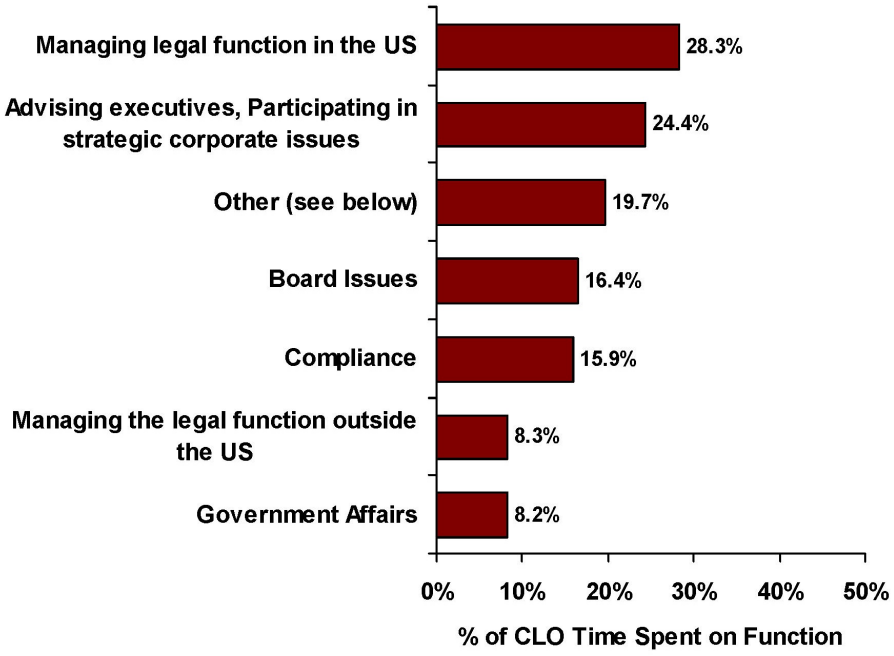
This categorization is also something that we can extract from a relative survey about the CLO role [47] where their findings, figure 23, imply and can lead to such kind of categorization. You can find the detailed analysis of those categories in the related study [46] we will not proceed into a more deeper analysis, but rather provide a general overview of the role.

But first a small glance at the CLOs history, the chief legal officer starts playing the role of a major player in the industrial market in 2002 when the Sarbanes-Oxley act

[20] http://www.investopedia.com/terms/c/chief-legal-officer.asp
[21] Chief Legal Officer and Secretary, The Procter & Gamble Company
[22] Executive Vice President and General Counsel, CBRE Group, Inc.

14. CLO Time Allocation

Please estimate how you have allocated your time over the last 12 months in your role as Chief Legal Officer.



Other functions:

Top four responses in order of frequency

- Practicing law / Providing legal services to the corporation
- Litigation management
- Managing other corporate functions that report to CLO
- Professional associations, Boards, Community involvement

Figure 23: **CLO Time Allocation (Picture Extracted from white paper Chief legal officer survey [47]**

in U.S.A. is introduced placing federal law deep inside a company's governance. An example followed by many other governments. The governments changed the scope of the global market introducing harsh fines for rule-breakers. CEOs and C-suit executives start facing strong legal accusations for violations hardly anyone understands which in many cases lead them to jail-time. Issues like bribe investigations and accusations, endless lawsuits, class-actions and battles over patents and intellectual properties became commonalities in the modern world. Companies are destroyed by prosecutors without any accusations even reaching a courtroom. All these everyday life or death situations companies are facing produce the need of a very large and talented legal department. Thus, made the nowadays CLO one of the mightiest figures in the C-suite. Its time to see what he does. A chief legal officer oversees all the legal aspects of a company. Thus, assuring that the company's strategy and governance complies with the current federal laws of the state/country the company is located or belongs to. One of the key characteristics for a CLO is to be preventive and proactive. Thus, investigating, identifying and proposing solutions to compliance issues that could be raised before they become core problems for the company. That requires him, firstly to know and understand how the company operates, it's business units and business strategies as well as goals and means to achieve them, and secondly to know and assure that the company complies with the specific regulations for the industry the company belongs too. Furthermore, he should follow all the new laws, and foresee changes in the regulations that are yet to come and could affect the company and drive the company towards that angle in order to be prepared when the regulations will be eventually introduced. In addition he has to educate the staff in legislation and compliance requirements and keep the awareness high for legal matters in the company assuring that the staff are well aware of the legal consequences they might face for rule/policy breaking. A CLO is a key advisor to the board of directors and the CEO. A CLO is a lawyer by trade and he is different from the traditional C-suit members and brings different views. And as common knowledge indicates and also Deborah Majoras suggests: " *Diversity breeds greater creativity richer discussions and ultimately, better decision-making.*" [44]. The CLO has a strong connection with the board of Directors and usually reports to them and the CEO. He is a trusted advisor who has to forecast and assist them in the governance of the company keeping it in track with the regulations and promoting a legal culture in the company. One of the biggest challenges is to have to forecast future outcomes with limited time and information that makes a necessity for the CLO to be a quick thinker and a strong analyst and intuitive person that can see when the board and the CEO are taking a wrong turn in order to drive them back. Even if he has to place an ultimatum or a veto against them to prevent the losses that that track of action could lead to. That is one of the biggest qualities a CLO has and has to have. In addition to that a CLO is also a mediator and a negotiator, thus something all lawyers have by nature. Therefore, he is one of the first people who will handle deals with third party partners of the company protecting the company's interests. Last but not least, depending on the size of the company he has to build a qualified and talented legal department and cut necessary costs in order to stick to the assigned budget by the CFO and the board of Directors for the Legal department. Additionally, when lawsuits arrive, either with the company as the plaintiff or defendant he has either to be the lead litigator ,if the case is critical for the company, or act as an adviser on strategy to senior lawyers throughout the litigation process.

2.9.3 Role analysis from a security perspective.

We live in a society with written and unwritten laws. People build relationships based on trust and beliefs, mutual respect, morale and ethics. A handshake was once a symbol of an agreement that waged more then a signed contract, but nowadays in the pure capitalistic era things work differently everything is controlled by laws specially in corporate environments. Newton's Third Law of Motion: "For every action there is an equal and opposite reaction." We can say more active then ever, but adjusted to the modern view "For every action there is a law reaction-consequence-requirement". Our lives and society are based on laws, everything we do is decision based on the common sense and regulations. We as people are keeping a balance and frequently walking on what is called the grey area between the black and white side of the law, which is obey and comply or break and face the consequences. An example of a grey is for instance when we cross a street where there are no cars and we should wait for the green light. Some of us might wait others wont. Thus, how we live, every decision we make has a risk and has a law background. There are so many things we could write so many examples we could describe, but we will keep this short and keep it simple. Regulations are implemented to keep an order and let people live in a civilised world. Thus, also the way they imply for companies as well to keep everything in order and with proper functions. But where does Information security in particularly and security in general comes in to the game? In a previous section we give a small overview of what is security information is, but what we haven't presented you so far is what drives information security and why is it so necessary? A lot of us think of information security as a technical requirement, as a tool, a mean to protect the assets of a company but is this really the true nature of information security? Does this technical requirement create such a powerful gap that we need to fill it in and thus why we use it? Those were questions discussed between the author and Prof. Bernhard M. Hämmerli were we both agreed that "Yes it is partially true" security is a technical requirement, it is a driver thus the obvious part thus what most of us will think and treat it likewise! But that's just another misconception, what is true is that information security is both a legal requirement and a technical requirement! A lot of us would raise a question "Why is it Legal? " Despite the obvious answer that there are strong compliance requirements that is not the correct answer! Prof. Bernhard M. Hämmerli explained: "*Information security is a regulation requirement is the requirement to protect the investors and stakeholders of the company.* " It is the responsibility and the obligation of a company to protect the stakeholder-investors interests. Those people invest their money in a company and hence the law requires that the companies protect those investments. Thus, the ultimate requirement of the protection of company's assets enforced by law creates the strong requirement of information security. This is something that few people in the industry acknowledge and realise but those who do, create a strong information security governance in their companies. The bottom line is information security is a legal requirement which creates a technical requirement in order to be met and covered. Thus, makes it both! Now that we have revealed the true nature of information security and reveal it primary driver we can come back to the CLO role in this picture. If we go back to the figures 20-21 we can see that the CLO is present in almost every procedure and task the CISO has to do. That is logical, since legal concerns are those which generate those actions in the first place. Hence the CLO is a trusted guide-friend and consultant to the CISO, together they will shape the information security governance of a company

based on the company's nature and information security requirements. The CLO is the person who has to keep in track all the law changes and inform the CISO of their changes and address all the compliance problems regarding information security a company has to face. He is the person to oversee that the law is kept and complied with in all the information security procedures. When we speak of the law, we include all the laws that apply in the current industry and nature of a company. Such as technical laws, telecom laws, privacy laws, document control laws, software liability laws and many others, we cant go deeper in the way that the CLO has to assist and participle in the information security of a company because of the broader concept and nature of the company there will be specific requirement and tasks for the CLO based on the industry and procedure a company has. Hence the generalization is that the CLO has to assure that the law is kept and obeyed by the company.

2.9.4 Role Responsibilities

Now that we have given an overview of the CLOs role it is time to generate the role's responsibilities. We summarize them in table 3 listed bellow.

CFO Management Responsibilities	**Task brief description**
1.Legal Adviser to Corporation and Its Constituents	A CLO is a key advisor to the board of directors and the CEO. A CLO is a lawyer by trade and he is different from the traditional C-suit members and brings different views.
2. Corporate Officer and Member of Senior Management.	A CLO has to be preventive and proactive. He is a trusted advisor who has to forecast and assist in the governance of the company keeping it in track with regulations and promoting a legal culture in the company.
3.Administrator of the Internal Legal Department.	A CLO is required to create and manage the Legal department including recruiting talented personnel, cutting costs, managing budget and oversee departments procedures.
4.Agent of the Corporation in Dealings with Third Parties.	The CLO has to be a strong mediator and negotiator and represents and protects the company's interests in dealings with third-parties.
5.Legal Representative in court.	The CLO might be the lead litigator ,if the case is critical for the company, or act as an adviser on strategy to senior lawyers throughout the litigation process.
Security Related Responsibilities	**Brief Description**
1.Information Security Driver	The CLO is the person who will create the need for information security.
2.Trusted guide-friend and consultant.	The CLO will assist in the shaping of the information security governance of a company.
3.Compliance Enforcer	The CLO has to ensure that the company's information security complies with the regulations and standards introduced by law.
4.Law keeper and tracker	The CLO has to keep track of all changes in the law that affect the information security and inform the CISO of them, assisting him to deal with possible compliance issues.

Table 3: **CLO Responsibilities**

2.10 CHRO

2.10.1 Role Global definition

Chief Human Resources officer as defined by the Business Dictionary[23] is an " *individual within an organization responsible for hiring new employees, supervising employee evaluations, mediation between employees and bosses as necessary, and general overseeing of the personnel department.*"

2.10.2 Role analysis from a management perspective.

What is a company without people? Can it exist without people? Of course not. They are the beginning and the end of a company, they make the company. It's there existence that give breath to any kind of operations or procedures. As we clearly understand humans are important to any company and of great importance. Thus, creates a need of a person to manage all of these people. That's the reason companies have a Chief Human Resources Officer. Employees are considered as valuable resources for a company, but the fact is that they are people which makes it impossible for them to be treated like other material resources. Each and every one of them have their own special characteristics and require a different approach and treatment. Thus, what the CHRO brings to the table, is that he humanizes the company's life and introduces human values in the company. But is he just a manager who deals with the employees everyday? It was so some years ago where a CHRO was responsible for bringing employees and hiring the best employees that serve the needs of the company. Nowadays, they do far more then just bring new faces to the company. Today's CHRO is a complex role that has many requirements and expectations. As we can see in figure 24 there are factors that a CHRO has to deal with on daily basis.

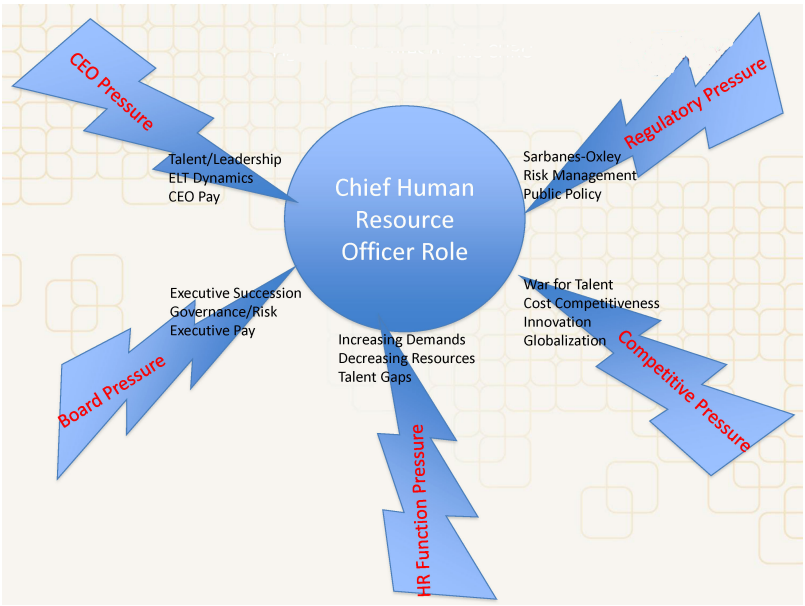


Figure 24: **CHRO Pressures (Picture Extracted The Chief HR Officer: Defining the New Role of Human Resource Leaders [48]**

[23] A web based business dictionary (www.BusinessDictionary.com)

We reviewed related studies on the CHRO role, [49] which is a visualised and extended version of [50] which study is itself later included in [48] book, as well as the [51] which is a consulting white paper, where they have a detailed analysis of the modern CHRO role. Therefore, from the [49], [50], [48] we have the summarised findings in figure 26 and from [51] figure 25. We can easily identify similarities and differences in the findings of the two related studies, those are differences between academic and industrial approaches. However, both studies agree on the nature of the CHRO role. That of a business partner, driver and developer, governance asset, employee recruiter, manager and evaluator. The CHRO as a C-level executive is a business partner, a key advisor to the board of directors and the CEO in the shaping of the companies strategy towards the companies goals and objectives. He is the person who knows the employees talents, strengths and weaknesses and has to pin-point them. He has to lead the strategy to a direction where the company will take advantage of its existing talents which of these benefits the company the most. The era when the board was shaping the strategy first and then letting the CHRO seek the correct people to implement the strategy is long gone. Nowadays, you know your employees and try to take the most out of them and recruit more people to fill in the possible gaps. The CHRO has to be a great analyst and judge of character. In other words he has to be an excellent recruiter. Today, when companies hire employees they make an investment which they expect to pay off. Thus, one of the key responsibilities of the CHRO is to find, talented employees and create the necessary environment to see them grow and reach their potential always according to the company's needs. Hence, the CHRO is a talent developer, he is a coach that will assist, guide, reward and motivate the employees in order to maximize their efficiency and productivity to assist the company achieve its goals. Thus, makes a CHRO a value creator for the company. In addition, he is also the person who will evaluate the employees performance and take appropriate measures if necessary. Furthermore, he is a balancer, a person who will solve any conflicts that might be raised between employees, regardless of their rank, top level employees or simple staff, create a happy and friendly working environment. The CHRO will assist and oversee the daily governance functions of a company, such as arrange board meetings, interact with employees, ensure regulatory compliance and oversee and assure high quality human resources services that include enhancing controls for human capital processes and mitigating risk around HR. Summarizing this chapter there are many different ways to categorize and present the CHRO role. We provided just two of them derived from different perspectives and backgrounds. However, the commonalities are very strong in any approach and the nature of the role remains identical just described with different words.

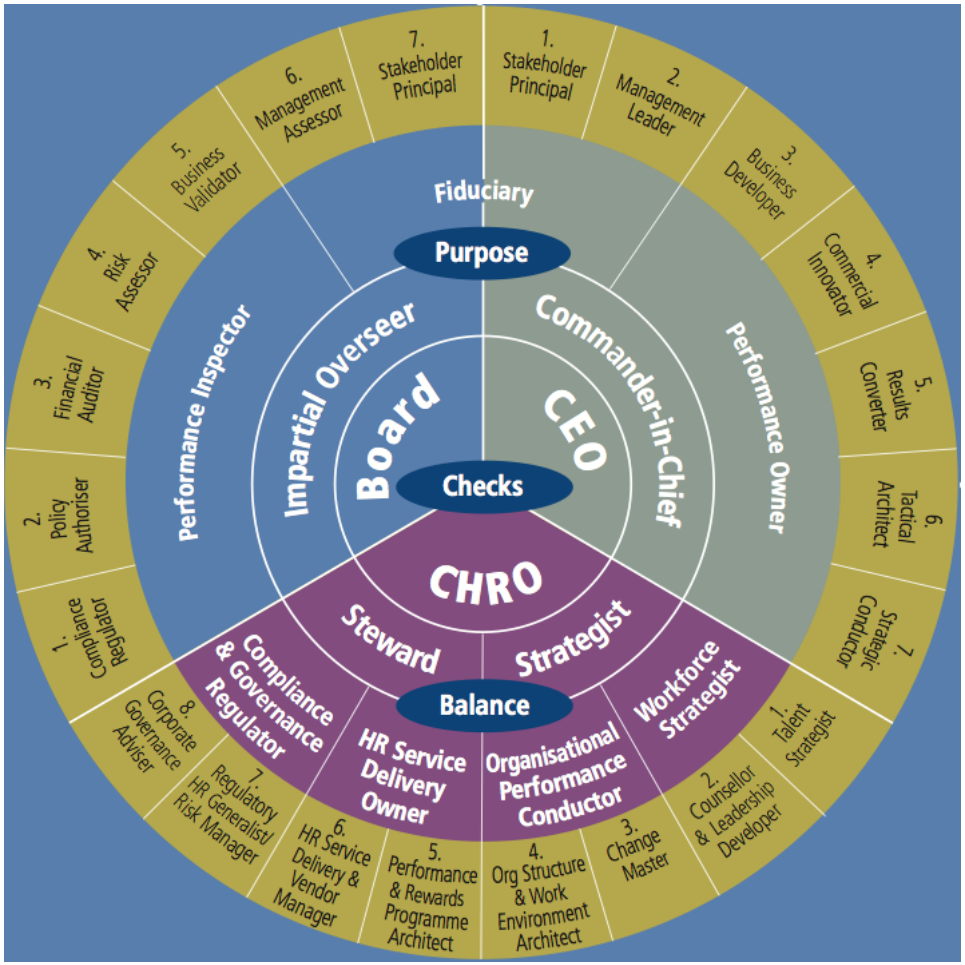


Figure 25: **CHRO ROLE (Picture extracted from The Evolving Role of the Chief Human Resources Officer [51])**

Figure 26: **Roles of the Chief HR Officer (Picture extracted from The Chief Human Resource Officer: Shifting Roles & Challenges [49])**

2.10.3 Role analysis from a security perspective.

Nowadays, it is not a secret that CHRO tend to be really well informed about the latest employee legislation, but they usually have no or very limited knowledge of information security. However, the CHRO plays a vital role on information security. Every employee that is hired has its own character, personality, education,"παιδεια"(pedia)an ancient Greek word that cannot be translated but means the way that a child is raised. How his character is shaped according to the principles, the beliefs, the values of his parents and the surrounding society he is living in. A persons honesty, dignity, self-respect, respect of others are characteristics that he gains from his early childhood and accompanies him through his entire life. The way of thinking, the way of living, the traditions and principles differ from country to country and that what makes people different. Of course every person has a different way of life and different experiences but still, a country shapes the character of its people. How does all this relate to firstly CHRO and then security? The CHRO is the person in charge for the hiring process of a company. Therefore it is essential for him to know all the above information for a person. Knowing the cultural background of the employees is essential for security and it gives you way more information about a person then from a cv or an interview. Knowing the cultural background of a potential employee reduces the risk of employing personnel likely to present a security concern [52]. Companies spend a lot of money to protect themselves from outside attackers but most of them forget about the insider threat and human errors. And here is the place where the CHRO plays a vital role, firstly reducing the risk of hiring the wrong people and secondly the CHRO [53] is in an ideal position to drive security messages, policies and procedures. Therefore, he has to assure the high security awareness is maintained in the company and that employees read and follow the security policies and procedures. In ISO 27002 series figure 15 you can see the HR linked with four processes, Joiners, Movers, Leavers, Awareness training and education. With joiners it means the recruitment process of the employees which we already discussed, by movers it relates to the relocation of resources (staff) and privileges that an employee has, such as access to sensitive information e.t.c. to fulfil his job. It is the responsibility of CHRO to oversee that there are proper records of who, when and what kind of access he has had in the system and inform the security department to change the clearances and privileges according to the current needs. In other words thus, closing down opportunities for the abuse of the organisation's assets[52]. When it comes to leavers either someone is fired or leaves the company for any reason, it is the CHROs role to oversee that proper communications between the HR and the Security department is kept and up to date, in order to assure that their access to all the systems are terminated and their accounts are suspended. We have already discussed about the awareness and education campaigns that HR can conduct and assure that the employees develop security concerns and a security culture. Thus, they can identify suspicious behaviour and report it accordingly to the proper people assisting in mitigating the risk of the internal threat of an insider and as well lower the potential of human errors. Furthermore, the CHRO has to oversee that proper framework is in place in order to verify that the potential employees are who they claim they are, something that also applies to the third-party contractors. Thus, [52] establishing that applicants and contractors are who they claim to be. This can be achieved by screening and vetting which includes security checks, background checks and other procedures which also lower the security risks. In our modern world

company/organization/government espionage is an every day phenomenon. We have heard a lot of stories about the games of spies in history. If we take a look at the cold war period between U.S.A and Russia there were a lot of spies stealing valuable and strategic information from each other. It was a very dangerous and extreme game but gave advantages to the one or the other party and that made it worth it. Nowadays these games haven't changed, they have advanced side by side with technology, but now they are not played only by governments but by private companies/organizations. It seems that bad habits have the tendency to survive through the ages. A lot of companies/organizations adopt the espionage technique in order to win the race against their competitors. This leads them into trying to bribe employees from another company to sell secrets, valuable information or even perform strategic hits on the company they work for. This is why Human Resources is a valuable asset for security, since they handle people, they know the employees and it is known to all of us that peoples behaviour and nature is unpredictable and that poses a threat on its own towards any kind of security. Human "errors" will always make a systems security vulnerable due to their unpredictability no matter what technical measures we take. The role of the CHRO is to assist and provide counsel and solutions interacting with the CISO in order to mitigate all these risks. Such consulting could be for example the cultural analysis of the employees and their potential behaviour to proposed security controls. In addition a very important issue is to assist the CISO into conducting a security policy that will be written in a way that employees can understand what their responsibilities and obligations are. What is the point of having a security policy if the employees don't understand what is written there and what is expected of them. This is of extreme importance since if an incident occurs and things get to court you should be able to prove that the responsible employee, if any, understood what he was doing and knew that he wasn't following the policy. Another important aspect that raises of security incidents is that they have to be investigated. Thus includes investigating employees, and *investigating an employee for any cause is serious business, and the process of conducting an interrogation is filled with employee relations land mines, so it is essential that HR and Security departments work together during an investigation. Thus, because a collaborative effort between Security and HR during an investigation provides the best of both worlds; a properly trained investigator is more likely to gain a confession, while timely advice and counsel from HR will provide valuable insight, in understanding the elements of the job, and they will help prepare the investigator to ask the right questions, and help preserve the rights of the suspect employee. After all, there is nothing worse than paying a million dollar settlement to a known thief simply because a slanderous statement was made about them during an investigation*[54]. This collaboration is extremely beneficial for the company since if an investigation ends with a successful outcome or otherwise it will give the opportunity for the CHRO and CISO to sit down and analyse the lessons learned from the process and identify weaknesses in the processes or policies and make future improvements. Furthermore, the CHRO has to have a very good understanding of what information security means to a company and what kind of people are needed to perform such a job [53]. What is the required skill set in order to bring success to the information security department; After all they are the people who will be hiring the CISO and assisting him to hire more employees to the security department. The correct people in the correct places will always make the difference between success and failure.

2.10.4 Role Responsibilities

Now that we have given an overview of the CHROs role it is time to generate the role's responsibilities. We summarize them in table 4 listed bellow.

CFO Management Responsibilities	**Task brief description**
1.CHRO a value creator.	The CHRO is a talent developer, he is a coach that will assist, guide, reward and motivate the employees in order to maximize their efficiency and productivity to assist the company achieve its goals.
2.Excellent recruiter.	The CHRO has to be a great analyst and judge of character in order to hire the right people for the right position.
3.Business partner and strategist.	A CHRO as a C-level executive is a business partner, a key advisor to the board of directors and the CEO in the shaping of the companies strategy towards the companies goals and objectives.
4.Performance evaluator.	A CHRO will evaluate the employees performance and take appropriate measures if necessary.
5.Balancer.	A person who will solve any conflicts that might raise between employees, despite their rank, top level employees or simple staff and create a happy and friendly working environment.
6.Manager	The CHRO will assist and oversee the daily governance functions of a company, such as arrange board meetings, interact with employees, ensure regulatory compliance and oversee and assure high quality human resources services that include enhancing controls for human capital processes and mitigating risk around HR.
Security Related Responsibilities	**Brief Description**
1.Excellent scouter and character analyst.	Knowing the cultural background of a potential employee reduces the risk of employing personnel likely to present a security concern.
2.Employees Awareness and education driver.	The CHRO is in an ideal position to drive security messages, policies and procedures.
3.Hiring,Termination and Relocations keeper	The CHRO keeps track of the access privileges an employer has, had to perform his duties and when those have to be terminated.
4.Identity and authentication	The CHRO has to establish that applicants and contractors are who they claim to be.
5.Valuable asset and advisor for security.	The role of the CHRO is to assist and provide counsel and solutions interacting with the CISO in order to mitigate all these risks.
6.Security incidents investigation asset.	The CHRO will provide valuable insight, in understanding the elements of the job, and they will help prepare the investigator to ask the right questions, and help preserve the rights of the suspect employee.
7.Solid understanding of information Security	The CHRO has to have a very good understanding of what Information Security means to the company and what kind of people and skill-set are needed to perform such job.

Table 4: **CHRO Responsibilities**

2.11 CRO

2.11.1 Role Global definition

Chief Risk Officer (CRO) as defined by Investopedia *is the executive responsible for identifying, analysing and mitigating internal and external events that could threaten a company. The chief risk officer works to ensure that the company is compliant with government regulations and reviews factors that could negatively affect investments or a company's business units.*

2.11.2 Role analysis from a management perspective.

The CRO role is a modern role with a small history behind it. The first CRO that was appointed *in August 1993, when GE Capital gave James Lam a job that brought together management of credit risk, market risk and liquidity risk, and he coined the term chief risk officer for his business cards [55].* The CRO role is usually found in the financial industry, usually we could identify it in banks, until recently when the global economical crisis started and it became a compliance requirement. Nowadays the CRO role is rapidly spread into many different industries. Thus, according to [56] is because there are many factors listed in figure 27 contributing to the need for sophisticated and integrated risk management solutions. As we clearly can see in figure 27 the drives for a CRO role in

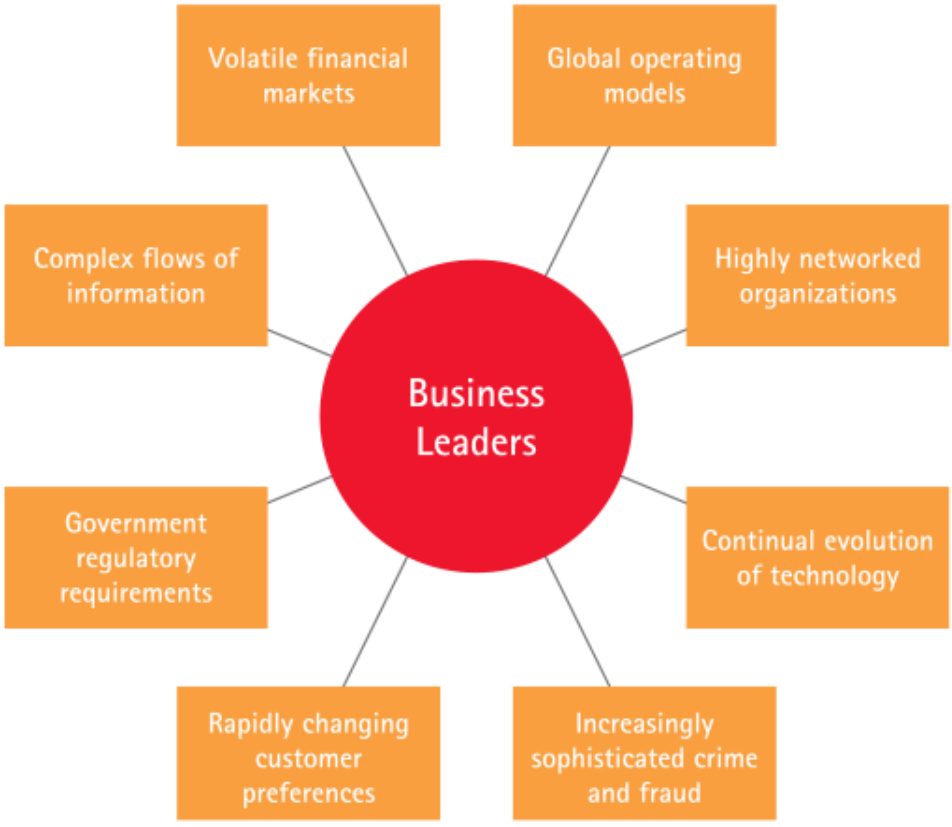


Figure 27: **Factors Contributing to the Need for Sophisticated and Integrated Risk Management Solutions (Picture extracted from [56])**

a company are way beyond a legal and compliance matter. And that is what makes the roles existence a necessity in almost every company. Furthermore, a survey [55] about the CRO role shows what a CRO brings to the table. We can see them in figure 28

Figure 28: **Greatest benefits of having a CRO (Picture extracted from [55])**

where we can see the different responsibilities and tasks that a CRO performs. In our review of these findings we clearly understood the nature of the CRO role, that of a person responsible for the so called: "Enterprise Risk Management" (ERM) of a company. But what does this mean? What is Enterprise Risk Management actually? In our studies the Enterprise Risk Management was defined as:

1. *The methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives.*
2. *Provides a framework for risk management, which can involve identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress.*
3. *By identifying and pro-actively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.*
4. *ERM can also be described as a risk-based approach to managing an enterprise, integrating concepts of strategic planning, operations management and internal control.*
5. *ERM is evolving to address the needs of various stakeholders, who want to understand the broad spectrum of risks facing complex organizations to ensure they are appropriately managed.*

We have so many definitions and explanations of the ERM because the Enterprise Risk Management strategies focus around global standards such as COSO, ISO/IEC 27001, the Information Security Forum's Statement of Good Practice (SOGP) and various others such as ITSEC (Information Technology Security Evaluation and Certification) and IA (also known as the Information Assurance Maturity Model) and others. We can see in figure 29 the typical areas of risk management in a company. In addition we can see in figure 30 the typical way of conducting the ERM. Here we have to note that there are various ways and frameworks for ERM we are presenting a simplified example in figure 30.

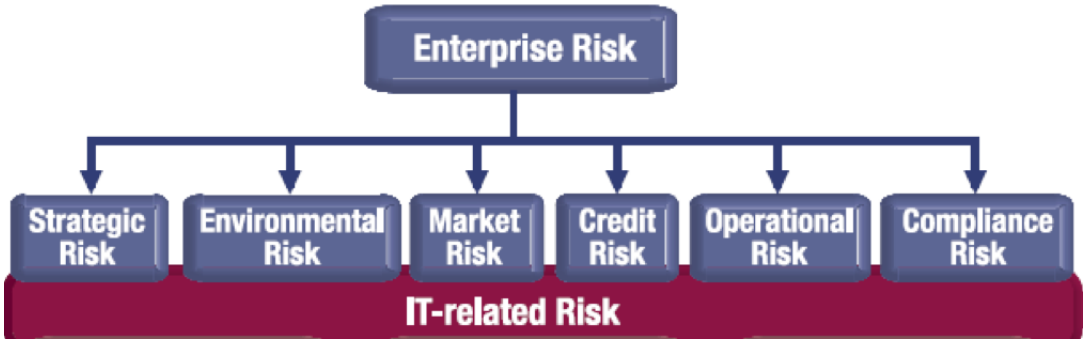


Figure 29: **Typical ER Picture extracted from Risk management lectures of GUC**

Figure 30: **Typical ER functions Picture extracted from Risk management lectures of GUC**

Now that we have introduced you to the concept of ERM, in reality we introduce to you the role of CRO, since that is what a CRO eventually does. Here of course lies a

question that is often raised by academia: "Why do you need a CRO when you can fully adopt to a ERM framework and have an embedded risk-aware culture? " The answer to this question lies in two parts. Firstly, many companies have tried this but failed [57] in the process because the process of integration would be divided between top executives which in the complex and demanding nature of their own roles responsibilities didn't have the appropriate resources to oversee this integration. Secondly, a CRO understands relationships between risks within separate business units that may never have emerged before. That's because the CRO is responsible in overseeing all the risks of a company. There might appear risks that a manager of a business unit would think as acceptable for the department but at the same time they might be unacceptable from the point of view of a company as a whole. Such kind of linkages can only be identified if there will be a man in the middle who can put the pieces together and manage the risks more effectively. In addition we have to note that there is no such thing that one size fits all when it comes to risk managements. Thus, said it is unrealistic to expect that the CRO is an expert in all the domains listed in figure 29. Its quite the opposite, he is just a person with a good understanding of Risk Management and can communicate with the rest of the managers and combine the whole picture of the company's risks and present them to the CEO and the Board of Directors. That makes him an interpretor of risks for a company. Summarizing our discussion we agree with the statement of Lauren Brown [57] : " *If organizations are serious about risk management they require a dedicated senior role to spearhead the program. It is the only way to ensure that ERM will be fully embraced. This is why the role of the CRO should be here to stay.*"

2.11.3 Role analysis from a security perspective.

Chief Risk Officer is a new role which people believe to be the natural evolution of the CISO. A role that has overall ownership of the enterprise risk management and leads its activities. In the modern industries a CRO is a person who will oversee and lead the integration of information security into a broader concept of effective ERM. This, means that information security will align with the ERM procedures and become a valuable asset. The role of information security in an ERM is to identify, evaluate threats and vulnerabilities to the information assets and infrastructure and implement, monitor and mature the controls in order to mitigate those risks. In this aspect, information security provides valuable data about business impacts and creates a risk profile towards the identified threats. This is the place where the CRO plays a significant role. He gathers the given data and performs a risk assessment providing feedback to the CISO with the risk-tolerance level associated with the threats and vulnerabilities. Therefore, the CISO can proceed with developing the appropriate controls and mapping them to the business needs of the company. This process assures that the risks in a company, not just information security risks but overall risks, are prioritised and that resources are spent accordingly and appropriately starting with critical risks in a company. The CRO role is a role of a coordinator, a coordinator of risk that receives valuable information from various departments regarding threats and risks and integrates them into a united framework providing risk profiles and the overall risk tolerance of the company to them in order to act and align accordingly. That is critical for the business savvy and hence it is relevant to the security of the company. Therefore, he can also participate in the creation of the business continuity and disaster recovery plans that the CISO has to lead and

provide him with valuable advice. Closing this section we would like to give a real view of a CRO towards information security. Therefore we quote James Lam [24] in an interview [58] where he was asked: " *As a Chief Security Officer, how can I tie my enterprise security risk assessments into an ERM program?* " and he answered: " *As a former CRO, I think the CSO has three important roles to play in ERM. The first is to ensure that corporate-wide policies and standards are established for information security (including end-user computing, privacy, and more) and that business units are in compliance with these policies and standards. Second, I looked to the CSO to help improve the quality of risk assessments, key risk indicators, and reporting related to information security. Finally, since the CRO office deals with highly sensitive information, I solicited the expert input from the CSO to ensure that effective information security controls were in place for the risk management systems, databases, and dashboard reporting.*"

2.11.4 Role Responsibilities

The primary responsibility of a CRO is to plan and implement a ERM framework for the company and oversee that it functions properly. We summarize the contents of such framework in the following table.

CRO Management Responsibilities	**Task brief description**
1.Compliance	The CRO has to identify the policies, standards and regulations with which the organization is required to comply.
2.Privacy	The CRO has to identify and establish the privacy requirements for the information flows in the company according to government regulations and laws and company's policy.
3.Finance Risk	The CRO has to evaluate financial risks that the company is exposed to such as credit, capital, investments, fraud and any other financial risks that may occur in a company's activities.
4.Market and Strategy Risk	The CRO has to evaluate potential impacts of business activities and events initiated by market activities and company's overall strategy.
5.Operational Risks	The CRO has to identify business process risks and analyse in what extent they may affect the business utilizing appropriate risk response measures.
Security Related Responsibilities	**Brief Description**
1.IT related Risks	The CRO has to create a risk assessment on the IT threats and vulnerabilities and provide to the CISO the hierarchy of the information that needs to be protected.
2.Information Security	The CRO has to provide the overall risk tolerance of the company to the CISO for him to develop controls that will mitigate the risks accordingly to the risk acceptance of the company.
3.Advisor	The CRO has to participate in the disaster recovery and business continuity plans providing valuable insight regarding the risk-profile of the company.
4.Risk Coordinator	The CRO is a coordinator of risk that receives valuable information from various departments regarding threats and risks and integrates them into a united framework providing risk profiles and the overall risk tolerance of the company in order to them to act and align accordingly.

Table 5: **CRO Responsibilities**

[24] World's first Chief Risk Officer

2.12 IT Security Auditor

2.12.1 Role Global definition

The IT Security Auditor as defined by business dictionary [25] is the person responsible for the "*Scrutiny of an organization's physical, financial and computer access control procedures and systems to determine its level of vulnerability to attacks or intrusions from unauthorized personnel or criminals.*"

2.12.2 Role analysis from a management perspective.

Information security auditor, is a role completely associated with information security. Hence we cant give a management overview. But instead we will give a brief overview of what an audit is as a process before we proceed investigating the IT security auditor role in the security section. First of all in a company there are many types of audits, such as financial audit, operational audit, IT audits and many others depending on the nature of the company and the industry it belongs too. Audit as a process itself is an evaluation of a system, a person , a company, a service or a product. An official definition of audit according to ITIL [8] is "*Audit, is a formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.*" Hence, an auditor is an evaluator! People's common conception of the term audit is the financial audit. Thus, the process of investigating the financial records of a company in order to validate, both quantitative and qualitative, the set of financial statements a company makes. In simple words it is an effective check of the, as it is known in the financial world "books" of the company. The financial audit is a process that a company has to conduct frequently at least once per year. That is due to the fact that it is enforced by law in most of the countries around the globe. That means that a financial audit is a legal requirement for every company, but it is a requirement that actually develops another requirement and a necessity of another type of audit; that of the information system audit. This association and combination of requirements derives because of the modern technology that companies tend to use. Since the so called book keeping is done by information systems and the financial audit can only provide validity of the books but not they way those records are stored, created and conducted. This actually means that there is a need to validate that there is no cheating, errors or manipulation in the book keeping process. Thus, altering records, percentages or any other kind of information manipulating the way the information system behaves. Therefore, there is a need to validate that the information systems, regarding at least to the financial processes, is behaving as it is supposed to and no signs of modifications or tampering with the data is present. That makes information systems audit a very important process and a law requirement as well. Usually companies run a broader audit, the information security audit which among others covers the requirement to examine the state of the IT systems and the way they behave and provides also other forms of valuable information toward the overall security state of a company. After all, an IT security audit is a tool in the hands of C-level executives which provides valuable results and inform them about the information security state of the company. Thus, of course also a way to check, control and not blindly trust the CISO with the security. Everyone makes mistakes! However, the IT security audit is a process from which the CISO has also to gain a lot, rather then just being evaluated, since it might uncover security issues that he might not

[25] http://www.businessdictionary.com/definition/security-audit.html#ixzz2QcgeQkhH

have identified and provide him suggestions on how to solve them. Our purpose is to investigate the role of the IT security auditor. Therefore, at this point we would like to give a small introduction to IT security audit. It is often the case that upper management wonders "why they need to perform security audits on a regular basis? " We already gave a partial answer to that question. Firstly, because it covers a legal requirement (book keeping) and secondly it evaluates the work of the CISO if of course there is one. However, that is just a small portion of the truth. There is often a misconception that having good security tools, such as firewalls and security controls, are enough and provide security. They couldn't be more wrong. Building a barricaded castle/fortress with firewalls and other security controls playing the role of the walls and watch towers aren't enough! In the absence of guards, the policies, frameworks and procedures in place provide little or no protection at all. Therefore, we need an IT security audit, because it will ensure that a company's security is in order and that IT security controls, processes and IT systems are functioning as intended. Moreover, it is a tool that will reveal possible compliance issues with various legislation requirements. Last but not least, but very important it will reveal flows, vulnerabilities and security gaps in the existing security of a company. In previous sections we already highlighted our view on visual representations. Therefore, you can see in figure 31 the road to IT security audit.

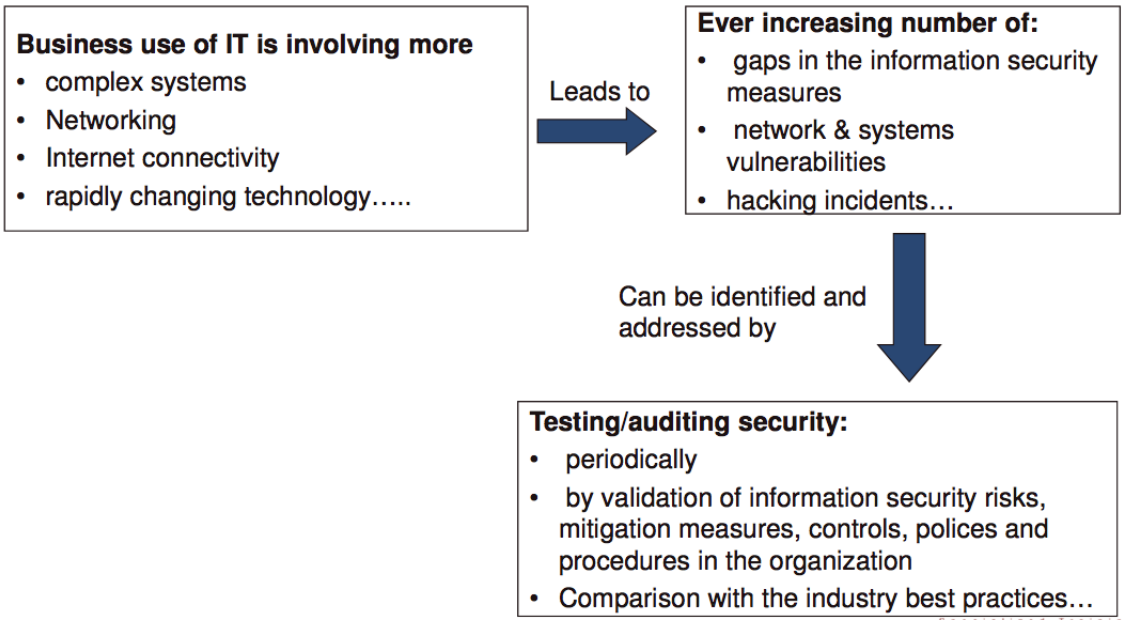


Figure 31: **Road to IT security audit picture extracted from [59]**

Now that we introduced the concept of IT security Audit we would like to give a small overview of its contents figure 32.

As you can see an overall IT security audit is divided to three core functions: a) the review of physical security, b) the review of technical security and c) the review of administrative security. As you can see each of these categories has a list of preventive and detective procedure/controls that have to be evaluated in an audit. We will discuss these core functions in the next section while we review the role of the It security auditor. Closing this section we gave a brief overview of IT security audit but we left the most

	Preventative	Detective
Physical	▪ locks and keys ▪ backup power ▪ biometric access controls ▪ site selection ▪ fire extinguishers	▪ motion detectors ▪ smoke and fire detectors ▪ CCTV monitors ▪ sensors and alarms
Technical	▪ authentication ▪ Firewalls & IPS ▪ anti-virus software ▪ encryption ▪ access control….. ▪ **Vulnerabilities assessment** ▪ **Diagnostic reviews…**	▪ audit trails ▪ intrusion detection ▪ **automated configuration monitoring** ▪ **penetration testing**
Administrative	▪ employment procedures ▪ supervision ▪ technical training ▪ separation of duties ▪ disaster recovery plans ▪ security awareness training ▪ **Diagnostic reviews…**	▪ security reviews and audits ▪ performance evaluations ▪ required vacations/rotation of duties ▪ **incident investigations**

Figure 32: **Contents of IT security audit picture extracted from [59]**

valuable part of the truth for the end. Hence, IT security audit [59] is the final step in implementing a company's defences! (figure 33)

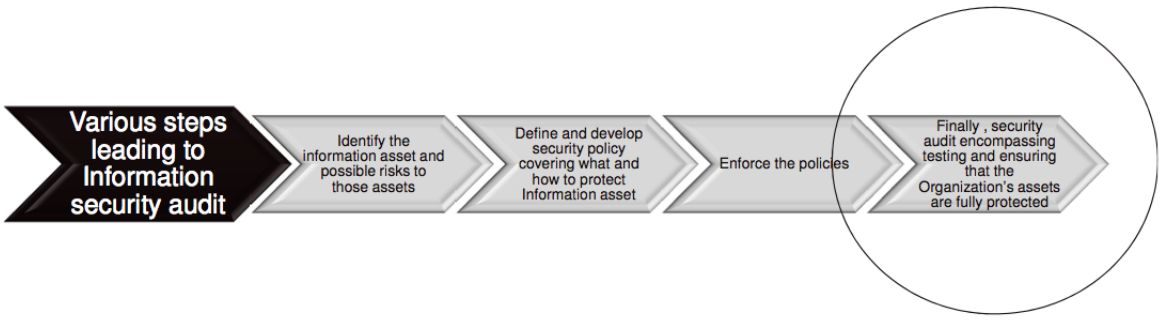


Figure 33: **The final step in organizing IT security. Picture extracted from [59]**

Therefore, there can't be a good security governance in a company if IT security audits aren't performed on regular basis and that is what makes the role of IT security auditor an important one.

2.12.3 Role analysis from a security perspective.

In the previous section we introduced the concept of IT security audit. Now it is time to proceed with the person in charge of this process. Thus, the IT security auditor. Hence the answer to the rhetorical question: "What does this role do? " is "He is the person or team of people that perform the IT security audit in a company." There are two categories that IT security audit is divided to: a)internal security audit and b)external security audit. The difference between them is actually the scope of the audit. While the nature and the process of the audit remains the same. Here, we raise an obvious question "Why do we have such separations and do we really need both audits?" The answer to this comes actually from the cost benefits approach companies take. An IT security audit is a timely and expensive process and the external third party doesn't have an insight of how things work and would require a costly pre-audit process before he could proceed with the audit process. Such a pre-audit process could be questionnaires, gathering of critical information, analysing the company's structure business units and processes and gathering all the necessary data for an audit process. Which in terms of industry equals to time and it is commonly known that time equals money. Therefore, companies resolve this issue by employing an IT security auditor, who will actually serve a double purpose role. He will be the person in charge to prepare the company for an external IT security audit. That of course will lead to lowering the costs of the external audit as well as providing valuable insights to the external auditors upon request. The second big advantage of having an internal auditor is that he will conduct internal audits which are less formal and serve as proactive measures in comparison to the external audit which is a formal process and a regulations requirement. In this aspect internal security audits [60] are extremely useful since they evaluate the state of information security and identify discrepancies that can be rectified before they can become serious issues. Although internal audits are as we said extremely useful, the internal auditor may have a conflict of interest [60], since he is an employee of the company and he will be a person who evaluates the work of a CISO. Therefore, company's politics may play a role and thus the reason that an external IT security audit is in place and mandatory to assure that the IT Security auditor will be a person who doesn't have any bias of internal politics or system ownership [61]. But rather will be a "righteous judge" without any personal vested interest in the findings of the audit process. At this point we have explained the differences between the internal and external IT security audits. Therefore we will analyse the role of the IT security auditor when employed by the company. Thus, the preparation he has to make before an internal or external audit is taking place. Furthermore, we will explain the process of the audit itself and what the IT security auditor does.

Internal Security audit (Pre-audit Phase)

When it comes to information security all information security professionals know that the way is to work smart, not hard [62] and in this case working smart means to allocate all the necessary resources in order to prepare best for the audit. Assuring that the audit wont end up being an ordeal for the company. This means that the IT security auditor has to perform a series of tasks listed in table 6 below in order to achieve the desired outcome.

IT security auditor pre-audit tasks	**Task brief description**
1.Previous audits.	The IT security auditor has to gather the previous audit reports that have been conducted and provide documented steps that were taken to resolve the possible findings of those audits.
2.Technical description.	The IT security auditor has to prepare the technical description of the host, meaning a detailed review of the hardware and software the company is using.
3.Security incidents.	The IT security auditor has to prepare detailed documented analysis of security incidents that occur and the steps taken to resolve them and prevent them from occurring again.
4.Company's overview.	The IT security auditor has to prepare a detailed overview of the company's business units, processes and procedures as well as goals, mission and objectives.
5.Information audit assets.	The IT security auditor has to prepare an analysis of the critical information (data) and its assets (information processes) and their value to the company.
6.Security policy and procedures documents.	The IT security auditor has to provide up to date security policies and various of procedure documents such as BCP, Incidents Management policy, DRP, data policies, etc.
7.Company's physical infrastructure.	The IT security auditor has to prepare a detailed map of company's infrastructure regarding physical security. Such as locations of servers, routers, firewalls as well as the controls that handle the physical access to such devices.
8.Network infrastructure.	The IT security auditor has to prepare a detailed network diagram.
9.Security controls.	The IT security auditor has to prepare a detailed overview of hardware and software security controls that are in place in the company.

Table 6: **Pre-audit series of tasks**

The mentioned above tasks can vary in different companies and are generated by the author from literature and industrial reviews of the following documents [59], [60], [61], [62], [63], [64].

IT Security audit process

During the years people developed a misconception to think of an IT security audit process as a reactive approach. That means that the IT security audit was conducted when a security incident occurred in order to find the root of the problem and its trigger. Thus people saw an IT security auditor as "a soldier who enters the battlefield after the war is over and attacks the wounded." However, that might still be the understanding and somewhat true, but the industrial standards and government regulations pose the IT security audit as a repetitive proactive measure. Something that aligns with the global understanding of information security that it is a continuous process, so should be the IT security audit. There are various frameworks that an IT security auditor can use to conduct an audit such frameworks could be the followings:

1. ISO/IEC 27001:2005 [6] and its adoptions always including the plan-do-check-act model figure 34.

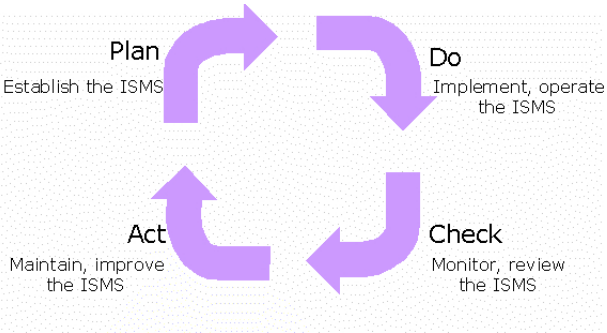


Figure 34: **PDCA model**

2. The Security by Consensus (SBC) model developed by prof. Kowalski [65] figure 35 which was mapped to the ISO 17799 by Tarimo [66] figure 36 from where it is easy to understand which component of the model a company is strong or weak and take appropriate measures to cover the identified weaknesses.

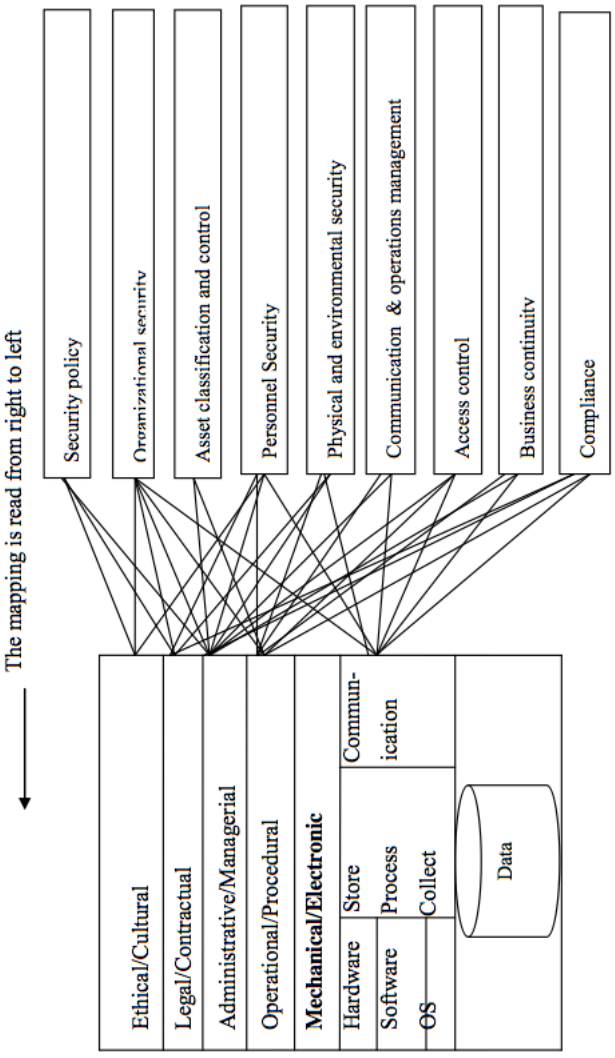


Figure 35: **SBC model**

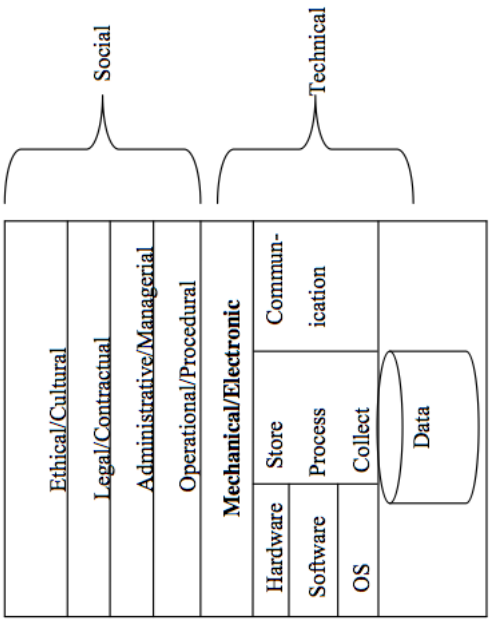


Figure 36: **SBC mapped to ISO 17799 model**

3. ISACA's COBIT and various of others ISACA's frameworks and guidelines listed in figure 37 bellow.

S1-Audit Charter - the purpose of this IS auditing standard is to establish and provide guidance regarding the audit charter used during the audit process

S2 – Independence - the purpose of this IS auditing standard is to establish standards and guidance on independence during the audit process

S3 – Professional Ethics and Standards - this standard is about professional ethics where auditor needs to stick to certain defined core code of ethics

S4 – Competence - the purpose of this IS auditing standard is to establish and provide guidance so the IS auditor is required to achieve and maintain professional competence

S5 – Planning - this part of the standard is to give guidance on effective planning to conduct information systems audit

S6 – Performance of Audit Work - this provide guidance about the audit work

S7 – Reporting - the purpose of this IS auditing standard is to establish and provide guidance on reporting so that IS auditor can fulfill this responsibility.

S8 – Follow-Up Activities - the purpose of this IS auditing standard is to establish standards and provide guidance regarding follow-up activities undertaken during an IS audit process.

S9 – Irregularities and Illegal Acts - the purpose of this standard is to establish and provide guidance on irregularities and illegal acts that the IS auditor should consider during the audit process.

S10 – IT Governance - it is to establish and provide guidance on IT governance areas that the IS auditor needs to consider during the audit process.

S11 – Use of Risk Assessment in Audit Planning - the purpose of this standard is to establish standards and provide guidance regarding the use of risk assessment in audit planning

S12 – Audit Materiality - the purpose of this IS auditing standard is to establish and provide guidance on the concept of audit materiality and its relationship with audit risk.

S13 – Using the Work of Other Experts - the purpose of this IS auditing standard is to establish and provide guidance to the IS auditor who uses the work of other experts on an audit.

S14 – Audit Evidence - the purpose of this standard is to establish standards and provide guidance on what constitutes audit evidence, and the quality and quantity of audit evidence to be obtained by the IS auditor.

Figure 37: **ISACAS models Picture extracted from [67]**

4. And various other frameworks, standards that can be used for information security audit.

However, in a more broad and independent approach from frameworks and standards a relative study [62] provides the following steps and procedures listed in figure 38 where you can see a seven step auditing plan and the deliverables of any audit process which are: the vulnerability report, the threat/ Risk assessment report and the audit report. Things that are expected from an IT security auditor to conduct and deliver.

In order to deliver such reports the IT security auditor has to conduct a series of tests on five core domains of a company listed in figure 39, out of which the most frequent and most noticeable tests and reviews are listed and briefly explained in table 7.

IT security auditor audit areas of test tasks	Task brief description
1.System architecture design.	The IT security auditor has to analyse the network and systems architecture from a security, integrity and availability perspective.
2.Application security.	The IT security auditor has to review the security settings and configurations of the applications as well as their design and state and recommend updates or patches to solve any potential issues.
3.Databases.	The IT security auditor has to review the security settings and configurations of the databases and the database servers in order to ensure that the data stored in the databases are protected.
4.Network/firewall vulnerability assessment.	The IT security auditor has to run network penetration tests to identify weaknesses and holes in the network's defences.
5.Web based applications and web servers.	The IT security auditor has to conduct tests to identify security holes of web applications and web servers.
6.Security policy and procedures documents.	The IT security auditor has to review the security policies and procedures documents and ensure that they comply with industrial frameworks and standards, hence they comply with law regulations.
7.Company's physical infrastructure.	The IT security auditor has to review the physical security controls that are in place are ensuring the protection of the company's assets.
8.Operating systems.	The IT security auditor has to check the operating systems for malware and assure that critical software updates are patched.
9.Security controls.	The IT security auditor has to review and assess the hardware and software security controls that are in place in the company.
10.Routers, switches and firewalls.	The IT security auditor has to review and assess security settings and configurations of firewalls, routers and switches to ensure that they aren't vulnerable and open to hacking attacks.
11.Wireless Networks.	The IT security auditor has to review the wireless network security and ensure that no unauthorized wireless access point are in place.

Table 7: **Most frequent IT security audit areas of tests**

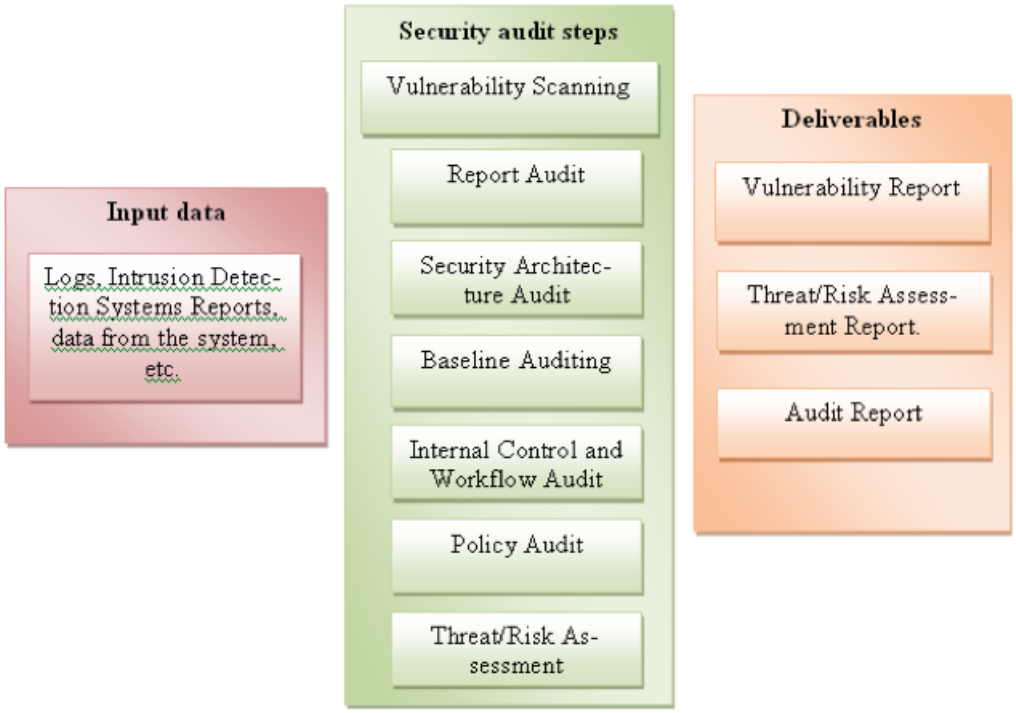


Figure 38: **Audit Process. Picture extracted from [62]**

2.12.4 Role Responsibilities

Summarizing, the IT security auditor is accountable for:

1. The verification of the effectiveness of the company's IT security.

2. Preparing the ground for the IT security audit process to kick off.

3. Evaluation of the company's financial and IT systems identifying any possible frauds, mismanagement, misuse, dysfunction of resources, procedures and controls.

4. Evaluation of effectiveness, efficiency and most importantly compliance of company's security processes and procedures with global accepted best practices and government laws and regulations.

5. Propose solutions to resolve the potential issues that the audit findings might reveal.

Last but not least we would like to recall a famous quote about auditors that totally reflects our perspective and understanding of the role of the IT security auditor. "The auditor is a watchdog and not a bloodhound![26]"

[26]Lord Justice Topes

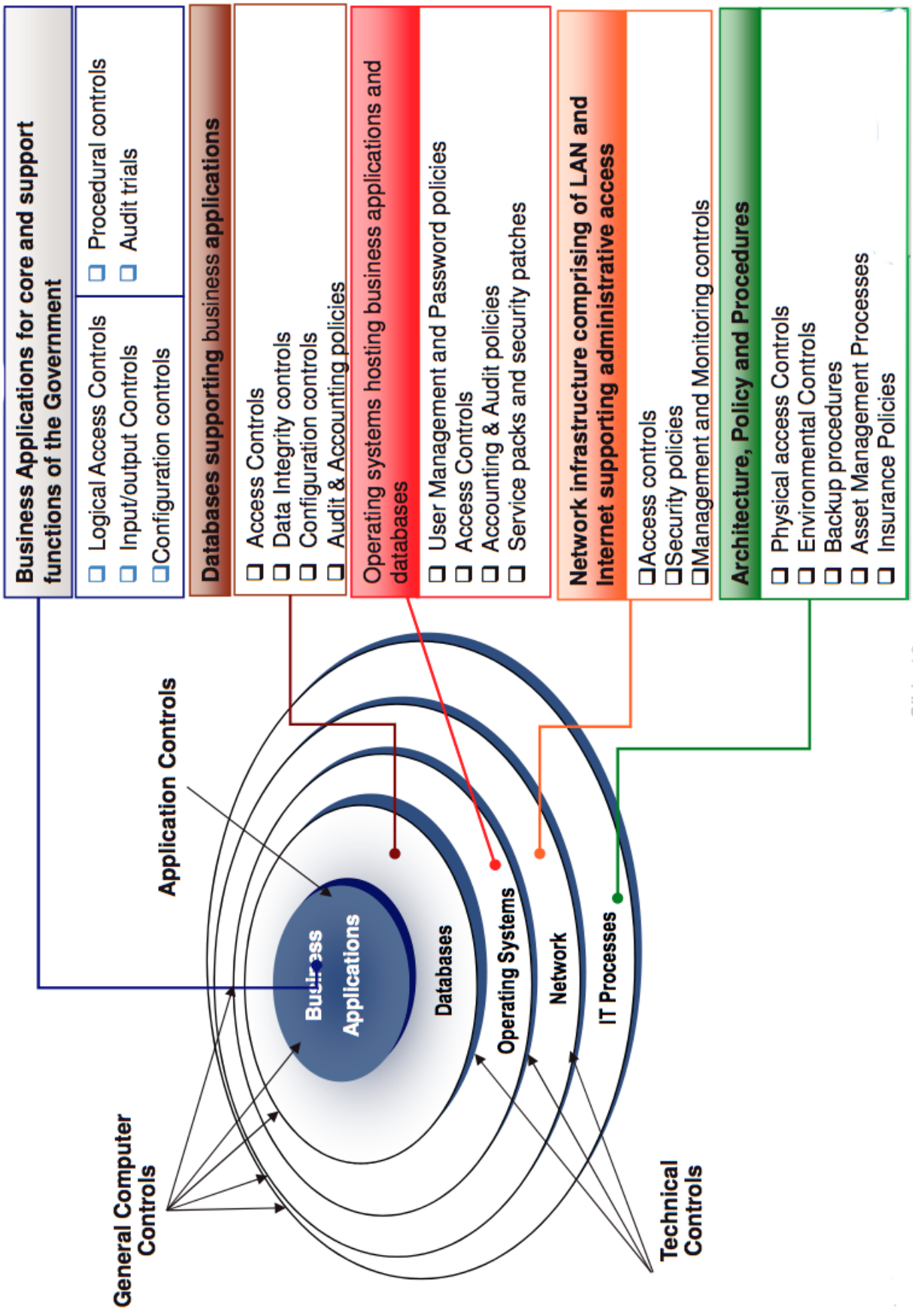


Figure 39: **IT security audit core areas. Picture extracted from [59]**

2.13 Supervisors & Manager & Directors

2.13.1 Role Global definition

There are many definitions of the roles of supervisors, managers and directors we will list a set of definitions by F. John Reh [27] as he defined them in the about.com management.[28]

Supervisor: "*For many people, their first management level job is as a supervisor. The supervisor is a first level management job. This individual is responsible for a small group of people, usually doing the same job or very similar jobs. Typically the supervisor has significant experience doing the work of the individuals they supervise.*"

Manager: "*A manager may be a first level manager who supervises employees directly or a second level manager who manages supervisors. The size of the company usually determines which. The duties and responsibilities of a first line manager are similar to those of a supervisor although the manager generally has more personnel responsibility, more HR responsibility, and more discretion. He or she usually supervises a small group of employees doing the same or similar work.*"

Directors: "*A director is a senior management position responsible for the strategic and tactical management of a significant piece of the company Directors typically manage a few subordinate managers. Within their area of responsibility they generally have wide latitude and are expected to meet broad goals. Normally they have P & L responsibility and have hiring authority within their budget.*"

2.13.2 Role analysis from a management perspective.

Nowadays, every company consists of supervisors, managers and (project managers, senior managers, middle managers etc.) directors who assist the C-level executives in the governance and daily operations of a company. Due to their nature these three roles can be identified in various departments of a company with different delegation and nature of responsibilities. Hence, we cannot provide a detailed overview of their responsibilities with respect to management approach, since they vary and depend on the department and industry they belong to. However the reason we group these roles is of their relevance, hierarchical a supervisor reports to one or several managers and they report to one or several directors; Besides the chain of command they all manage a group of people with the size depending on the role and its nature. We will refer to these three individual roles as "line managers". Thus because if an employee calls someone as "boss" he refers to a line manager that could be any of the three roles.

2.13.3 Role analysis from a security perspective.

The fact that line managers oversee and are on a daily basis in touch with many employees put them in a key position to safeguard and promote information security. In academia and standards like NIST, ISO/IEC, COBIT, ITIL there is a generic and short review of the roles and responsibilities towards information security if any. Therefore, we conduct an industrial review of various of information security policies documents and

[27] John Reh is a senior business executive whose broad management experience encompasses managing projects up to $125 million and business units including up to 200-plus people. A published author, most recently as a contributing author to Business: The Ultimate Resource

[28] http://management.about.com/od/begintomanage/a/Management-Levels.htm

generate a specific set of security responsibilities regarding line managers.

2.13.4 Role Responsibilities

Please note that this set of responsibilities is generated from a sample of 40 different policies. Hence, we provide our findings in respect to this sample and we acknowledge that this is a case of Hasty Generalization. However, in our humble opinion the proposed set of responsibilities aligns well with Information Security Management frameworks, guidelines and complies with our obtained knowledge during our studies in Information Security Management at GUC. We list our findings bellow:

1. The line managers have to conform to and implement security policies and procedures in the domain of their responsibility.

2. The line managers have to monitor and identify any non-compliance issues with the security policies and procedures in their domain of responsibility and take appropriate corrective steps.

3. The line managers have to develop and build a trust culture and promote a security culture encouraging the staff to report any compliance issues or security incidents that come to their attention.

4. The line managers have to ensure that the employees acknowledge, understand and follow the security policies and procedures in the domain of their responsibility.

5. The line managers ought to notify the employees in his domain about changes in the security policy or procedures as well as explain and ensure that the employees understand their responsibilities towards information security procedures or requirements and the absolute need to comply with them.

6. The line managers are responsible in identifying the weaknesses of the employees in their domain in respect to compliance with the information security policies and procedures and ensure that necessary guidance and training is provided to the employees.

Closing this section we can see that line managers play a vital role in the safeguarding, promoting and creating an information security aware environment. Hence, they are a vital part of an effective information security management system/framework.

2.14 CMO

2.14.1 Role Global definition

Chief marketing officer (CMO) as defined in business dictionary[29] is: "*The company executive responsible for corporate branding, advertising, marketing channels, customer outreach and all other marketing aspects. The CMO is considered part of the top management tier with responsibilities which generally cross all company product lines and geographic regions.*"

2.14.2 Role analysis from a management perspective.

Chief marketing officer (CMO). The key word of this C-level executive is marketing. Hence we can't proceed to our review of the role without first clearly introducing the concept of marketing. Marketing as defined by Philip Kotler [68] is " *a societal process by which individuals and groups obtain what they need and what through creating, offering and freely exchanging products and services of value with others.*" The role of CMO goes way back in history and is the natural evolution of the chief advertisement officer. A chief advertisement officer was the person responsible for creating the advertisements and advertisement campaigns. He was the brand developer and protector [69], but the rapid advance of technology, business globalization, market fragmentation and the inefficiency of the traditional marketing methods [70] demanded a more complex role. Thus, the death of the chief advertisement officer [69] and the rise of the modern version of the role known now as CMO. However, the chief advertisement officer's functions have been preserved over time and still remain as a part of the modern CMO duties. The digital era we live in that has evolved during the last decade brought a network-driven empowerment of individuals [71]. This network driven empowerment gave customers tremendous power and raised their needs, expectations and means of evaluating products and services. Thus , creating one of the core challenges for today's CMO, that to identify the customer, satisfy them and keep them for a long term period. The network-driven empowerment disruption changed the world of marketing. Marketing will never be the same! The role of the modern CMO is to own this disruption otherwise, woe to the CMO [71]. The CMO is a complexed role. Thus, because the way he brings value to a company differs from industry to industry. Hence, there are various responsibilities and job descriptions of the CMO role [72]. This is due to the fact that there are three different models of the CMO that could fit a company based on its nature and its needs and requirements. In Harvard's study [72] this categorization is explained in detail. We list below the categorizations of Harward's study in a short context. Those three categories are as follow:

1. **VP of Marketing Services**. "*A vice president of marketing services operates a cost center made up of marketing professionals. Business unit managers have profit-and-loss accountability and use the marketing expertise in this "center of excellence" as they deem necessary.*"

2. **Classic CMO**. "*In an organization not led by marketing, the classic CMO role is to ensure that longer- term marketing and brand-building considerations are part of the top management team's deliberations. The CMO must monitor the evolving consumer land-*

[29] http://www.businessdictionary.com/definition/chief-marketing-officer-CMO.html

scape, represent the voice of the customer, and act as the cata- lyst to develop and then interpret the consumer insights that can produce new product or service development."

3. **Super-CMO.** " *The classic CMO who can prove himself or herself by gradually winning internal support and earning the trust of the CEO can become a "super-CMO," with greatly expanded authority. The super-CMO is a senior and seasoned marketing executive, widely respected both inside and outside the company. This executive has typically been a general manager or even a CEO, can certainly talk the language of business strategy and finance, and has the stature to direct global brand strategy. He or she usually has authority over the company's marketing budget.*"

As you can clearly understand there is no "one size fits all" role of CMO. However, in the various studies we reviewed in our research of the role, [69], [70], [71], [72], [73], [74], [75], [76], we identified a number of shared attributes among those studies of CMO. We summarized these findings and list them bellow:

1. **Public relations & events.** The CMO has the responsibility to promote the company and manage the flow of information from the company to the public. The scope of public relation is to build relationships and ensure exposition of the company to the company's audience. Where audience is interpretative as mass media, investors, customers, employees, partners and other possible stakeholders. The CMO is responsible for the creation of appealing and successful promoting events of the company. Whether they are the company's presentations of new products or services, conferences or any other events it is the CMO's responsibility to identify the companies audience and create appropriate attractive events.

2. **Marketing Services** This is the, preserved in time, activity that the modern CMO inherits from his predecessors. In this area, the CMO has to oversee the development of advertisement campaigns, the protection and development of the company's brand name and he has to create value for customers as individuals [74]. The CMO is responsible for overseeing the development of marketing services such as complain handling, service recovery, delivery systems, pricing, communications with customers services, balancing market demands with capacity and various other marketing services that might derive based on the nature of and the industry a company belongs too.

3. **Growth Manager** The modern transformation of the CMO role to that of a Growth Manager is a matter of time. The CMO is responsible for the market research and analysis. He has to familiarise himself with the latest trends, modern technology and market globalization in order to explore market opportunities and seize them when they are beneficial for the company. He is responsible for analysing the customers feedback and forecasts their new expectations and demands to ensure that the company is focused on meeting them. This factor will initially protect the market share of the company and will be the basis for further "market attacking" that will lead to a bigger market share and additional recruitment of customers. That will eventually

produce bigger revenue for the company. Last but not least he has to preserve the company's brand name. Hence to maintain the existing fan base of the company and to explore means that will contribute to its expansion. However to implement such a requirement the CMO has to be a strong leader and corporate advisor.

4. **Leader and Corporate advisor** The CMO has to possess strong analytical skills and out of the box thinking in order to contribute to the development of a robust business strategy and vision that will ensure a good marketing policy and development in the company. He has to be a cross-function person since marketing is the same as security, everyone plays a role in it one way or another. Thus he has to build relationships with the business units and line managers as well as with the rest of the C-level executives and assure that everyone understands the value of what efficient marketing brings to the table. Besides the strong analytical skills he has to possess he should be also a strong leader that will provide valuable insight and inspiration both to the CEO and the board of directors, but these leading skills don't stop just on the C-suit management but due to the fact of market globalisation he has to serve as a global marketing ambassador and lead the marketing department and its global branches if any.

5. **Marketing ROI** The last piece that completes the overview of the CMO role from a management perspective is the most challenging part of this role. The CMO has to become the CFOs closest friend, since he is a part of the C-level executives he has to speak the same language as them. That of numerical numbers. There is no hiding behind the hardcore numbers. Although the way of measuring marketing success is a very hard process and varies in different industries, the CMO has to be able to perform a return on the investment (ROI) analysis and forecast and provide proof of success or failure in terms of numbers to the CEO and the board of directors. This requirement makes an absolute requirement for the CMO to be a good forecaster and a person who can make good estimations based on uses cases or scenario development which are key tools in a CMO's arsenal. Not only to estimate the initial investments but to also use them as self evaluation and guidelines through the marketing process.

Closing this section we would like to refer to two interesting quotes we read in [76] about marketing. "*Marketing is unique from other functions the last mile of marketing occurs in the mind of the customer. That isn't a controllable environment; it relies on psychology;*" "*The role of Marketing is to identify revenue opportunities and nurture those opportunities.*"

2.14.3 Role analysis from a security perspective.

A CMO and information security share a mutual beneficial relationship. The CMO is one of the roles who can take full advantage of the good information security procedures of a company and turned it into a value producer for the company, Meanwhile he relies on information security to safeguard marketing services and procedures. But lets see how all these come to life. Starting with the fact of creating value for the company using and promoting companies information security. In the digitised era we live in, online transactions and recruitment of personal data happen on daily basis. Customers trust

companies to safeguard their personal data when they will be using their services. Hence, customers concerns about information security are raise daily. A fact also confirmed by the finding of a relevant study "secure the trust of your brand" [77]. In fact the key findings of the study indicate that:

1. *U.S. consumers polled were most concerned with identity theftâĂŤeven more so than terrorist threats and other personal safety issues. Conversely, European consumers cited Internet transaction security as their biggest information-based worry.*

2. *Computer security breaches, such as viruses and spy ware, are clearly a unifying force in both geographies: two thirds of consumers across the U.S. and Europe have been victims of these types of breaches.*

   More and more customer concerns have been raised during the passed few years due to major security incidents hitting the media, leading to a huge demand for information security from customers. As the fundamental law of marketing indicates " The customer is always right " the companies tend to cover the customers needs by focusing on information security. That brings us to another key finding of the same study [77].

3. *There's room for companies to literally make a name for themselves with robust security policies and response strategies. When asked an open-ended question about their "most trusted" type of industry or specific company in terms of security, consumers' answers varied widely, indicating an opportunity for companies and industries to further build brand trust. Banking was the industry most often named by respondents as "most trusted" for protecting its customers' security, and Symantec/Norton was the company/brand most often named by respondents, with McAfee and Microsoft tied for second.*

which indicates how a CMO can use information Security to create value. The CMO can use information security to promote the company's brand and indicate that the company takes in high consideration information security and data privacy and has all the necessary security controls to safeguard the private information of its customers. Thus, the CMO will develop and add value to the company's brand name building a security reputation for the company. Which will be translated into a growth of their customer base and revenue. Hence, information security assists the CMO in marketing strategies, services and development. But is it the only way that information security interacts with the CMO? As we discussed its a mutual relationship. Therefore, by promoting information security the CMO enhances the need of its constant development and leads the way into the company's strategy towards information security. Since in taking such a course, of promoting your security, you must assure that the raised expectations by the customers are met. Thus, means more investment in the constant development of information security. That of course is providing you a brand name itself as indicated in the third finding of the study. However this is not the end! Information security assists the CMO in other ways as well. Such are that it safeguards the company's reputation, the Q-terms financial results, the launch of new products, pricing strategy and various of other forms of information flows that could harm both the company and the marketing department

and its processes. As a result, one of the key responsibilities of the CMO as well as other managers is to ensure that the staff of his department have a security awareness culture and adhere and implement the established security policies and procedures. But that is not the last part of the CMO role when it comes to information security. Agatha Christie wrote: " When large sums of money are concerned, it is advisable to trust nobody!" That statement is something that in our modern world companies face from customers on a daily basis and specially when there is a major security breach of data. We saw recently the estimation of billion dollar losses from a recent security breach of the Sony playstation network which left Sony to handle angry and disappointed customers. Here comes the role of CMO to make a difference! The way a company treats a security incident when one occurs and how they communicate it among the customers, business partners and public makes a significant difference in the company's losses. After all, a negative publicity is still publicity that a good and well prepared CMO can make the company benefit from this with the correct handling. However according to another finding of the [77] study most CMO aren't sufficiently prepared to handle such situations. Something that has a direct affect on the stock performance of the company and they estimate that a loss from 0.63 to 2.10 % value in the stock price when a breach hits the media. Thus, the CMO responsibility to assist the CISO in training a spokesman in the crisis team if any and assure that any security incident or disaster is handled appropriately protecting the brand name of the company and the company's reputation and interests in the media coverage and the public.

2.14.4 Role Responsibilities

Now that we have given an overview of the CMOs role it is time to summarize the role's responsibilities. We list them in table 8 listed bellow.

CMO Management Responsibilities	**Task brief description**
1.Public relations and events.	The CMO has the responsibility to promote the company and manage the flow of information from the company to the public.
2.Marketing Services	The CMO has to oversee the development of advertisement campaigns, the protection and development of company's brand name, he has to create value for customers as individuals.
3.Growth Manager	The CMO is responsible for the market research and analysis. He has to familiarise himself with the latest trends, modern technology and market globalization in order to explore market opportunities and seize them when they are beneficial for the company.
4.Leader and Corporate advisor	The CMO has to possess strong analytical skills and out of the box thinking in order to contribute to the development of a robust business strategy, vision that will ensure a good marketing policy and development in the company.
5.Marketing ROI	The CMO has to be able to perform a return on the investment (ROI) analysis and forecast and provide proof of success or failure in terms of numbers to the CEO and the board of directors.
Security Related Responsibilities	**Brief Description**
1.Value Creator	The CMO has to use information security to promote the company's solid approach to information security and data privacy and develop or expand the brand name and reputation of the company.
2.Information flow keeper	The CMO has to ensure that appropriate measures and controls are taken to protect information leakage about marketing events, procedures, services that could harm and affect the company.
3.Key Media Handling	The CMO has to be prepared to handle the media appropriately and in advantage of the company's interests when a security breach occurs.

Table 8: **CMO Responsibilities**

2.15 Chief R & D officer

2.15.1 Role Global definition

Chief R& D officer CRDO as defined by investopedia is the *leader of Investigative activities that a business chooses to conduct with the intention of making a discovery that can either lead to the development of new products or procedures, or to improvement of existing products or procedures. Research and development is one of the means by which business can experience future growth by developing new products or processes to improve and expand their operations.*

2.15.2 Role analysis from a management perspective.

The role of the R/D leader has been intensively studied for many years. The role that once represented a gate keeper who was the primary reservoir of ideas for new services and products and a first-line supervisor in a research group [78], has nowadays developed into a role of a business leader, a person who is capable to manage and lead internal teams, collaborate with external partners, has an understanding of the market and the customers orientation with the ultimate goal to bring innovation in the company and create valuable intellectual property [79]. The role of the modern CRDO requires a vast understanding of business strategy and business goals combined with a solid academic background. In other words the modern CRDO needs to be a brilliant scientist that has developed managers skills. Thus the hardest demand of this position, is in fact that the CRDO has to understand that its no longer just scientific research but rather a successful product development, placing the customers at the heart of the business [79]. The CRDO has to secure the business future of his company by developing and releasing products that would hit the market and preserve and grow the market share of the company. In a relative study [80] they categorize the key success factors for a successful R/D Manager which according to them are:

1. **Predominance in Competition**
   Predominance in competition means to have something special that competitors cannot create.or copy easily.
2. **Evaluation** *Impartial evaluation is a catalyst for fair competition and proper cooperation, which will result in effective distribution of research funds.*
3. **Organizational Economy** *R&D consumes a company's precious resources (personnel, capital and equipment), therefore improving the efficiency of research is an all- important factor.*

Thus, in other words the fact is that a CRDO has to be an R&D promoter. He has to be able to speak the language of the other C-level executives and have the required competence to sell his ideas to them in order to receive proper financial support for the R&D department. He is the person responsible for running the department and overseeing the research-development of new products and ensuring value creation for the company. A value that is translated to innovation and intellectual property. Innovation is the alpha and the omega of the CRDO role. We would like to recall two statements of United states Presidents about innovation.

"We need to build a future in which our factories and workers are busy manufacturing the high-tech products that will define the century... Doing that starts with continuing investment in the basic science and engineering research and technology development from which new products, new businesses, and even new industries are formed." [30]
"America leads the world because of our system of private enterprise and a system that encourages innovation. And it's important that we keep it that way. See, I think the proper role for government is ... to create an environment in which the entrepreneurial spirit flourishes...the Government can be a vital part of providing the research that will allow for America to stay on the leading edge of technology...I think we ought to encourage private sector companies to do the same, invest in research."[31]

As you can see innovation is the future not only of a company but also at a countries level. Thus, the need of an excellent CRDO, who will play an [79] integral role in defining and developing strategy, combine strategic planning and execution skills and be able to deliver projects and products that will hit the market. To put it in other words: "*to crystallize ideas and make them reality* " [79] . Summarizing the CRDO can be found in various industries with different requirements. However, in a broader approach we list five of the core properties that follow the CRDO role in the modern industry. The CRDO has to:

1. Be a great Scientist.

2. Be an innovator, bring new ideas to the table.

3. Oversee the proper function of the R&D department ensuring the financial support for the projects.

4. Understand the market and the customers.

5. Be a safeguard and developer of the company's intellectual property.

2.15.3 Role analysis from a security perspective.

A CRDO contribution to the overall information security of a company is not bigger than any general manager, director, supervisor as discussed in the homonymous chapter. Thus of course in the case that the R&D department is not dedicated to information security development. However, information security plays a vital role in safeguarding the intellectual property and its development. In the modern world tremendous investments are made by companies to research and develop with the purpose to achieve benefits of intellectual property and eventually see it develop into a product that will hit the shelves. In this rally, of patent claims and intellectual property corporate espionage is remarkably blooming. Here is where information security comes to play the role of the protector. The guardian of the intellectual property, hence the guardian of the company's investment. Information security protects the intellectual property dealing both with the technical solve risks and the human factor risks a company faces. Which are also the risks that the R&D department is facing. In the value chain of intellectual property development

[30] President Barack Obama, February 2012
[31] President George W. Bush, April 2004

there are many players. Hence it is exposed to the most challenging threat. Thus, of an insider, here we would like to note that we don't neglect the technical solve risks but it is common practice that company's spend a lot of money to protect themselves from an outside attacker but usually fail to mitigate the insider threat. Where an insider is a human factor risk, whether this is a human error or a sophisticated pre-designed attack, it is a high risks on the company's investment. In a relevant study about internal crime and recommendations conducted by the author under the supervision of Professor Dr. Bernhard M. Hämmerli ,as a partial requirement for a GUC course, we demonstrated the vital role that information security plays in handling the insider threat. We list below the findings of that study since they play a crucial role in protecting the process and findings of the R&D department which are critical for every company.

Internal Crime and recommendations study findings:

1. **Educate, inform and keep the awareness high in the staff.**
   The board should be providing specific training in detecting manipulative attempts to all customer facing staff. Warning all staff to be alert to anyone asking for sensitive or restricted information. Being alert to all unknown enquirers who try to extract information in a rush, with intimidation, stressing authority or refusing to give contact details. Encouraging managers to be alert to individuals who are excessively negative about the organisation or their work. Establishing a formal grievance procedure for staff to vent their feelings. Setting up an easy and confidential system for staff to report any abnormal behaviour from their colleagues. Educating is critical also performing security training and awareness. Educating third party assets those outside your organisation.

2. **Ensure the presence of security controls.**
   Security controls are the mechanisms that ensure our security . Security controls such as:

   - *Encryption of data.*
   - *Access controls.*
   - *Minimum privileges.*
   - *Monitoring, auditing and reporting.*
   - *Enforcing baseline security policies and procedures.*
   - *Extending traditional policy and guidance.*
   - *Conducting ongoing personnel checks.*
   - *Implementing focused risk assessments.*

   Should be taken into a serious consideration when implementing the security controls and should be deployed when possible. In addition to these measures we should make sure that, *when employment is terminated for whatever reason ensuring that all access to systems, sites and information is ceased. And that the information should be backup and a secure copy should be kept in another location. And also we must ensure real understanding of the reasons for security controls.*

3. **Ensure that the staff are aware of their responsibilities.**
   The board of directors and the upper management have to make sure that the staff are aware of the procedures,policies and regulations of the company/organization

and that penalties will occur if they wont follow them. Few examples of such policies and regulations are listed bellow. The employees should:

- *Only use equipment for which they have been granted authorization.*
- *Not leave computer equipment in a parked car or in an unsecured location where it might be stolen.*
- *Follow established procedures when removing equipment from premises. This usually requires a property pass.*
- *Not install or use unauthorized software or hardware on the network, including personal laptop computers, pocket computers, or personal digital assistants and network enabled cellular phones, except as expressly authorized.*
- *Not alter the configuration, including installing software or peripherals, on government equipment unless authorized.*
- *Notify management before relocating computing resources.*

4. **Take appropriate physical security measures.**
   Physical security shouldn't be neglected since its a part of security procedure and part of our defence. The company/organization should: When possible, use physical locking devices for every laptop. Have a list of individuals who are authorized to access the servers should be re-verified as much as possible. Changing key codes on doors frequently and performing revocation of ID badges at frequent intervals.

5. **Personal proposal.**
   Thus every organization/company should pay a lot of attention to the cultural background of their employees investing towards knowing them better and understanding their needs, beliefs and traditions and providing a secure and happy environment to work in. Building a genuine relationship between the company/organization and the employees which will build trust and respect between them. This way the risk of the insider will be mitigated. After all the best security measure is not the one deployed by a policy or a control but by gaining and investing in a personal trust and mutual respect. Human interactions are way more important than any money or controls. If you manage to show loyalty to your employees they will follow you and trust you. Its the same as genuine leaders that people follow through the ages. The same approach should be obtained in this environment too or at least its our recommendation and belief.

2.15.4 Role Responsibilities

The CRDO has to:

1. Be a great Scientist.

2. Be an innovator, bring new ideas to the table.

3. Oversee the proper function of the R&D department ensuring the financial support for the projects.

4. Understand the market and the customers.

5. Be a safeguard and developer of the company's intellectual property.
6. Has to acknowledge and follow the security responsibilities of a supervisor, manager, director as they are described in the homonymous section of this thesis.
7. On the other hand, information security has to protect the R&D department and the intellectual property from human factor risks as well as technical solve risks.

2.16 CRM Director

2.16.1 Role Global definition

A customer relationship management Director as defined by business dictionary [32] is a person responsible for overseeing the development of *A computerized system for identifying, targeting, acquiring, and retaining the best mix of customers. Customer relationship management helps in profiling prospects, understanding their needs, and in building relationships with them by providing the most suitable products and enhanced customer service. It integrates back and front office systems to create a database of customer contacts, purchases, and technical support, among other things. This database helps the company in presenting a unified face to its customers, and improve the quality of the relationship, while enabling customers to manage some information on their own.*

2.16.2 Role analysis from a management perspective.

The role of CRM Director, also known as chief customer relationship management officer, is to lead the design, implementation and integration of a customer relationship management framework/system in a company. But what is CRM ? There are many definitions of a CRM over the years, in a relative study [81] about CRM they gather the various definitions and defined CRM as follows: *Customer Relationship Management is a comprehensive strategy and process of acquiring, retaining, and partnering with selective customers to create superior value for the company and the customer. It involves the integration of marketing, sales, customer service, and the supply-chain functions of the organization to achieve greater efficiencies and effectiveness in delivering customer value.* Thus, said we can clearly see that the scope of a CRM is to increase and improve marketing productivity. There are many studies and scientific analyses on how to develop and integrate a CRM framework/system that it can be a topic for a thesis itself. Hence we wont go into a deeper analysis on how such a system is developed and the advantages and benefits that it brings to the companies that implement it but rather refer to [82], [83], [84], [85], [86], studies that can provide a good overview of the CRM as a system and hence assist in the developing process of it or a selection of an already developed CRM solution. This actually revels the primary responsibilities of the CRM Director, which is to focus on assisting the C-level executives to build a customer focused culture. Thus, placing the customer at the core of the business processes and strategy. According to [87] the CRM Director has to understand that " *A CRM solution isn't about imposing a standardised way of operating as defined by a software vendor, rather forward-looking organisations need a solution that can meet their needs now and grow and change along with them* " When doing

[32] http://www.businessdictionary.com/definition/customer-relationship-management-CRM.html#ixzz2Qiot7Ajs

so, he will be in the condition to perform an analysis of the current needs of the company and forecast possible future needs. Following, he will conduct a market research in order to obtain a solution that suits the company or recommend to the board of directors that the company invests into implementing it herself or hire a third party to do so on their behalf. In the same industrial consulting study [87] they focus on the characteristics of such a system which briefly are that a CRM has to a) deeply understand what customers need, b) to be able to engage with the customers for example through social media, c) get close with customers and maintain a close relationship with them by closely analysing their needs and meeting them beyond customers expectations, d)be easy to use and attractive to everyone both the employees and the customers. Summarizing, a CRM director's role is to:

1. Analyse the needs of the company's CRM solution.
2. Oversee the development or acquisition of the CRM solution ensuring that it meets both the current and possible future needs of the company.
3. Place the customers into the heart of the business assisting the C-suit executives and board to develop a customer focused culture.

2.16.3 Role analysis from a security perspective.

We have already determined that the purpose of a CRM is to increase and improve marketing productivity. Thus, to identify, acquire and retain customers [88]. The CRM is an IT based system which according to SANS study [89] includes technologies such as

- Database servers to store customer data.
- Web servers to present data to internal employees, sales representatives, field service technicians and customers.
- CRM application.
- Web browsers.
- Wireless devices such as cell phones, tablets, laptops etc.

As we can understand there is a large variety of technology used in a CRM that brings technical security risks on many fronts. Such security risks according to [88] could be

1. Denial of service attacks.
2. Database attacks.
3. Identity thefts.
4. Malware infections.
   Additionally we add:
5. Social engineering hacking attacks.
6. Other various of forms of attacks that can happen on IT base systems.

Those risks pose a serious threat to a company. Customer's sensitive data are stored in a CRM system such as credit cards, social security numbers, identities etc. and a potential breach will lead to money loss, law suits and even to bankruptcy for a company due to possible fines/settlements or customer's loss. Thus, where information security comes to

play a key role into protecting and safeguarding both the system and the data that it stores and processes. Besides that, another very important issue that information security comes to cover in a CRM is data privacy and data processing law compliance which of course derives from the nature of the CRM system which stores customers, employees and third party contractors data. Hence it requires proper handling and appropriate security controls. Thus, where the role of the CRM director fits into the whole picture. He is responsible to be a security aware person understanding the challenges and risks that a CRM system poses to the company's information security [89]. Thus, means that he will be able to collaborate with the CISO of the company in order to follow the fundamental principles of information security regarding software development and ensure that together they will make it right and secure from the beginning. That of course in the case the company chooses to implement the CRM by itself. In the other case he again has to consult with the CISO in order to review the selected by him solutions and choose the only one that fits best with the security policy, procedures, controls of the company but also ensuring that the CRM meets the company's needs. In addition to all these requirements, the CRM director, as any other director, has to acknowledge and follow the security responsibilities as described in the Supervisor, Manager, Directors section.

2.16.4 Role Responsibilities

Now that we gave a holistic overview of the CRM directors role we summarize and list his responsibilities below. A CRM director has to:

1. Analyse the needs of the company's CRM solution.
2. Oversee the development or acquisition of the CRM solution ensuring that it meets both the current and possible future needs of the company.
3. Place the customers into the heart of the business assisting the C-suit executives and board to develop a customer focused culture.
4. Possess a security aware culture.
5. Acknowledge the security risks and challenges a CRM system has.
6. Collaborate with the CISO in the development or acquisition of a CRM system.
7. Has to acknowledge and follow the security responsibilities of a supervisor, manager, director as they are described in the homonymous section of this thesis.

2.17 Users

2.17.1 Role Global definition

Users. A user is any individual using a computer connected to a company's network or those who have been granted privillages and access to a company's computing and network services, applications, resources and information.

Definition adopted by the author from [90].

2.17.2 Role analysis from a management perspective.

There aren't many things to write about a user from a management perspective. Rather than that the users are the workforce of a company that are using the company's resources in order to achieve the company's objectives and goals. Hence a user from a management perspective has to fulfil the responsibilities and tasks defined in his job

description.

2.17.3 Role analysis from a security perspective.

What is a company/organization without people? Can it exist without people? Of course not. They are the beginning and the end of a company/organization they make the company/organization. It's there existence that give breath to any kind of operations or procedures. As we clearly understand humans are important to any company/organization and their importance is out of question. But what about the security of a company ? Are the employees posing a threat to the company/organization? A lot of discussion and research is being held nowadays towards the human factor in the security of a company/organization. Peoples behaviour and nature are unpredictable and that poses a threat on its own towards any kind of security. Employees are people and not machines. It's in our nature to do mistakes after all as Albert Einstein said: " Anyone who has never made a mistake has never tried anything new." and it is the way we learn things by learning from our mistakes. This factor of human error is the most unpredictable of all the risks. We might consider that something is wrong with an employee if we identify some suspicious behaviour but to predict when an employee will make a mistake it's like entering a casino and expecting to win, when all the research and statistics show that it is almost impossible. That leads us to a small conclusion that a company gambles with her employees and whether they win or not is determined by many factors.[33] Before we start our discussion about the users responsibilities we believe it is wise to take a look at ourselves the information security professionals. Every information security professional knows that if he is to fight and face the users, its a battle he cant win. It will most likely cost him his place in the company if he heavily goes against the users. In this aspect we (as security professionals) have to understand that implementing heavy security controls and trying to become a police man who is trying to enforce the law and order will result in an epic fail! The heavy security fatigue should be avoided but rather transformed into a social personality. Building a relationship of mutual respect and trust with the users. In the modern digitised era, users are more sophisticated about technology capabilities more then ever before [91]. Hence, they will find a work around of any security controls if that eases them in fulfilling their job requirements. Such behaviour can jeopardize the information security of the company and lead to an information security breach or exposure with various risks for the company. Thus, [92] security controls cant stand on their own! It is essential that the users are aware and truly understand the nature of the security controls and the necessity of their existence. This can only happen if there is an appropriate security awareness campaign and education program in place. The desired outcome of such program is that users fully understand why there is a need for information security; what is information security protecting; what are the consequences of a security breach, and how they affect both the company and the person responsible as well. When they understand the answers to those questions they will be motivated to adhere and follow the security policy. A security policy that should explain in detail the security procedures and answer questions like: what is allowed to be attached to the network; to whom a stolen/lost laptop, phone or any other device that has company's data or provides access to company's network has to be reported to; what is the purpose of access authentication mechanisms; explain the

[33] Text reused from the author taken from a previous study by the author Internal Crime analysis and recommendation supervised by prof.Hämmerli

role of access privileges (why should user accounts not be shared); and what is the difference between a good or bad password; Ensuring that the nightmare of every security professional of passwords stickers attached to the monitor wont turn into reality! It is essential that all users are familiar with, understand and know how to use the security policy and procedures. However, as we said in the beginning people aren't machines, therefore incidents can and do happen [92]. Therefore, besides the general awareness culture, users have to be able to detect, react and protect the company[92]. They interact with the system on a daily basis and usually they are the first to discover a security issue and it is essential that they are educated to recognize signs of compromise [92] and be in a position to react against them. Among such compromises lies not only the breach that comes from an outside attack, in various forms, for example penetration of the network, fishing emails, Malware, social engineering hacking attempts, impersonating and various of other forms of threats but the threat of an insider as well discussed in the R& D section. The bottom line is, users should be aware, prepared and educated to face security breaches attempts and as stated by Motorola in [91] " *User awareness is an important defensive weapon in your information security arsenal. As users gain a fuller understanding of the risks and potential costs of poor security practices, they can more easily recognize the part they can play in protecting the organization's mission. Better informed users can be proactive security allies, more readily accepting controls and applying them more consistently. Most important, in accepting shared responsibility for protecting critical information assets, your human assets become more valuable. That means higher value, lower risk exposure and lower costs for the entire organization.* "

2.17.4 Role Responsibilities

Closing the user role discussion we would like to present the user role in information security as defined in NIST publication [93] which summarizes our discussion and approach of the user role. Hence according to NIST a user must:

1. *Understand and comply with agency information security policies and procedures.*
2. *Be appropriately trained in the rules of behaviour for the systems and applications to which they have access.*
3. *Work with their management to meet awareness and/or awareness training needs.*
4. *Keep software/applications updated with security patches in those cases in which users are responsible for doing so.*
5. *Be aware of actions they can take to better protect their organization's information. These actions include, but are not limited to, proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of information security policy, and following rules established to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms.*

2.18 CDO

2.18.1 Role Global definition

Chief Data officer as defined by Usama Fayyad: [34]

Chief Data Officer described exactly what the executive team and the company were

[34]The world first chief data officer appointed by Yahoo.

looking for: someone to lead all strategic data activities and to represent Data as a strategic asset that DRIVES business and that helps lead the company in new directions.

2.18.2 Role analysis from a management perspective.

Chief data officer is a new evolving role in C-level executives. The digitised era brought with her a tremendous rise in electronic-al data used in companies environment. Thus, generated a vast need for data handling figure 40 as you can see data handling is divided into seven parts/processes.

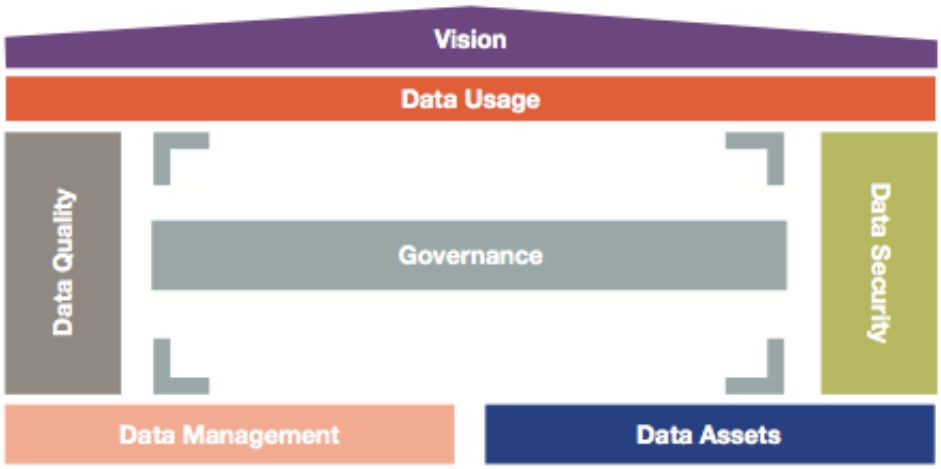


Figure 40: **Data Handling Picture extracted from** [94]

Although these processes can be distributed among different departments in a company. New regulations and laws indicate a need of a person accountable for the handling of data. Thus, the need of a chief data officer. Besides the law compliance, a relevant study [94] used a cost benefit approach to illustrate the benefits and the costs of poor and good data handling. We list their findings below in figure 41. As we can see in figure 41 the costs benefits approach indicate that a company has much to gain in many areas and much to lose if they don't implement data handling properly. But that is just one side of the coin. Another study of the CDO role [95] took a different approach and illustrated 18 reasons/drivers figure 42 for a company to appoint a CDO. Which also describes and pinpoints the responsibilities of the CDO.

On the same page with this study another MIT [96] survey comes to complete the puzzle of the CDO role, we list their findings in figures 43, 44. As we can see there are various approaches to the CDO role but they all lead to the same conclusion and that is the definition of the CDO role as it is defined by Usama Fayyad: [35]

Chief Data Officer described exactly what the executive team and the company were looking for: someone to lead all strategic data activities and to represent Data as a strategic asset that DRIVES business and that helps lead the company in new directions.

Thus, stated we believe there is nothing to add on this description of the CDO role the definition speaks for itself. Ultimately we understand the role as the person responsible for overseeing and unifying the data handling processes of a company in order to maximise profit (shaping the business strategy based on statistical data) and the working

[35]The world first chief data officer appointed by Yahoo.

efficiency of a company.

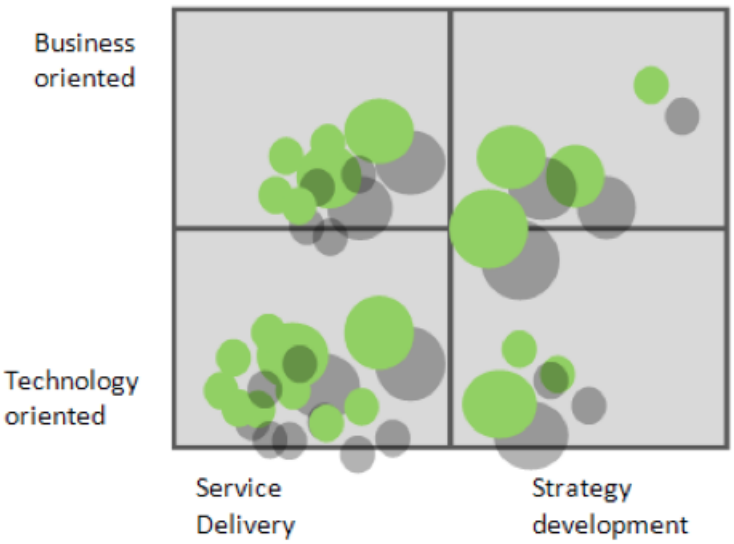
	Cost of poor reference data	Business case considerations
Sales	• Marketing: limited ability to cross-sell and up-sell due to lack of single customer view • On-boarding: revenue leakage due to lengthiness of on-boarding processes • Analytics: no capability to produce insights on client and product profitability	• Faster on boarding of new clients through automated workflow applications • Cross product sales by providing a single global view of client including restrictions and legal agreements in place • Cross-region and cross-product revenue analysis and reporting per client
Execution	• Decision Support: erroneous data results in ineffective pre-trade analysis and risk assessment • Timeliness: delayed or erroneous product setup results in poor pre-trade analysis, potential trade delays or pricing errors • Volume: flow capacity is restricted by manual processing required post execution	• Global execution services through single firm wide view across product, counterparty and book • Faster trade execution through timely creation of new instruments and accurate counterparty and book data • Accurate quotes through better pricing data and pricing inputs
Middle & Back office	• Reporting: errors require manual effort to produce accurate internal/external reporting. Finance and Risk use different book hierarchies which do not reconcile and cause reporting discrepancies and inconsistencies • Settlement: erroneous settlement instructions as well as inaccurate, inconsistent client and product data lead to reconciliation issues, delays, breaks, incorrect payments, settlement errors, and potential financial and reputational losses	• The push towards T+1 settlement using single golden source for reference data, automated data distribution and reduced manual keying overhead • Better cash flow management through consistent and accurate settlement instructions
Risk	• Exposure: accurate and consolidated view of client or market risk exposure is not available without manual intervention that increases costs and losses • Timeliness: limited confidence in real-time reporting	• Reduced capital charges through more accurate and trusted data • Improved counterparty data control as required by regulatory initiatives • Better P&L control and fewer manual journal entries through fewer duplicated trades, trade failures and trade breaks
Servicing	• Client Reporting: reputational damage results from providing inaccurate statements to clients, or sending statements to the wrong client • Corporate Actions: issues arise from incorrect application of corporate action events (missed dividend payments, wrong names after acquisition)	• Improved collateral management through better counterparty exposure metrics • Optimised capital reserving through more accurate risk exposure calculations • Better client service through better valuation and reporting on client positions • Accurate calculation of brokerage fees, commissions and stamp duties
All	• Duplication and breaches of vendor contracts • Multiple data management teams – "who do we go to?" • Limited visibility of data consumer base	• Licence rationalisation cost benefits • Clear data governance • Increased control of data usage

Figure 41: **Cost benefit approach on Data Handling Picture extracted from** [94]

Figure 42: **18 reasons/drivers for appointing a CDO. Picture generated from** [95]

Issues	Example Quotes
What are the roles and responsibilities?	• "A CDO is really almost a crisis manager and an innovation manager [more] than anything else." • "The most important role of the CDO is to ensure that data stewards understand their responsibilities." • "…teach the meaning of data governance to the entire organization." • "Acquire a practical understanding of the business's data problems." • "Develop a process to produce visualization data product data management function." • "Maximum effectiveness at whatever levels the leader demands that information." • "Manage global definitions. Maintain a glossary of information products Audit data or information stores." • "…we know which technology to get for analytics that works for more than one business functions…" • "…delivers what business wants and sees if they like it…" • "…ought to develop data strategies for business values and missions…"
What are the functions of the CDO office?	• "…A separate organization that was in between Operations and technology…" • "Data governance" • "Focal point for developing data strategies for enterprise..." • "Function of transformation" • "Corporate data infrastructure" • "…Enterprise analytics, data governance, data architecture and enterprise data assets. Of those 4 things, the last 2 have more of a technology flavor, and the first 2 have more of a business flavor…"
Who should the CDO report to?	• "CDO is ultimately responsible for CEO" • "Chief Technology Officer" • "I think it should probably be a joint reporting relationship to a CEO". • "They report to the CEO. That's the only way to do it. The leader of the enterprise has to be the one that demands timely and accurate information." • "The senior executives reporting to the Chief Risk Officer" • "COO", "CFO"
What kind of resource the CDO should have access to?	• "Database systems, people from IT and Operations, and business areas labor requirements" • "I don't think they need a lot resource if they have the authority vested in them by the CEO" • "…Think it would be the access to the changing rules and regulations…" • "Network of communities in the business units and the board members" • "Senior VPs" • "I think the external communities would be vital resource."
Does CDO complement the role of CIO?	• "I think the CDO needs to be next to the CIO, maybe on top. It's hard to say. I think they need to have equal seats at the table" • "Data has becoming so complex and big, CIO cannot handle it anymore and require additional role." • "I've had some experience with that inmy precious company, trying to put the CDO under CIO. What you get is a lot of architects and don't get a lot of improvement, and nothing gets done."
What skill set should the CDO possess?	• "Technical issue is 20%, business issue 80% " • "Build relationships with their peers, and if it's a decentralized organization, build relationships with key staff in those decentralized locations."
CDO's role of bridging the gap between Business and IT	• "CDO worked with CFO and the COO, and the heads of all the business units: securitization team, the risk management team, and all of the groups that were responsible for generating business and revenue." • "We had communications with the stakeholders." • "We used to talk about cultural barriers, which were organizational, sometimes people driven, sometimes the professional development of the people they just didn't have the tools to understand. They were very seldom technical or budgetary barriers to get the right information to the right people."

Figure 43: **CDO role in Quotes.Picture extracted from** [96]



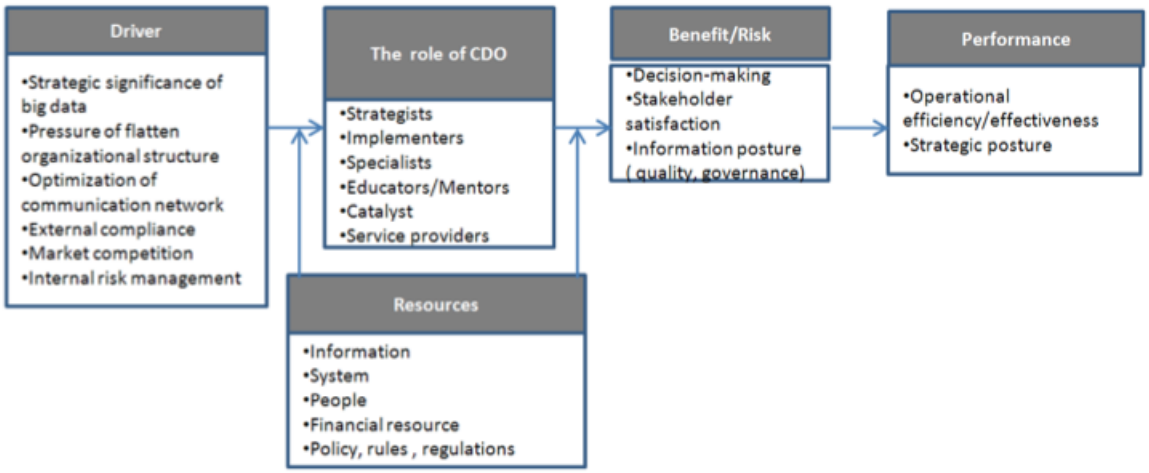


Figure 44: **CDO role overview. Picture extracted from** [96]

2.18.3 Role analysis from a security perspective.

We know that the CDO is responsible for data handling. One of the functions of data handling is data security. The CDO is responsible for anything a company does with its data. That could be storing, sharing, copying, transmitting, communicating and of course, processing data. All the data handling processes are defined by state laws and regulations. Every modern country has a Data Protection Act (PDA) that defines the way that data should be treated in companies and government agencies. It is essential that the companies comply with this law requirement and guidelines of the PDA. Usually such data protecting acts include rules about data privacy and security among others. The role of the CDO is to be fully aware about the requirements of the PDA and ensure that the company is capable and has implemented all the necessary steps to ensure compliance with the act. Otherwise, the risks of fines and penalties, of law suits in case of data breach/leak occurs due to non-compliance are extremely high, not including the reputation damage, customer losses and settlements the company would have to pay. Therefore, the CDO has to conduct data policies according to data act guidelines and ensure that everyone in the company is aware, understands the described process and capable of implementing and following the data handling policies. The PDA in most countries also covers the data security requirements. Usually such requirements ask a company to ensure the confidentiality, integrity, availability and physical security of the data. As well as places security requirements in data processing, storing and overall data handling steps. The scope of the PDA is to provide the minimum security requirements a company has to implement in order to protect its data. Hence the role of the CDO is to cooperate with the CISO in order to provide valuable insight about the security requirements as they are defined in the PDA so that they can develop the appropriate controls, policies and procedures to firstly comply with the PDA and secondly ensure the security of the company's data. Last but not least, another responsibility of the CDO is that he ensures that everyone receives adequate training towards data handling in order to create a data handling awareness culture which includes security awareness as well. However, laws and regulations change fast and frequently therefore the CDO has to constantly monitor the changes and ensure that the company complies with the new requirements both from a security and management point of view.

2.18.4 Role Responsibilities

Now that we have given an overview of the CDO role we summarise and list his responsibilities listed below.

The CDO is accountable for:

1. Ensuring data quality in a company.
2. Overseeing data management.
3. Data governance. (Thus assisting the company's governance by using statistics based on the data analysis.)
4. Data assessment. (It is the process of evaluating data using analytical and logical reasoning to examine each component of the data.)
5. Establishing guidelines for data usage.
6. Assist into shaping the company's vision by transforming data in valuable informa-

tion.

7. Assist in the Development of security controls, policies and procedures of data handling.
8. Ensure security measures and develop policies to ensure that data privacy requirements are met.
9. Ensure company's overall compliance with the Data Protection Act law.
10. Monitor changes in the PDA and ensure that the company takes appropriate steps to comply with the new requirements.

2.19 CPO

2.19.1 Role Global definition

Chief Procurement Officer (CPO) as defined by business dictionary is an: [36] *Executive level employee of an organization whose responsibilities include sourcing, supply management and procurement for the company.*

2.19.2 Role analysis from a management perspective.

One after the other, global companies enhance the activity of procurement and recognize its strategic role. The time when the chief procurement officer played the role of the dispatcher of other departments desires and commands is way gone, now he [97] is a business partner that participates in the shaping and implementation of critical business decisions. While for many businesses to organize an effective procurement service is still a desirable goal, the market "globalization" brought a vast need for transforming internal operating structures and supply chains. Today's pressure for continuous improvement and a ruthless intensity of competition brought a high demand for CPO's in companies. A role that comes to bring new ideas and solutions with an absolute goal to " Cost Less & Produce More" [98]. A CPO plays an important role in the operations of the company they work for, since he ensures that the purchasing of the required goods is done efficiently and on time by preserving both the quality and costs. When a department of a company needs to acquire a product or a service the CPO sets the necessary criteria by which the supplier will be chosen. Then, he conducts market research and records the offerings and the potential suppliers. In collaboration with the department, they review the offers and choose an appropriate supplier. The CPO has to negotiate with the supplier in order to achieve cost-effective prices and qualitative goods and eventually sign a contract with the supplier. But that is just one side of the coin. As we said the CPO is now a business partner and developer, thus because of the rapid advance of technology and the opportunities its provides. Due to speedy dissemination of knowledge, mainly because of the internet and other communication channels, the CPO has access to organizational and technological tools which can be converted to a strategic weapon of the business. Thus, the CPO continuously learns new skills and innovative techniques that add value to the final product/service of the company, which is something directly perceived by customers. In his role as a C-level executive besides the obvious tasks of sourcing, procurement, and supply management he also participates in business decisions [99]. He collaborates with other C-suit executives to establish the terms of competition, whereby suppliers are invited to submit bids. Also they take decisions related to quantities ordered

[36] http://www.businessdictionary.com/definition/Chief-Procurement-Officer-CPO.html#ixzz2QrGRvz00

and the stock of products a company should have either to cover her operational needs or the to cover their markets share demands. As a business developer he has to discover alternative/innovative sources of supply in order to lower a company's expenditures and maximise the profit [100] as well as take a proactive measure in the event that the regular supply channels are interrupted. As a CPO he has to oversee the proper function of the procurement department. That means keep records of the received goods, to assure on time delivery of goods and payments, to monitor the consistency, services and the products quality delivered by the suppliers. Another aspect that the CPO starts taking under his wing is the outsourcing of services for the company [100]. The CPO is a person who knows better then anyone the needs of the company as well as the global market of suppliers, whether they supply goods or services. Hence, he is a person that can recommend to the board of directors and the CEO strategic decisions of outsourcing services and procedures of the company that would cut costs for the company and increase it effectiveness and robustness. Last but not least, a CPO has to constantly monitor the conditions in the market firstly searching for new opportunities and seizing them when they occur, and secondly the cost of materials that are necessary for the company, as well as preparing reports to inform the board of directors and the CEO.

2.19.3 Role analysis from a security perspective.

We gave an overview of the CPO from a management perspective and there the things are pretty clear, but this role has a double nature when it comes to information security and that attracts our interest. Let us start with the first "boring" and obvious part, the CPO deals with tons of data on a daily basis, contracts, prices, offers, customers, thirds party vendors and IT systems interactions are just some parts of the CPO's arsenal. It is obvious to say that all this data has to be protected for various reasons, for example contracts and prices should be only available for internal use for reasons of market competition. Any kind of data leakage will pose risks to the procurement department and its procedures. Thus the responsibility of information security to protect all the data and ensuring that information security guidelines about the procurement procedures exist in the security policy. On the other hand the CPO as any other supervisor, manager, director has to adhere and implement the responsibilities described in the homonymous chapter. On the contrary the second part is where things start to get interesting. We mentioned in the previous section that the CPO is responsible for outsourcing. And we say that we mentioned because we deliberately didn't analyse it in that section but rather align it to the security section. But before we proceed and explain the reasons behind this we would like to clarify the concept of outsourcing. Outsourcing is a term that gained popularity in the United States in the beginning of the 21st century and actually means contracting out an internal business process to a third party company. There are many debates on whether this is good or bad practice. However, we wont fall into the trap of participating in it! Usually, if a company decides to outsource he/she does it for one of the following reasons:

- To reduce both fixed and recurrent costs.
- To allow the client organization to focus on its core business.
- To access skills and technologies.
- To provide flexibility.

- To increase accountability.

But how outsourcing, which is a key responsibility of the CPO, relates to information security? One of core functions that companies tend to outsource is IT, thus because of its sophisticated nature and specialized requirements. Hence it is profitable for some company's to outsource it. However, IT outsourcing comes with risks besides the many various benefits. Before we proceed any further we believe it is wise to explain what IT outsourcing is.
As defined in [101] *IT outsourcing is the delegation of IT services from a customer to an external service provider (often called an "outsourcer") specializing in these services.*

IT outsourcing despite the region it happens in, either locally or internationally, doesn't change the benefits or risks [101] . Although outsourcing to another country might provide lower costs it might as well have more complexity and regulations requirements. When outsourcing IT, companies have to realise that they expands the company's security perimeter by extending access to and control of information to an external third party [101]. And here the CPO plays a vital part, since he is the person to search and identify and select the third party IT service provider which will meet the needs and fulfil the demands of the company, it's partners and customers. One of the core challenges of outsourcing is that despite the fact that a company delegates the IT responsibilities to a third party he/she is still liable for the security of all information processed by the service provider [101]. Therefore, a company once again relies to information security to protect her interest and ensure law compliance. In the Microsoft and the Swiss Security Exchange forum [101] they conclude on two key points on how information security protects a company when it decides to outsource IT. According to [101] a company and the outsourcing provider, with respect to information security, should always:

- *Set up external security audit structures prior to going into production with an outsourcer. When the whole IT staff gets involved in security, it's harder to ensure that policy oversight, audit, and administration functions stay separate - which they must. Throwing an IT outsourcer into the equation just muddies the waters further. Specify in your contract that either your own security team (which must report outside IT operations) or a third party (such as a managed security services provider or security consulting firm) must audit your outsourcer's implementation of security policy on an ongoing basis.*
- *Outsourcers should implement risk management and security policy, not make it. Frightened by reams of regulation, firms may feel tempted to defer to the expertise of their outsourcers. This is a mistake. Only your firm can determine its maximum acceptable level of risk. Your security chief must determine your company's appetite for security risk and set policy accordingly. The outsourcer's role is to implement that policy, in everything from setting the number of failed log-ins a server permits to creating perimeter firewall rules.*

2.19.4 Role Responsibilities

Now that we have given an overview of the CPOs role it is time to generate the role's responsibilities. We summarize them and list them below.

A CPO is accountable for:

1. To oversee and lead the functions of sourcing, procurement, supply management and outsourcing.

2. Consult and assist on strategic decisions of the company.
3. Ensure that best practises of Procurement are followed in the company to ensure a "Cost less-produce more" culture in the company.
4. Negotiate contracts and earn the best possible deals for the company.
5. CPO as any other supervisor, manager, director has to adhere and implement the responsibilities described in the homonymous chapter.
6. On the other hand he has to ensure that information security implements guidelines on how to protect the procedures and processes of the procurement department.
7. Outsourcing, to search and identify and select the third party outsourcing service provider which will meet the needs and fulfil the demands of the company, it's partners and customers.
8. Oversee that information security is not neglected upon outsourcing.

2.20 Chief Facilities Officer also known as Facilities Manager

2.20.1 Role Global definition

There are various definitions for Facilities Management. We use the European standard for Facility Management, EN 15221âĂŘ1:2006, prepared by the Comitee Europeen de Normalisation (CEN) where: "*Facility management is the integration of processes within an organization to maintain and develop the agreed services which support and improve the effectiveness of its primary activities.*"

2.20.2 Role analysis from a management perspective.

Chief facilities officer, from a management perspective, is a role were we cant provide a very accurate and detailed analysis. Thus, because the requirements and responsibilities of the role are shaped by the company and the industry he works in. For example a person who is a facilities manager in a hospital environment his primary concern will be to assure infection prevention when on the contrary in a manufacturing company his priority will lie in the safety and productivity. However, there are common functions of the role identified in many industries. According to [102] there are three FM reference areas: the strategic, the analytical and the managerial-operational. We list their description as they are defined in [102].
The strategic area concerns the facility management company policy (internal, external or mixed), the managerial responsibility, the sharing of the company policy in finding, maintaining and distributing the resources to support the company goals (budget definition and management, costs allocation, etc.), the contractor selection, etc.
The analytical area concerns the comprehension of the end-user's service needs (expressed or not expressed), the control of the management results (efficiency in service delivery) and the identification of new techniques and technologies supporting the company business. It plays a fundamental and essential role in enabling the facility management to contribute to the business success preventing it to be instead an obstacle to its achievement.
The managerial-operational area concerns the management and the coordination of all the services, thoroughly intended (not of the single services), and includes the definition of systems and procedures as well as the implementation and re-engineering of the service delivery processes. Hence a facilities manager is responsible for the overall maintenance of the

physical facilities while staying within a defined budget and ensuring compliance with all applicable laws and codes. From a strategic perspective he should forecast additional resources requirement of the company based on insights from the C-level executives and take appropriate steps to fulfil them.

2.20.3 Role analysis from a security perspective.

Although the role is not appealing and somewhat unfit for analysis from a management perspective when it comes to security he has a well defined role to play. For many years we had a diversification of physical and IT security. However, nowadays companies realise that the convergence of physical and IT security will offer many benefits, with the most significant being the centralized view of all the company assets and risks [103]. In this convergence the facilities manager plays a vital role. Since first of all he is the key keeper! That means he is the person who has access to all the facilities. In terms of security he is the person responsible for the physical security. There are a number of risks and exposures to a company's facilities, specially facilities where telecommunications switching equipment, network infrastructure are potential targets for attackers. Examples of these attackers are vandals, thieves, political driven attackers or other various of causes attackers, but the most dangerous and motivative attackers is the corporate spy. Therefore physical security play a key role in the overall security. The best IT security controls can be bypassed if the attackers have physical access to the network they are to attack. Therefore physical security controls such as locks, biometric access controls, surveillance equipment, sensors and alarms have to be installed as well as security guards to be hired to safeguard the facilities. Therefore, the facilities manager is the person who has the knowledge and can recommend to which facilities which measures should be implemented. That, requires the collaboration with the CISO in order to assure that all the companies assets are secured in the best possible way. Another important aspect of physical security is dedicated to safety and it is by far the most important measure a company has to implement. Thus, because there is nothing more valuable than human life. The facilities manager is responsible to implement and oversee that appropriate safety measure are taken in order to prevent loss of human lives and as much as possible to avoid accidents. Among such measures, are emergency and evacuation exit plans, fire extinguishers, smoke and fire detectors etc. But that is only one side of the facilities manager role. The other part is his participation in the development and implementation of business continuity plans of a company. But what is business continuity? The British Standard for Business Continuity Management (BS 25999), defines business continuity as follows: "*Business continuity management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.*" In simple words it is the plan that the company will initiate during a disaster to ensure that he can continue operating until he fully recovers and restores his processes. That means that the company will mitigate the losses and somewhat control them and stop "bleeding money" if a disaster occurs. Incidents handling and Disaster recovery as well as business continuity are aspects that are covered by information security. How such plans are conducted and developed, is a huge topic for discussion and a core part of our studies, but this is not the place and the time to open such a discussion. Thus, we will just mention that there are appropriate standards

and globally known best practises to develop such plans. But what is the role of the facilities manager in business continuity? In order for a company to recover and continue her operations it is essential that there will be a temporary facility where the company can relocate and continue working. For instance if there is a fire and the headquarters offices are destroyed there should be a back up plan and a back up facility to move to at least temporary. That also applies for the backups of the company's IT systems and data which have to be stored at least in two safe locations in parallel. These locations have to be chosen wisely and properly and the person responsible for this selection is the facilities manager with the collaboration of the CISO and the other C-level executives. These are just some small examples of how a facilities manager participates in a BCP. Moreover in a relative study [104] the author demonstrates and categorizes five different roles that a facilities manager can play in a BCP plan/management. We give a brief overview of this categorization and the finding of this study.

1. *FM has the leading role. In this role, FM operates at the strategic level within the organization as a strategic owner of the BCM process and is responsible for the entire BCM policy.*
2. *FM supports the strategic management. In this role FM has the function of BCM manager, during business as usual. FM will support.*
3. *FM assures continuity of critical FM processes. In this role the FM has the function of BCM coordinator.*
4. *FM is responsible for safety and security. In this role the FM department handles the BCM function as the specialist in the field of safety and security.*
5. *FM provides preventive support. FM takes care of prevention, but during a crisis there is no role for the FM.*

As you can see there are different roles that a facility manager can play in a BCP. Hence he is a key participant when it comes to the security of a company and contributes on many different levels. Whether it is to safeguard the physical security or the IT security, in a big company. After all, facilities are the places where all the magic happens and if you don't assure that you have great ones you will face the bad consequences.

2.20.4 Role Responsibilities

Now that we have given an overview of the facilities manager role it is time to generate the role's responsibilities. We summarize them and list them below.

The facilities manager has to:

1. Ensure compliance with state laws and requirements regarding facilities.
2. Oversee the management and maintenance of facilities.
3. Ensure safety controls are in place to protect human lives.
4. support for Disaster recovery and business continuity plans both in their development and their implementation.
5. Ensure the physical security of the company.

2.21 Insurance Agent/broker

2.21.1 Role Global definition

An Insurance Agent is a state-licensed professional who represents an insurance company in selling and servicing policies. An insurance broker is a person or company registered as an adviser on matters of insurance and as an arranger of insurance cover with an insurer on behalf of a client. [37]

2.21.2 Role analysis from a management perspective.

Nowadays, all the companies face the possibility of loss, injury or damage which can force them out of business. Therefore, they acquire insurance coverage. Thus, the reason they either appoint a broker in order to conduct market research on behalf of the company and find the best suitable insurance for the company's needs or sign a contract with a big insurance provider that will appoint an agent that will deal with the companies insurance needs. However, every company is different and has different needs of insurance. Therefore we cant accurately describe either of these roles. But one thing we can tell about business insurances is that there are usually three factors [105] for their acquisition:

1. Asset Protection. This protects the company from liabilities of any kind, protects the physical assets and protects the company from business interruption.
2. Revenue protection. *Revenue protection can provide your business with cash to compensate for the loss of revenue and costs of replacing a key employee or business owner should they die or become disabled. [105]*
3. Ownership Protection. *Ownership protection can provide the continuing owners, or their nominees, with sufficient cash for the transfer of the outgoing owner's equity to the continuing owners, should a business owner die, become disabled, or suffer a critical illness.*

Hence the role of the insurance agent/broker is to cooperate with the Chief risk officer and research the market in order to provide acquisition options of insurance policies that meet the established, by CRO and the board of directors, insurance plan of the company. Since the nature of the company's varies, so are the needs we can't go deeper on what kind of insurance schemes are applicable or appropriate to companies and which are the standards to acquire insurance policies.

2.21.3 Role analysis from a security perspective.

The selection of this role as well as placing it as the last role that we will review in this thesis is deliberately done. Thus, because we would like to discuss a little about the future of information security and how we see it as well as how memorable security experts predict it! We use the role of the insurance agent because we want to take part in a hot information security topic that is at the beginning of it's rise. Its none other than information security insurance or else known as Cyber security insurance. This is a modern topic and a lot of discussion and research is conducted on techniques, frameworks and nature of how this could become a trend and a must for every company? Is it really worth selecting such path? In an article we review [106] the author discusses about the appealing market of cyber-insurance and proposes a model on how this market could evolve.

[37] Definitions taken from Oxford dictionary.

However he concludes that such a development is something very hard to accomplish and he states that it will be very hard to see it evolving in the near future. However, due to the tremendous rise in cyber - crime, we see today an evolving market and companies are starting to demand insurance for data loss/leakage and we start seeing information security insurance policies appearing and hitting the market. As an information security student and future professional the author understands that information security insurance is a possibility for information security risk management. However, there is a core challenge and a problem in this approach at least in our humble opinion. Thus, is the problem of accurate statistics about how security incidents occur. It is well known that insurance companies rely heavily in accurate statistics and their whole structure of assets valuation is based on accurate statistics. In information security there are no accurate statistics yet they rely on risk management. Therefore, one could say that the insurance companies providing information security insurance schemes are gambling. But this far from the truth! Even thought they provide such schemes, the claims for information security incidents are often denied or even if they are accepted the compensation paid is far lower than the company claimed. Thus, because asset valuation is far from an objective process; hence it will always favour the insurance company and as we observed in many industrial cases when a security incident occurs and the insurance claim is denied or paid less, the companies tend to drop the insurance scheme soon after. Here we would like to recall a statement of Ros Andersen where in [107] he stated:
"A trusted component or system is one which you can insure."
Thus, said we acknowledge that information security insurance is a hard industry to evolve. However, we would like to see it evolve and we believe it will and when it does the forecast of the memorable security professional and professor Eugene Schultz will eventual be a reality. In an interview he stated that:
"*Cyber risk coverage is one of the great hopes for setting a "commercially reasonable" floor for information security-because once such insurance is broadly available, it will become a commercially UN-reasonable practice to NOT carry that insurance. And so everyone will have to meet the security standards mandated by the insurance industry.*"

3 Use case/Scenarios

3.1 Introduction

We often encounter the terms "scenarios and use cases" when we deal with information security. But what do they really mean? A lot of people in our modern world believe that history repeats itself. We do as well. It is common knowledge that history teaches us valuable lessons, gives us valid information about the mistakes we made and provides us with the option and the opportunity to learn from them and not to repeat them in the future. *You're not a fool if you make a mistake, but a fool if you make the same mistake twice. We learn from failure, not from success!* These are the use cases, our mistakes or mistakes made by others that we can learn from and ensure not to do the same. On the other hand, scenarios are quite the opposite, Michael Porter defined scenarios [108] as "*An internally consistent view of what the future might turn out to be - not a forecast, but one possible future outcome.*" In our case, we understand a scenario as an assumption someone has about a course of action or a decision taken by the organization or an individual in order to secure themselves and based on that decision what the outcome will be. Now that we have given a small overview of what use cases and scenarios are we can now proceed to them.

3.2 Power game

A CISO in a big international company identifies an information security issue. That problem needs to be fixed and requires a big investment. The opinion of the CISO is that it is critical for the company's "well being". Therefore he takes this issue to the CEO of the company. But the CEO doesn't want to hear anything about it and rejects every notion the CISO does. However the CISO wants to do his job right, therefore he goes to the CRO and the CLO and discusses with them the issue, since it is of relevance and is both a risk and a compliance issue problem and asks them all together to address the CEO putting pressure on him into dealing with the situation, hoping that this time the CEO will listen. Unfortunately for them the CEO rejects any discussion and warns them to drop the matter telling them that it is not that urgent and there are way bigger problems the company has to concentrate on. The CISO is frustrated by this situation as he knows that this is not a small problem that can be ignored and wants it fixed regardless of the CEO's opinion, for the "well being" of the company. Therefore he plays the only hand he has in the situation and orders an external IT security audit, a process that a company has to conduct on a regular basis, making sure that the problem is addressed by the external auditor and that it becomes a compliance issue, meaning that the company wont have any other choice than fixing the problem. The CEO of the company having the results of the audit presented in the boardroom understands that he is "played" and is angry about this, but he was left with no choice but to resolve the problem. The security issue was resolved, the investment was made, but the CISO had to pay the price, he was replaced by someone else by the CEO that lead to the fact that he had to go on his own from the company, even though what he did was for the best of the company. This is a real life

industry story where we can see that the CEO of a company has the first and the last word to say in a situation. This is also a matter of a person's ethics. The CISO wanted to do his job and have a clean concious that he did what he could and perform his job to the best of his knowledge ensuring that the company is protected. However he knew what it meant to go against the boss, therefore we have professional ethics colliding with personal prosperity. As we can see the CISO chose the admirable way even though it cost him his job, a job that he could keep if he just documented that he made a request for the security issue and it was rejected, if an incident did occur he would not be held responsible. However he chose to protect the company rather than his personal benefits. This story teaches us a lesson that in order for a CISO to do his job and protect the company he needs the support of the CEO, if not either the information security of a company will result into an epic fail or as we saw it will cost the CISOs job.

3.3 Delegation of duties

In this section we would like tell you another real life story. An intern was working in a big commercial bank and the director of the branch as well as the deputy director and some seniors officers with access privileges to the banks systems due to their overloaded work schedule trusted the intern with their user-IDs and passwords and asked him to perform various tasks for them on a daily basis. Thus a very familiar situation to many people working in a network environment where users privileges and access controls are in place, people do share credentials in order to get a job done. This is a huge mistake and exposes the company's information security to various risks. In the case of the intern, the highest level officer is the branch director, in many other companies the same situation could happen where a CEO gives his credentials to his secretary or somebody else to do some tasks for him. But lets analyse this situation further, what could the intern or anyone else in the same position do. There are three possible courses of actions a person can do:

1. It's your boss, so it's okay to do this.
2. Ignore the request and hope he forgets.
3. Decline the request and remind your supervisor that it is against security policy.

The intern chose at first option number two, but this never works. Unfortunately for him, he had no other choice but to accept the trust of the director and the senior officers and hopping that nothing goes wrong. If something did go wrong and an incident did occur, during the investigation he would be the first to take the blame, because he is the weakest link in the circle. The management would face the constituencies for giving out the passwords and would be held accountable but the intern would have to go and prove that he did nothing wrong and that was a risk for him personally, as specially as it was in the interns case a financial bank where large amounts of money are processed on a daily basis and he could end up facing criminal charges and possibly pay settlements to the bank if any money was lost or stolen. A lot of us would here raise a question? Why it is that the intern didn't choose the correct answer that is obviously the third option? This is not a choice made only by the intern, but many other employees who don't dare to choose that option although it is the correct choice. There are two explanations, one is that the users don't have security awareness and education which means that they have

never read or familiarise themselves with the security policy of the company or because they trust, respect, fear their supervisor and know that a possible answer like that would endanger their relationship with them, something that will lead to possible disadvantages or change of behaviour of the supervisor towards them. This example illustrates a very common situation that happens in every company where we have delegations of duties and hierarchical roles distribution. This situation is tough to handle because of its nature and it is based on the relationship between people. Information security can be compromised and exposed by such behaviour on some occasions or in the interns case, luckily everything ends with a happy end. These delegation of roles and responsibilities is a risky game and the CISO has to be a balancer in between managers, C-level executives, supervisor, directors and users ensuring that all are educated and understand the consequences both for the company and themselves on a personal level of such behaviour. Thus, understanding that the access controls and user privileges are there for a reason, the same reason we have different roles in a company, therefore avoiding the credentials sharing is a must for every company.

3.4 Roles in Security Incidents

Early one Sunday morning the CEO, CLO, CRO, CDO, CMO, CFO, CHRO, CIO of a major bank received an urgent call from the CISO. He requests that they travel immediately to their office. When they arrive at the bank's office, they find the Chief facilities manager and the CISO waiting for them, the chief facilities manager was also informed by the CISO so that they could get access to the facility. When everyone arrived they get in a meeting where the CISO informs them that the bank's security has been breached and that one million credit card numbers and information of the holders of the credit cards as well as some of the bank's employees personal data have been stolen by a hacker. Everyone is very worried about the economic cost and potential loss of market share. They immediately initiate the incidents response plan and alert the Crisis Management team to deal with the security breach immediately. In the meanwhile they remain in the meeting and start shaping the strategy and their course of action. They delegate responsibilities and proceed with the appropriate actions. The CDO provides the necessary data input and collaborates with the CRO and CFO and they conduct the incident's risk assessment estimating the cost of the security breach for the bank. The CISO and the CIO are in direct contact with the crisis management team commander in order to oversee the course of action and notify the rest of the C-level executives of the progress and the status of the crisis management team. The CLO on the other hand contacts the appropriate authorities to alert them, press charges and take appropriate legal measures to protect the bank's interests. The CEO and the CMO are preparing a press release statement to inform the public and the customers about the security breach and their course of action. The CHRO is informing the board of Directors as well as the rest of the Managers, Supervisor and Directors and the affected employees about the situation. The crisis team handles the security incident, and documents the cause, the results and all the steps that they have taken during and after the incident. The board of directors are gathered along with the rest of the C-level executives that are dealing with the incident. The CISO presents the findings, results and course of action of the security incident. The CMO proposes the developed press release statement and media handling policy he shaped with the CEO. The board of directors in collaboration with the CEO decides on further actions, restoring the

operational stage of the bank and developing a plan for handling the affected customers. This is a scenario of a data breach incident in a bank (could be in any company) where you can see that the collaboration of different roles is necessary when dealing with an information security incident. This example demonstrates how roles interact in a security incident and defines how their responsibilities are delegated, once again emphasizing the trivial fact that "everyone is responsible for security".

3.5 Product Security

In the industrial world companies spend time, money and effort in order to develop products, products such as movies, music, software, games, operating systems and various other kind of computer related products, therefore they don't want to see their investments not paying off. We already stated that information security is a "tool" to cover a legal requirement, that of protecting a company's investors and their investments. Thus actually protecting company's products ensuring that they will deliver the desired revenue when hitting the market. Let us discuss a couple of real life examples in order to illustrate how information security plays a role in a company's finances. In the first example we would like to take the Sony playstation game console. This game console is designed by Sony in the way that it only plays the authorised copies of the games and movies. Thus happens, deliberately by Sony in order to ensure profit not just from the gaming console itself but from the sales of various games that will hit the market for the gaming platform. This is the way that Sony set up its industry and the way it generates the biggest part of the revenue. This revenue relies on information security to protect it. Thus because Sony implemented security controls and authentication mechanisms that allow only authorised games, movies etc. to run on the console. However, the implemented security of the device was explored and compromised by a well known hacker known as geohot which explored a security vulnerability and was able to so called "jailbreak" the device. That means to compromise and work around the security controls so that all the security measures Sony implemented where lifted and the console was able to run unauthorised copies of games. Something that is translated in a lot of millions dollars revenue loss from the games sales. Sony of course took legal measures to protect the company's interests and sue the hacker, a law suit that ended up in settlement out of court. However the damage was done, millions of dollars were lost for Sony and users unlocked their devices to enjoy the blooming world of pirate games. Speaking of games there is no difference whether they are games or software where hackers explore security vulnerabilities of the software and so called "crack" them making them available free of charge, and users obtain illegal unauthorised copies. Once again a failure in information security leads the software developing company's in loss of profit. In a second example the situation is somewhat the same, another global industrial giant, Apple had their iphone's security compromised by hackers and the device "jailbreaked" and carrier unlocked allowing users to use unauthorised applications and network carries costing millions of dollars to the applications developers, Apple and network carriers. These are just a few examples where the failure of a company to secure her product lead to loss of revenue for them. Therefore we see more and more industrial giants to heavily investing into securing their products. It is historically known that security always was an afterthought in software development but no more! Now it is a priority for every company. Thus because in the modern industry the CEOs of companies want to see lower costs

and revenue growth making the profit and future existence, prosperity of a the company a primary goal. That means that they will concentrate in product security if it poses a threat to the company's revenue. After all, the importance of a product's information security depends on what that product is. But when it is important, the CEO with the other C-level executives try to deliver a secure, qualitative product with a low cost. Speaking of costs the person dealing with them is the CFO who has to ensure that products security is developed but in the meanwhile doesn't take them out of business. That's because time to market of a product is equally critical with its security, maybe even more critical. Who knows better when to hit the market than the CMO who with the cooperation of other C-level executives will determine the goal and ensure that they will meet the deadlines and have a product ready to hit the market. On the other hand the CISO knows that nothing is secure and that "*There is no castle so strong that it cannot be overthrown by money*" [1]. Therefore against a sufficiently funded and motivated attacker the security will be compromised. Thus the question of time, money and effort that the attacker has to put into compromising the security. This means that the CISO has to ensure that the products security would be hard, timely and costly to attack something that would discourage the attacker and slow him down. Something that would ensure more sales for the product and more profit for the company. In order for a product to hit the shelves there are many roles that interact in the life cycle of product development but this is not for us to discuss. However in terms of securing a product besides the above mentioned roles there are two more roles that can play a factor. These roles are the Chief R& D and the Chief Procurement officers who play a vital role in the process of securing a companies product/service. A company either invests into developing their own security mechanisms and controls in their product/service or they buy a ready solution to secure their product/service. In any case both of the officers have to consult and interact with the CISO of the company since he is the person who will assist in the evaluation or development of the security controls. The Chief R& D with the collaboration of the CISO will ensure that the staff of the security department such as security analyst, engineers, programmers will assist the company's research and development department into securing the product/service that they are developing and ensure that the security is implemented and in place from the beginning of the design. On the other hand the Chief procurement officer will have to consult the CISO, the Chief R& D officer, the CMO, and CFO usually, when it comes to acquiring a security control or solutions to secure the product ensuring that the product's functionality and cost is not affected.
This example demonstrates the importance of information security in products and illustrates the roles interactions to way of securing a product.

3.6 Information Security its all about ETHICS!

Blaming the victim is a common practice in our modern world. When something goes wrong it is always someone's fault. Is it though? In an article Bruce Schneier stated that: " *Security systems that require the user to do the right thing are doomed to fail.* " Thus, because people aren't machines and they regularly don't do things as they are supposed to. This is human nature, people usually don't pay attention to practises that don't affect them until eventually one day they will and then they face the consequences and learn

[1] Marcus Tullius Cicero, was a Roman philosopher, statesman, lawyer, orator, political theorist, consul and constitutionalist.

the hard way. Thus usually the case with information security as well. But what is the trigger behind a persons behaviour, we are not psychologists but in our humble opinion in a modern society it is not the regulations that keep things in order but rather peoples ethics. People make choices based on their ethics, imagine someone being attacked on the street we have two options either alert the police and go and help him or walk away pretending we never saw anything. We make choices and decisions on a daily basis and all of them come from our ethics, logic and culture. Imagine you found a laptop, phone, tablet etc. what is the correct thing to do open and check the data inside evade someone's privacy, a company's critical data and distribute the contents to the internet or sell them to someone to gain personal advantage/benefit or just do it for personal amusement. All has to do with ethics. A decent person would probably search for the devices owner or give the device to the police. A less decent would wipe its contents and use it for personal use. Another person would try to gain benefit by exploring the contents of the device. Thus just a small example of how ethics play a vital role in every step we make. The rapid non stop advance of technology creates a constant security gap. Thus, the problem of balance between the attackers and the defenders. Since technology has the ability to magnify power and multiply force for both sides. In chess, the player with the white color usually has the first move advantage and that is also the case with information security the attacker has the first move on hand with no restrictions. These situations illustrate the need to look deeper in information security, there is no solution, no model to resolve this loophole but one! It is Ethics. Ethics and people's behaviour is shaped by his family and their nation's culture. If everyone was an ethical person we wouldn't have the situation of an attacker and a defender! The accidentally lost laptop, tablet etc wouldn't threaten the security of a company or its owners. People would follow the laws and regulations and we would, possibly, be living in a better world. But what is the purpose of this discussion? We speak of ethics that is because we want to introduce a conception that we sometimes encounter in the industry. That of "blue eyes" management. Thus where we have a company's CEO and some C-level executives being ethical people leaving with the understanding that everyone around are ethical people and no one wants to harm the company. Such people would live by a code of ethics in their lives and would acknowledge and believe in computer ethics code as well. A code named "Ten Commandments of Computer Ethics" developed by Computer Ethics Institute listed below:

1. *Thou shalt not use a computer to harm other people.*
2. *Thou shalt not interfere with other people's computer work.*
3. *Thou shalt not snoop around in other people's computer files.*
4. *Thou shalt not use a computer to steal.*
5. *Thou shalt not use a computer to bear false witness.*
6. *Thou shalt not copy or use proprietary software for which you have not paid.*
7. *Thou shalt not use other people's computer resources without authorization or proper compensation.*
8. *Thou shalt not appropriate other people's intellectual output.*
9. *Thou shalt think about the social consequences of the program you are writing or the system you are designing.*

10. *Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.*

In this case the information security risk perception of the company is based on the ethics and these 10 points set the base line for information security in the company. Here the hands of the CISO are tied since he can't ask for security investments. However if he finds himself placed in a company's environment like that he has to be prepared for the potential threats and risks the company faces. That means that the CISO has to work hard developing projects and plans to mitigate a potential security incident as well as projects to improve the company's security, having them ready for a CEO to sign and stuffed in his drawer. Thus because the only way that blue eyes management will learn is the hard way. Thus is something the CISO knows so he has to be ready and seize the opportunity when a security incident occurs. After all as we already stated things change only when an incident occurs. However ethics plays another role in information security in the case where a company is at the edge of surviving a CEO wont be able to allocate resources to security but rather prioritise in saving the company by cutting costs. The first cuts the CEO will initiate will be probably in the security department. In a case like this a CISO has to be an ethical person without abandoning the ship. He needs to prepare cost effective projects which he could use in order to react to any situation, protecting and assisting the company into getting back on her feet. Ethics play a vital role in information security and in a company, not just at a executive level but also at an employee level. Thus because an ethical employee would be a responsible person and follow the laws and regulations, know and follow the policies and the procedures which are the guards of the barracked castle implemented by technical controls (figure 19). Such user behaviour would lower the information security threats/risks and mitigate the risks if a security incident occurs. This example illustrates a known situation of blue eyes management and how ethics play a role both in this situation and in the information security overall.

3.7 Information Security failure costs lives!

Up to this point we discussed the value of information security for a company regarding its business impact and revenue protection. However information security is not only affiliated with industrial companies that generate revenue for their investors but also with non-profit organisations with far greater value than profit the public wealth and peoples lives. In this example we will discuss about a public sector organisation. Although it is not the usual case of a company as we know it from the industrial market it still operates as a company, but in this case the profit is public service. In October 1992, the London Ambulance Service (LAS) suffered a disaster. The LAS had implemented a Computer Aided Dispatch (CAD) project in order to automate an ambulance dispatch system. The system was receiving emergency calls and dispatching the closest ambulance, knowing the location of both the caller and the ambulance it prioritised the response in order to provide best coverage and avoid double calls protecting human lives. The system crashed and its operations were stopped for 36 hours something that cost 20-30 peoples lives because the ambulance arrived late to the scene. This was a huge disaster and a huge investigation was held which concluded that neither the system nor its users were ready for full implementation of the system. There are many factors that went wrong and a lot of studies were concluded over the years analysing why this happened. The bottom line is that it is classified as an information security incident since the systems availability

failed. The system was down and due to its critical nature people's lives were lost. We aren't judges nor experts to analyse and provide the root cause of the incident. However, we will give a short overview on what went wrong and lead to the incident according to our obtained understanding of the various findings and studies of this incident. A crucial part of this incident was the common misconception that someone else is responsible for information security and the trivial fact that everyone is responsible for security was lacking. Starting with the CEO and the board of directors of the LAS who blindly trusted the whole project to the project team and the government procurement officer. A procurement officer who although followed to the letter the general governmental guidance on developers and projects bids accepting the cheapest solution and failing to realise that an IT system has different requirement than general acquisitions and that the need for external IT consulting was essential for the choice of the contractor. Something in combination with the absence of both a CRO and CISO lead to a poor risk management and information security implementation. In addition the LAS board of directors was not informed by the project team about their doubts on the CAD developers and their capability on delivering the project in an almost impossible timetable and high risk requirement. This failure of communications, delegation and entrust of deployment of such a critical system to a small group of people led to a failure of compliance with a PRINCE global project management standard of setting up and operating IT systems. Moreover the constant pressure of the board for results and performance improvement lead to additional pressure on the project team increasing the risk tolerance levels. The crucial point of this situation is the lack of clear roles and responsibilities, such as who is responsible for planning, testing the system, educating the users, testing the backup systems, deploying the business continuity, disaster recovery and incidents management plans, performing audits etc., in addition to the insufficient leadership belief that someone else is responsible for information security (thinking of the developer), adding to the fact of the lack of experience of the developers lead to a poor implemented system that eventually failed and cost peoples lives. We could analyse this disaster in a far more detailed way and could lead to an endless discussion but our purpose was just to illustrate that the need of crystal clear definition of roles and responsibilities as well as the crucial need of their good communications is a must for every company-organisation or else any kind of system/product or operation's will end up in a disaster. Thus, because core issues like business unit analysis, risk management etc, wont be properly conducted and communicated leading to a disaster. In addition it once again demonstrates the trivial fact that everyone is responsible for information security and unfortunately, both the trivial fact and the need for roles and responsibilities definition were lessons learned in the hardest and saddest way costing peoples lives.

3.8 Cyber Warfare

In the modern world we hear the term cyber attacks on a daily basis. We have seen a group of hackers named as "Anonymous" performing various denial of service attacks, defacement attacks on governments web servers and private corporations. On 27th April 2007 we witnessed one of the biggest cyber attacks against Estonia where most of the attacks such as DoS, spamming, ping floods etc. affected the general public. This attack was considered to be one of the biggest and most sophisticated attack, rumoured to be sponsored by a government. We have seen another example of such an attack named

Titan Rain which was a series of coordinated attacks on American computer systems since 2003. In the modern world the wars are transferred to the virtual world of the internet and terror scenarios have been already developed claiming that a multifaceted cyber attack coordinated professionally could take down the air traffic control systems, telecommunications grids, create a chaos in the stock market and even deny people from basic needs such as water, electricity and even emergency services such as ambulance dispatch, fire departments and police if the radio bands are silenced figure 45.

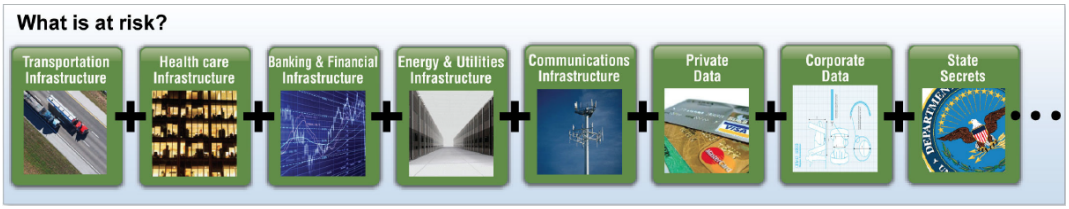


Figure 45: **Cyber Threats**

This scenario as terrifying as it sounds, with the rapid advance of technology and the constant evolution of networks is not far from becoming a reality. The modern world categorises these threats with a buzzword as "The advanced persistent threat (APT)". The APT acronym is constantly misused in the IT security scene and a misconception is generated, people tend to think that APT is a sophisticated malware attack. However it is not the sophistication of the malware rather the attacker's determination and unlimited resources he is willing to allocate to succeed in his mission. And that is the real threat of the APT, It is not a what, but who? The power of the APT lies in the competence, resources and motivation an attacker has who will never stop until he reaches his objectives, whether this is theft of intellectual property or damaging a country or company, he will adapt to the security measures you have deployed and will find a way to breach information security or he will quit if the costs of the attack exceed the value of the prize he is after. We speak of a cyber war between governments where it is very common for intelligence gathering and espionage. However this is no different between companies for competitive reasons. Cyber attacks on companies either for espionage or for the attackers personal benefit is a commonality in our modern world. Attacks such as data theft could be used to blackmail the owners of a company to pay money in order for the attacker not to release the data captured which would expose the information security failure of the company and damage her reputation. The attacker could also threaten the company in performing denial of service attacks taking the company out of business for a while. Both of these cases result in money lost for the company. Cyber threats are a new and evolving source of risks and most of the companies aren't yet prepared to mitigate and handle such risks. There is no secure company in any sector and the threat is growing but nobody can say that the world had not been warned. The world Economic Forum (WEF) in January 2011 placed cyber attacks on the top five threats the world is facing, next to threats of weapons of mass destruction, they emphasise that cyber threats shouldn't be underestimated. We discussed all these examples to highlight the modern threat of cyber attacks a threat which can be apprehended in a company only by clarifying roles and responsibilities. Starting with the CEO who has to understand the risks and the opportunities that the cyber world presents and lead the way to the company's entrance to the

virtual world. The CRO has to conduct constant risk assessments of the cyber threats and with the collaboration of the CISO and CIO to ensure that the IT department is constantly evolving its capabilities to deal with cyber risks. The CISO has to cooperate with other C-level executives and line managers, from which most importantly with the CHRO and the COO in order to develop an awareness campaign and educate the users about the current emerging cyber world and the risks it hides. The CEO with the board of directors have to invest in the development of cyber skills. Thus shaping the strategy of the company in order to mitigate the threats by having experts handling the threats. Thus, the responsibility of the CHRO to recruit talented people and along with the CISO to develop a plan on providing constant education and cyber skills development of employees. Thus, because it is difficult to recruit an expert with those skills in the current market therefore companies have to create their own. The CEO and board of directors have to allocate resources on the cyber threat and ensure its mitigation like any other threat the company faces and one of the core measures is to sponsor the creation of a Cyber incident response team a team that will be able to monitor, gather intelligence about the constant evolving cyber threats and prepare plans to mitigate them communicating from board level to business operations and even cooperating with other companies to strengthen their knowledge and share expertise. In addition, the company's strategy should be aggressive and active against attackers defending the company with legal means prosecuting the attackers. Thus, the requirement of a great CLO who will be well informed on cyber laws and requirements. Last but not least the CMO has to communicate publicly about cyber threats, incidents and responses promoting the cyber threats risks and promoting an information security awareness and culture. This discussion demonstrated the need of clear defined roles and responsibilities and the need of their interactions in order to achieve a cyber-savvy company and mitigate one of the most emerging threats the world and companies are facing.

4 Conclusions & Further Research

This thesis was a turning point for the author's academic career. It covered only a small part of the information security scene positioning in it the roles, interfaces and processes. However, it managed to lay the groundwork for further study of the roles and their responsibilities.

Above all, this work demonstrated the benefits listed below (enumerate) of defining the roles and their responsibilities regarding information security in a company's environment.

Benefits of defining the roles and their responsibilities:

1. They lower the labour costs of information security.
2. They establish an organisational structure avoiding chaos and unnecessary internal politics.
3. They mitigate the risk of information security staff being a single point of failure.
4. They ensure and promote C-level executives support for information security as well as establish formal communication channels with them.
5. They display compliance with internal policies, laws and regulations.
6. They heavily increase employee's efficiency and productivity by eliminating confusion of responsibilities.
7. They enable greater allocation of company's resources minimizing the costs of provision of adequate information security functions.
8. They encourage coordinated team effort firstly, to achieve good information security governance in the company and secondly, safeguard the informations flows of the company.

In this thesis we used the naïve inductivist approach defining at the first part the various roles we can find in a company's environment providing a holistic overview, firstly with an overview of their accountabilities from a management perspective and secondly with a detailed analysis of their security responsibilities and affiliation. We demonstrate the various benefits of placing the roles in the information security scene associating them with many different fronts of information security with each role placing a piece in the informations security scene puzzle. While on the second part we demonstrated with real life examples and scenarios firstly, the necessity of the roles and secondly, and most importantly the necessity of their interactions in order to achieve good information security governance in a company's environment while fulfilling the puzzle of information security and discussing the present, the past and the future of information security. We researched in detail the trivial fact "everyone is responsible for security" illustrating it's meaning for every role showing that each and every role has different and specific responsibilities. A fact that till today posed serious impediments in information security

management because many employees from C-level down to users didn't have a sufficient understanding of their own information security role and responsibility. Thus what we provide, our biggest contribution is a crystal clear delegation of security roles and their responsibilities creating a starting point in better development of information security management. In addition we explained the need of security awareness, education and training starting with the lower user ending to the top C-level management providing valuable insights of the live information security field in the industrial world. In figure 46 listed below we illustrate the holistic overview of the concepts introduced in this thesis.

The research introduced in this thesis provides a natural guide to future research. We revealed a long existing but non-researched domain of information security providing an initial study, which opens the road for gradual study of the domain in deeper levels. Following the research described in this thesis, a number of future studies could derive:

- Technology advances rapidly new features and processes are introduced on a daily basis, concepts as bring your own devices, cloud computing, ARM CPU architecture, powerful mobile devices are constantly changing the IT landscape and with it the information security requirements, therefore a revision of the study should be done over the years identifying and documenting the differences.
- Surveys with far greater resources and workforce power can be conducted to identify organizational structures regarding information security leading to the investigation and research of additional roles and performing their analysis.
- Following the previous point perform surveys to depict accurate data on the interactions of various stakeholder with respect to authority, competence and responsibilities always regarding information security.
- Perform surveys to determine the identified roles responsibilities with accurate statistics adding more responsibilities if any are found to complete the picture.
- Conducting detailed and in depth studies of a scenario or use case in order to demonstrate in detail different interactions of the roles in the information security scene, for example a detailed analysis of the roles actions in a security incident for instance study of the Sony Playstation network data breach.
- Conducting a study testing the hypothesis that the development of state legislations and law requirements of a crystal clear delegation of roles and responsibilities regarding information security would benefit the information security governance of a company.
- Conduct a study of the roles and responsibilities in Small medium enterprises which where neglected in this thesis due to resource limitations.

Summarizing, this thesis opens the path for further research of a hot topic proving the importance of roles distribution and interaction. In addition confirming the trivial fact that everyone is affecting security one way or another in an organisation demonstrating the role of various stakeholders regarding information security and the role of information security regarding them. Illustrative examples justify our approach and highlight in the best way the findings of the thesis which are of great value, those of the responsib-

ilities of each stakeholder regarding information security opening the road in fulfilling an information security consultants dream, of having information security responsibilities attached to the job description and responsibilities of different stakeholders in a company's environment leading to a great information security governance.

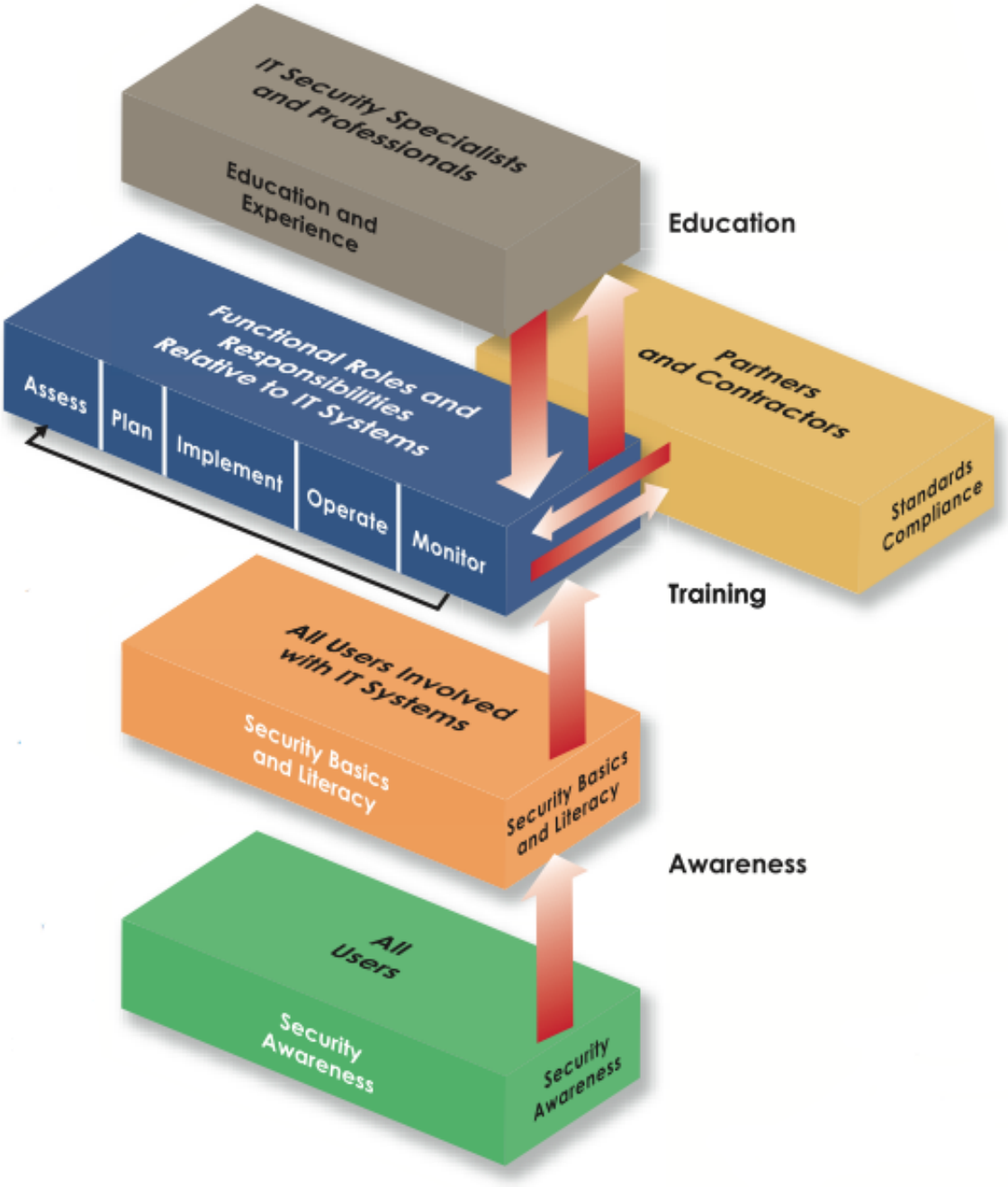


Figure 46: **Holistic overview of the concepts discussed in the thesis**

Bibliography

[1] AT&T. 2003. Achieving network security. *An AT&T survey and white paper in cooperation with the Economist Intelligence Unit*.

[2] Chahino, M. & Marchant, J. 2010. Computer security institute (csi) 2010 annual conference presentation. http://www.csiannual.com/.

[3] Kissel, R. 2011. Glossary of key information security terms. NIST IR 7298 Revision 1.

[4] Council, S. B. I. 2008. Time is now making information security strategic to business innovation. RSA The Security Division of EMC.

[5] Lacey, D. 2009. Managing the human factor in information security how to win over staff and influence business managers. Wiley.

[6] ISO. 2005. Iso/iec 27001 information technology security techniques information security management systems requirements. ISO, Geneva.

[7] ISACA. 2012. Control objectives for information and related technology. ISACA.

[8] Government-Commerce-Office. 2007. Itil v3 service design. The Stationery Office.

[9] NIST. 2008. Performance measurement guide for information security. NIST special publication 800-55 Revision 1.

[10] Savola, R. 2007. Towards a security metrics taxonomy for the information and communication technology industry. IEEE 2nd international conference on software engineering advances.

[11] Brotby, K. 2009. Information security governance a practical development and implementation approach. John Wiley and Sons.

[12] CASCARINO, R. 2007. Auditor's guide to information systems auditing. John Wiley and Sons.

[13] Stewart, J. M., Tittel, E., & Chapple, M. 2008. Certified information systems security professional study guide. Sybex 4th edition.

[14] Grossi, D., Royakkers, L., & Dignum, F. 2007. Organizational structure and responsibility an analysis in a dynamic logic of organized collective agency. Springer Science+Business Media B.V.

[15] TJR, A. & Consulting, G. H. 2009. Organizational structure and analysis. TJR Advisors.

[16] James, S. 2009. Information security: Starting out. SANS Institute InfoSec Reading Room.

[17] Haygroup. 2013. Job analysis. Newcastle University. http://www.ncl.ac.uk/hr/pay/job-evaluation.php (10.02.2013).

[18] Reagan. 2011. Characteristics and qualities of the top performers. Reagan Consulting Leadership Studies.

[19] Lumension. 2013. What every ceo should know about it security. Lumension.

[20] Synnott, W. & Gruber, W. 1981. *Information resource management: opportunities and strategies for the 1980s*. Wiley-Interscience publication. Wiley.

[21] Chun, M. & Mooney, J. 2009. Cio roles and responsibilities: Twenty-five years of evolution and change. *Information & Management*, 46(6), 323 – 334.

[22] Zmud, R. 2000. *Framing the Domains of It Management: Projecting the Future...Through the Past*. The Practice-Driven Research in IT Management Series. Pinnaflex Education Resources.

[23] Modis. 2013. The evolving role of the cio in today's businesses. White paper http://www.modis.com/it-insights/it-white-papers/.

[24] IBM. 2006. The evolving role of the cio. IBM CIO Leadership Forum Survey.

[25] Rahman, H. 2010. *Cases on Adoption, Diffusion and Evaluation of Global E-Governance Systems: Impact at the Grass Roots*. Premier Reference Source. Igi Global, Chapter 12: Roles, Responsibilities and Futures of Chief Information Officers (CIOs) in the Public Sector by Rachel Lawry ,Dianne Waddell and Mohini Singh.

[26] Gentile, M., Collette, R., & August, T. 2005. *The CISO Handbook: A PRACTICAL GUIDE TO SECURING YOUR COMPANY*. Taylor & Francis.

[27] Kouns, B. & Kouns, J. 2011. *The Chief Information Security Officer*. IT Governance Pub.

[28] IBM. 2012. Finding a strategic voice insights from the 2012 ibm chief information security officer assessment. IBM Center for Applied Insights.

[29] ISACA. 2009. An introduction to the business model for information security. ISACA.

[30] SANS. 2003. Mixing technology and business: The roles and responsibilities of the chief information security officer. SANS Institute InfoSec Reading Room.

[31] State, C. 2008. Guide for the role and responsibilities of an information security officer within state government. California Office of Information Security and Privacy Protection.

[32] Ladan, S., Yari, A., & Khodabandeh, H. 2008. Combination of information security standards to cover national requirements. World Academy of Science Engineering and Technology 13 2008.

[33] HKSAR. 2008. An overview of information security standards. The Government of the Hong Kong Special Administrative Region.

[34] Government, S. A. 2012. Government framework on cyber security ocio/f4.1 information security management framework. Office of the Chief Information Officer, Government of South Australia, Information Security Management Framework, version 3.1.1.

[35] Lacey, D. & James, B. E. 2010. Review of availability of advice on security for small/medium sized organisations. http://www.ico.gov.uk.

[36] Zorn, D. M. 2004. Here a chief, there a chief: The rise of the cfo in the american firm. AMERICAN SOCIOLOGICAL REVIEW, 2004, VOL. 69 (June:345 - 364).

[37] Dixit, H. & McCullough, D. 2010. The evolving role of the cfo dealing with the winds of change demands true agility. Aditya Birla Minacs (www.minacs.adityabirla.com)10.03.2013.

[38] Hoehl, M. 2010. Creating a monthly information security scorecard for cio and cfo. SANS Institute InfoSec Reading Room.

[39] vmware. 2011. Aligning cfo and cio priorities. White Paper (http://www.vmware.com) 10.03.2013.

[40] Liu, P. 2013. Information security: The cfo as a speared whale. Interview artical (http://www.cfoinnovation.com/content/information-security-cfo-speared-whale)10.03.2013.

[41] Ernst & Young. 2012. The dna of the coo time to claim the spotlight. White Paper Ernst & Young.

[42] Accenture. 2012. Succeeding in a critical and complex role: A research study on chief operating officers from around the globe. White Paper Accenture.

[43] ITIL. 2007. Itil3 service operation (chapter 5 section 13 pages 101-102). Published by TSO (The Stationery Office) ISBN 9780113310463.

[44] Ernst & Young. 2013. Boardmatters quarterly (january 2013). Ernst & Young.

[45] Midler, L. 2012. Ethics for in-house counsel: Tackling the tough issues. Argyle Executive Forum Chief Legal Officer Leadership Forum (San Francisco).

[46] DeMott, D. A. 2005. The discrete roles of general counsel. Fordham Law Review Volume 74 Issue 3 Article 2 Rev. 955.

[47] Weil, A. 2011. Chief legal officer survey. Altman Weil Inc.

[48] Wright, P., Boudreau, J., Pace, D., Sartain, L., McKinnon, P., & Antoine, R. 2011. *The Chief HR Officer: Defining the New Role of Human Resource Leaders*. Wiley.

[49] CAHRS. 2010. The chief human resource officer: Shifting roles & challenges. 1st Annual CHRO Survey by the Cornell Center for Advanced Human Resource Studies (CAHRS).

[50] Wright, P. M. & Collins, C. J. 2012. The chief human resource officer: Key challenges and strategies for success. Center for Advanced Human Resource Studies (CAHRS) ILR School (Industrial and Labor Relations) Cornell University.

[51] Deloitte. 2012. The evolving role of the chief human resources officer. Deloitte Consulting LLP's CHRO Strategist and Steward Series.

[52] CPNI. 2012. Personnel security practical advice for hr and security managers. Centre for the Protection of National Infrastructure (CPNI).

[53] ISC. 2012. Securing the organization: Creating a partnership between hr and information security. A White Paper from (ISC).

[54] Magazine. 2010. Hr and security...what a team. BANKERS' HOTLINE VOLUME XX, NUMBER 7.

[55] EIU. 2005. The evolving role of the cro. A report from the Economist Intelligence Unit Sponsored by: ACE Insurance, Cisco Systems, Deutsche Bank and IBM.

[56] Culp, S., Mouille, C., & Ebersbach, K. 2011. The changing face of risk management. White Paper Accenture.

[57] Brown, L. 2010. The chief risk officer: your business ally. Deloitte in the Middle East.

[58] Cognos. 2008. Top 10 answers from the world's first chief risk officer. Cognos, an IBM company.

[59] STEP. 2013. Course: Information security management in e-governance day 3 session 1: Information security audits. STEP http://step.nisg.org (10.4.2013).

[60] Government. 2008. Information security audit (is audit) a guideline for is audits based on it-grundschutz. German Federal Office for Information Security 2008 Version 1.0.

[61] Popescu, G., Popescu, A., & Popescu, C. R. 2008. Conducting an information security audit. Manager Journal N07 http://manager.faa.ro (10.04.2013).

[62] SUDUC, A.-M., BIZOI, M., & FILIP, F. G. 2010. Audit for information systems security. Informatica Economica vol. 14, no. 1/2010.

[63] Allen, C. 1999. Preparing for an external security audit. eServ pty. LTD.

[64] Hein, R. 2004. The application audit process - a guide for information security professionals. SANS Institute InfoSec Reading Room.

[65] Kowalski, S. 1994. *IT Insecurity: A Multi-disciplinary Inquiry*. PHD Thesis Department of Computer & Systems Sciences. Stochholm University.

[66] Tarimo, C. & för data-och systemvetenskap (Stockholm), I. 2006. *ICT Security Readiness Checklist for Developing Countries: A Social-technical Approach*. Report series / Department of Computer & Systems Sciences. Department of Computer and Systems Sciences, Stockholm University.

[67] Jorro, Y. B. 2011. Information system security audit readiness case study: Ethiopian government organizations. Department of Computer and Systems Sciences, Stockholm University.

[68] H.J.H.MacFie & Meiselman, H. L. 1996. Food choice acceptance and consumption. Page 267 chapter 7.2.

[69] SpencerStuart. 2006. The changing influence of the chief marketing officer. SpencerStuart.

[70] Egan, N. & Pearson, M. 2006. The chief marketing officer: An evolutionary role. Building News: Marketing Handbook for the Design and Construction Professional Third Edition Chapter 6 section 13 pages 581-591 ISBN10-1557013691 ISBN13-9781557013699.

[71] GANDHI, S., RODRIGUEZ, G., & BANKS, G. 2012. From mad man to superwoman. Deloitte.

[72] McGovern, G. & Quelch, J. A. 2012. The fall and rise of the cmo. Harvard strategy and business issue 37.

[73] Research, F. & Struggles, H. . 2012. The evolved cmo. Forrester Research and Heidrick & Struggles.

[74] IBM. 2011. From stretched to strengthened. IBM Global Business Services.

[75] Day, G. S. & Malcolm, R. 2012. The cmo and the future of marketing. Marketingpower.

[76] Partners, C. 2009. The cmo's agenda: Cmo 2.0. CMG Partners.

[77] Council, C. 2006. Secure the trust of your brand both reports the full and the executive summary report. A CMO Council research initiative in collaboration with Emory University/Zyman Institute of Brand Science and Sponsored by: Opinion Research Corporation.

[78] Ettlie, J. E. & Eisenbach, J. M. 2007. The changing role of the r & d gatekeeper. Research-Technology Management, Volume 50, Number 5, pp. 59-66.

[79] Shields, R. G., Speed, E., Walsh, P. B., & Wheatley, M. V. 2006. The evolving role of the r&d leader in the consumer packaged goods industry. A study by the Spencer Stuart Consumer Practice.

[80] Yarnada, I., Yamasaki, H., & Baba, J. 2001. The role of the r & d manager in the age of reform. In *Change Management and the New Industrial Revolution, 2001. IEMC '01 Proceedings.*, 113–117.

[81] Parvatiyar, A. & Sheth, J. N. 2001. Customer relationship management: Emerging practice, process, and discipline. Journal of Economic and Social Research 3(2) 2001, 1-34.

[82] BOLTON, R. N. & TARASI, C. O. 2007. Managing customer relationships. Review of Marketing Research (Review of Marketing Research, Volume 3), Emerald Group Publishing Limited, pp.3-38 ISSN: 1548-6435.

[83] Agrawal, M. 2003. Customer relationship management (crm) & corporate renaissance. Journal of Services Research, Volume 3, Number 2 (October 2003-March 2004) by Institute for International Management and Technology.

[84] Agrawal, M. 2003. Customer relationship management (crm) & corporate renaissance. Journal of Services Research, Volume 3, Number 2 (October 2003-March 2004) by Institute for International Management and Technology.

[85] Chen, I. J. & Popovich, K. 2003. Understanding customer relationship management (crm) people, process and technology. Emerald Research Business Process Management Journal Vol. 9 No. 5, 2003 pp. 672-688.

[86] Chen, I. J. & Popovich, K. 2003. Understanding customer relationship management (crm) people, process and technology. Emerald Research Business Process Management Journal Vol. 9 No. 5, 2003 pp. 672-688.

[87] Sage. 2011. The evolution of crm building a true customer relationship strategy. Sage (UK) Limited.

[88] Lee, H., Chen, K. L., Shing, C.-C., & Shing, M.-L. 2006. Security issues in customer relationship management systems (crm). Decision Sciences Institute 37th Annual Conference Bricktown - Oklahoma City March 1 âĂŞ 4, 2006.

[89] LaFrance, J. 2003. Security for a crm environment. SANS Institute InfoSec Reading Room.

[90] Meeks, R. 2005. Your role in information security. UW Medicine, Center on Human Development and Disability.

[91] Motorola. 2010. The user role in information security building effective and efficient environments in the age of mobility and social networking. WHITE PAPER: INFORMATION ASSURANCE SERVICES Motorola, Inc. www.motorola.com/services/government (10.4.2013).

[92] Bogart, K. J. 2012. Information security awareness: How to get users asking for more. Shaping the Future of IT Management Information Systems Eller College of Management The University of Arizona.

[93] NIST. 2009. Information security training requirements: A role- and performance-based model (draft). NIST Special Publication 800-16 Revision 1 (Draft).

[94] SWIFT. 2012. Growth, risk and compliance: The case for a strategic approach to managing reference data. SWIFT with cooperation with Delloite.

[95] Mathew, J. & Zimmerman, M. 2012. The role of the chief data officer in financial services. Capgemini Consulting Techonology Outsourcing.

[96] Lee, Y., Chung, W., Madnick, S., Wang, R., & Zhang, H. 2012. On the rise of the chief data officers in a world of big data. Accepted for presentation at the PreâĂŘICIS 2012 SIM Academic Workshop, Orlando, Florida.

[97] Accenture. 2009. Painting a portrait of the chief procurement officer. Accenture Consulting Techonology Outsourcing.

[98] SpencerStuart. 2010. Agent of change the chief procurement officer and the transformation of corporate procurement. Spencer Stuart.

[99] Bartolini, A. 2012. Cpo rising. Ardent Partners sponsored by Ernst and Young.

[100] Sandslätt, P. 2013. 2012-13 global chief procurement officer survey. Capgemini Consulting Techonology Outsourcing.

[101] Koetzle, L. & Gavin, M. 2006. Outsourcing - opportunities and security risks. Microsoft and the Swiss Security Exchange. Report conducted by Forrester Consulting.

[102] Pala, F. & Melzi, E. 2009. Facility management organizational models. OPEN FACILITY MANAGEMENT A successfull implementation in a public administration Alberto F. De Toni, Alberto Ferri, Mattia Montagner Chapter 4 pages 84-104.

[103] Koetzle, L. & Gavin, M. 2006. converging world of physical and it security: what is the value to the business? Microsoft and the Swiss Security Exchange. Report conducted by Forrester Consulting.

[104] van Eersel, F. 2012. The role of the facility manager within bcm. Business Continuity Journal, Volume Three, Issue Two.

[105] GWM. 2009. Understanding business insurance. GWM Adviser Services Limited.

[106] Böhme, R. 2005. Cyber-insurance revisited. Workshop on the Economics of Information Security (WEIS) 2005. Kennedy School of Government, Cambridge, MA, USA.

[107] Anderson, R. J. 1994. Liability and computer security: Nine principles. In Dieter Gollmann, editor, Computer Security (ESORICS '94), LNCS 875, pages 231-245, Berlin Heidelberg, Springer Verlag.

[108] Porter, M. 2004. Competitive advantage. Free Press, New York.

A Appendix

In the following pages you will find attached some examples/proposals of the job descriptions of the roles covered in the thesis.

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Data Officer
Reports to:	CEO
Administrative Report to:	CEO
Additional Report to:	Board of Directors
Reporting to this position:	Program Directors and Business Manager
Scale of organisation:	Number of employees

Job Summary

Chief Data Officer someone to lead all strategic data activities and to represent Data as a strategic asset that DRIVES business and that helps lead the company in new directions.

Accountabilities

Disciplinary Assignment:	Development of policies and procedures for data handling.
Principal Duties:	Data handling.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • ✉ *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 8 years experience in a senior management position. As chief data officer, this individual demonstrates critical competencies in broad categories: data quality, data governance, data management, data security, data assessment, data usage.

Working Experience: 8 years in relative field.

Personal qualities: Strong communication skills, strong analytical skills , and project management expertise.

Management oriented Tasks & Responsibilities

1. Ensuring data quality in a company.
2. Overseeing data management.
3. Data governance. (Thus assisting the company's governance by using statistics based on the data analysis.)
4. Data assessment. (It is the process of evaluating data using analytical and logical reasoning to examine each component of the data.)
5. Establishing guidelines for data usage.
6. Assist into shaping company's vision by transforming data in valuable information.

Security oriented Tasks & Responsibilities

1. Assist in the Development of security controls, policies and procedures of data handling.
2. Ensure security measures and develop policies to ensure that data privacy requirement are met.
3. Ensure company's overall compliance with the Data Protection Act.
4. Monitor changes in the PDA and ensure that the company takes appropriate steps to comply with the new requirements.

Recruiters officer name – address of company
phone number • *email address*

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Executive Director
Reports to:	Board of Directors
Administrative Report to:	Board of Directors
Additional Report to:	Board of Directors
Reporting to this position:	Program Directors and Business Manager
Scale of organisation:	Number of employees

Job Summary

Top executive responsible for a firm's overall operations and performance. He or she is the leader of the firm, serves as the main link between the board of directors (the board) and the firm's various parts or levels, and is held solely responsible for the firm's success or failure. One of the major duties of a CEO is to maintain and implement corporate policy, accomplish the company's mission and vision, oversee the day-to-day operations of the company and assist the board of directors in the governance functions.

Accountabilities

Disciplinary Assignment:	Development of annual goals and objectives
Principal Duties:	Decision maker, Manager, Leader, Visionary and Board Developer

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 12 years experience in a senior management position. As chief executive officer, this individual demonstrates critical competencies in four broad categories: commitment to results, business savvy, leading change, and motivating.

Working Experience: 12 years in relative field

Personal qualities: Strong communication skills, fund raising successes, and project management expertise

Management oriented Tasks & Responsibilities

1. Provide administration and support to the Board and the Staff.
2. Allocate Human resources wherever necessary. Manage HR policies and issue instructions.
3. Ensure proper function and delivery of Products and Services.
4. Manage financial resources, including taxes revenue generation and risk management.
5. Conduct proper investment plans.
6. Assure Law compliance and company's policies development.
7. Manage Public Relationships create a good community profile for the company.
8. Fund-raising oversee project developments to attract investors. Forecast opportunities seal profitable deals.

Security oriented Tasks & Responsibilities

1. Make Security a Board Issue.
2. Allocate resources to security. Make security investments.
3. Change company's culture and thinking. Security is no longer just a part of the IT it is part of the whole company.
4. Promote the belief that everyone is responsible for security.
5. Assure that proper plans on how to deal with incidents such as contingency plans, disaster recovery plans, business continuity plans are conducted.
6. Defence in depth.

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Financial Officer (CFO)
Reports to:	Board of Directors
Administrative Report to:	Board of Directors
Additional Report to:	CEO
Reporting to this position:	Program Directors and Business Manager
Scale of organisation:	Number of employees

Job Summary

The senior manager responsible for overseeing the financial activities of an entire company. The CFO's duties include financial planning and monitoring cash flow. He or she analyses the company's financial strengths and weaknesses and suggests plans for improvement. The CFO is similar to a treasurer or controller in that he or she is responsible for overseeing the accounting and finance departments and for ensuring that the company's financial reports are accurate and completed on time.

Accountabilities

Disciplinary Assignment:	Management of company's Financials
Principal Duties:	Decision maker, Finance and Accounting, Financial Planning and Analysis, Visionary and Merges and Acquisitions

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • ✉ *email address*

Qualifications & Skills

Required:

Education:	A Master's Degree is required with a minimum of 5-8 years experience in a senior management position. As chief Financial officer, this individual demonstrates critical competencies in financial reporting , internal controls, planning and control, cost accounting, projects, restructuring, mergers and acquisitions, implementation of ERP's, planning systems, tax planning.
Working Experience:	12 years in relative field
Personal qualities:	Strong communication skills, IFRS, Cost Accounting, Mergers, Restructuring, Financial Planners, Project Management, Forecasting, Internal Controls, Financial Reporting, Business Planning and Innovation

Management Related Responsibilities

1.Business Strategy	Assess annual organizational performance. Assist in establishing yearly objectives and goals. Oversees strategic long-term budgetary planning and costs management in alignment with the board of Directors.
2.Financial Planning and Analysis	Conducts regular financial planning reports. Conducts analysis of financial conditions of the company and forecasts financial expectations. Develop and execute analysis of various business initiatives. Develop and maintain capital budget.
3.Finance and Accounting	Oversee cash flow planning and ensure availability of funds as needed. Oversee cash, investment, and asset management. Ensure legal and regulatory compliance regarding all financial functions. Lead the development of accounting gimmicks to lower taxes and increase revenue.
4.Insurance and Real Estate	Manage company's insurance program. Manage the company's real estate affairs.
5.Merges and Acquisitions	Plan, develop and execute merges and acquisitions. Conduct analysis, forecast and provide future outcome of penitential merges and acquisitions.
6.Business value and Exit plan strategy	Conduct analysis recommend innovations to grow business value and companies stock value. Develop and oversee the exit plan strategy for the company.

Security Related Responsibilities

1.Security Culture	A CFO should be a security aware person. Allocate appropriate resources and funding for continuous improvement of security. Treat security as business risk.
2.DRP and BCM	Participate and assist the CISO in the development of Disaster Recovery, Business Continuity strategies and plans.
3.Compliance	Oversee and enforce compliance with regulations to avoid fines and penalties.
4.Ensure financial assets security	Ensure that financial deals, contracts, auctions, forecasts, product launch dates and prices are things that are within the information that has to be protected and can affect the financial well being of a company.

5. Information Security in M&A Ensure proper Information security infrastructure exists in the acquired company and compliance with regulations is at place and in order.

6. Bring-your-own-device policies They raise a lot of security concerns and issues, such as data losses, in appropriate usage of the devices, unauthorised access to the devices of non personal of the company and many more yet not fully revealed threats and risks to be handled and mitigated. If the CFOs haven't started to pay attention, now's the time to do it!

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Human Resources Officer
Reports to:	CEO
Administrative Report to:	CEO
Additional Report to:	Board of Directors
Reporting to this position:	Employees
Scale of organisation:	Number of employees

Job Summary

Top executive responsible for hiring new employees, supervising employee evaluations, mediation between employees and bosses as necessary, and general overseeing of the personnel department.

Accountabilities

Disciplinary Assignment:	Delivery of high quality human resources services that include enhancing controls for human capital processes and mitigating risk around HR.
Principal Duties:	Develop framework for HR services, Recruit employees, Evaluate employees performance.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 8 years experience in a senior management position. As chief Human Resources officer, this individual demonstrates critical competencies in broad categories: Human management, talent scouter,recruiter and coach, value creator, strategist.

Working Experience: 8 years in relative field.

Personal qualities: Strong communication skills, excellent analyst and great people's judger and reader.

Management oriented Tasks & Responsibilities

1. The CHRO is a talents developer, he is a coach that will assist, guide, reward and motivate the employees in order to maximize their efficiency and productivity to assist the company achieve its goals.
2. The CHRO has to be a great analyst and judge of character in order to hire the right people for the right position.
3. A CHRO as a C-level executive is a business partner, a key advisor to the board of directors and the CEO in the shaping of the companies strategy towards the companies goals and objectives.
4. A CHRO will evaluate the employees performance and take appropriate measures if necessary.
5. A person who will solve any conflicts that might raise between employees, despite their rank, top level employees or simple staff and create a happy and friendly working environment.
6. The CHRO will assist and oversee the daily governance functions of a company, such as arrange board meetings, interact with employees, en- sure regulatory compliance and oversee and assure high quality human resources services that include enhancing controls for human cap- ital processes and mitigating risk around HR.

Security oriented Tasks & Responsibilities

1. Knowing the cultural background of a potential employee reduces the risk of employing personnel likely to present a security concern.
2. The CHRO is in an ideal position to drive security messages, policies and procedures.
3. The CHRO keeps track of the access privileges a employer has, had to perform his duties and when those have to be terminated.
4. The CHRO has to establish that applicants and contractors are who they claim to be.
5. The role of the CHRO is to assist and provide counsel and solutions interacting with the CISO in order to mitigate all this risks.
6. CHRO will provide valuable insight, in understanding the elements of the job, and they will help prepare the investigator to ask the right questions, and help preserve the rights of the suspect employee.
7. The CHRO has to have a very good understanding of what Information Security means to a company and what kind of people and skill-set are needed to perform such job.

Recruiters officer name – address of company
phone number • ✉ *email address*

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Information Officer
Reports to:	Board of Directors, Chief Executive Director
Administrative Report to:	Chief Executive Director
Additional Report to:	Board of Directors
Reporting to this position:	IT Managers
Scale of organisation:	Number of employees

Job Summary

A company executive who is responsible for the management, implementation and usability of information and computer technologies. The CIO will analyse how these technologies can benefit the company or improve an existing business process and will then integrate a system to realize that benefit or improvement.

Accountabilities

Disciplinary Assignment:	Establishment of corporate information policy, standards and management control over all information resources.
Principal Duties:	Responsible for developing and maintaining Information Systems Infrastructure, Information Systems.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • *email address*

Qualifications & Skills

Required:

Education: A Master's Degree in Business or Computer Sciences is required with a minimum of 10 years experience in a senior management position. As chief executive officer, this individual demonstrates critical competencies in three categories: IT Strategy and Planning, IT Acquisition and Deployment, IT Operational Management.

Working Experience: 10 years in relative field.

Personal qualities: Enjoy working in a collaborative management style. Excellent written and oral communication skills. Excellent interpersonal skills. Strong negotiating skills. Ability to present ideas in business-friendly and user-friendly language.

Other Skills: Good Knowledge of business theory, business processes, management, budgeting, and business office operations. Good knowledge of data processing, hardware platforms, enterprise software applications. Proven 3 years experience with systems design and development from business requirements analysis to daily management.Demonstrated ability to apply IT in solving business problems. In-depth knowledge of applicable laws and regulations as they relate to IT. Strong understanding of human resource management principles, practices, and procedures.

Management oriented Tasks & Responsibilities

1. Identifying, promoting, and managing IT-enabled business agility.
2. Innovating and integrating IT in the enterprise
3. Communicating the impact of business decisions on IT costs.
4. Prioritizing and negotiating IT-enabled business initiatives.
5. Moving beyond managing the IT utility (supply perspective) to managing IT demand and value creation.
6. Demonstrating IT business value while maintaining IT goodwill among corporate executives.

Security oriented Tasks & Responsibilities

1. Identify what information has to be protected.
2. Develop an awareness of information's value and the need for its protection both to the staff and the board of Directors.
3. Build and promote trust culture in handling information in the company.
4. Collaborate with CISO and develop an information security strategy and policy framework that will safeguard the information.

Recruiters officer name – address of company
phone number • ✉ *email address*

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Information Security Officer
Reports to:	Board of Directors
Administrative Report to:	Board of Directors
Additional Report to:	CEO
Reporting to this position:	Security Officers
Scale of organisation:	Number of employees

Job Summary

Top executive that focuses on information security strategy within an organization. This security strategy can vary depending on the needs of an enterprise.

Accountabilities

Disciplinary Assignment:	Development of Security Policy, Architecture and Governance.
Principal Duties:	Assure the protection of information and it assets in the company.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • ✉ *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 10 years of information technology experience including 5 years of management experience with solid background in information security.

Working Experience: 10 years in relative field

Certifications: Professional security management certification, such as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or other similar credentials.

Personal qualities: Excellent staff management skills, Good technical knowledge of security technology, business system continuity planning, auditing, and risk management, Strong analytical, evaluative and problem solving abilities.

Tasks/Responsibilities

1. Risk Management.
2. Security Policy Management.
3. Organizing Information Security.
4. Ensure Asset Protection.
5. Integrate Human Resource Security.
6. Ensure Physical and Environmental Security.
7. Communication and Operations Management.
8. Develop Access Control measures.
9. Lead Information Systems Acquisition, Development and Maintenance.
10. Lead in Security Incident Management.
11. Participate in Disaster Recovery Management.
12. Ensure Compliance with laws and regulations.
13. Conduct Information Security Economics justify Security investments.

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Legal Officer
Reports to:	CEO
Administrative Report to:	CEO
Additional Report to:	Board of Directors
Reporting to this position:	Legal Department Personnel
Scale of organisation:	Number of employees

Job Summary

A publicly traded company's most powerful legal executive. The Chief Legal Officer (CLO) is an expert and leader who helps the company minimize its legal risks by advising the company's other officers and board members on any major legal and regulatory issues the company confronts, such as litigation risks. The CLO may also be a member of the company's operating committee and is overseen by the CEO. The CLO oversees the company's in-house attorneys.

Accountabilities

Disciplinary Assignment:	Handling Legal and Compliance issues.
Principal Duties:	Legal Adviser to Corporation and Its Constituents,Corporate Officer and Member of Senior Management Team, Administrator of the Internal Legal Department,Agent of the Corporation in Dealings with Third Parties.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 8 years experience in a senior management position. As chief legal officer, this individual demonstrates critical competencies in broad categories: Law keeper, compliance enforcer, negotiator and mediator, legal representative.

Working Experience: 8 years in relative field.

Personal qualities: Strong communication skills, Excellent legal knowledge, strong analyst and intuitive person, Visionary, quick decision maker.

Management oriented Tasks & Responsibilities

1. Advice the board and the CEO in the governance of the company, bring different ideas and diversity to the board of directors.
2. A CLO has to be preventive and proactive. He is a trusted advisor who has to forecast and assist in the governance of the company keeping it in track with regulations and promoting a legal culture in the company.
3. A CLO is required to create and manage the Legal department including recruiting talented personnel, cutting costs, managing budget and oversee departments procedures.
4. The CLO has to be a strong mediator and negotiator and represent and protect the company's interests in dealings with third-parties.
5. The CLO might be the lead litigator ,if the case is critical for the company, or act as an adviser on strategy to senior lawyers throughout the litigation process.

Security oriented Tasks & Responsibilities

1. The CLO is the person who will create the need for information security.
2. The CLO will assist in the shaping of the information security governance of a company.
3. The CLO has to ensure that the company's information security complies with the regulations and standards introduced by law.
4. The CLO has to keep in track all the changes in the law that affect the information security and inform the CISO of them assisting him into dealing with possible compliance issues.

Recruiters officer name – address of company
phone number • *email address*

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Marketing Officer
Reports to:	CEO
Administrative Report to:	CEO
Additional Report to:	Board of Directors
Reporting to this position:	Program Directors and Business Manager
Scale of organisation:	Number of employees

Job Summary

Chief marketing officer (CMO) is the company's executive responsible for corporate branding, advertising, marketing channels, customer outreach and all other marketing aspects. The CMO is considered part of the top management tier with responsibilities which generally cross all company product lines and geographic regions.

Accountabilities

Disciplinary Assignment:	Development of Marketing strategy and structure.
Principal Duties:	Brand Development, advertisements campaigns, Marketing services, Growth management.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • ✉ *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 8 years experience in a senior management position. As chief Marketing officer, this individual demonstrates critical competencies in broad categories: commitment to results, business savvy, brand development, advertisements campaigns, marketing services, growth management, marketing ROI.

Working Experience: 8 years in relative field.

Personal qualities: Strong communication skills, leadership skills, project management expertise, strong market knowledge, strong analytical skills, visionary skills.

Management Related Responsibilities

1.Public relations and events. The CMO has the responsibility to promote the company and man- age the flow of information from the company to the public.

2.Marketing Services The CMO has to oversee the development of advertisement campaigns, the protection and development of company's brand name, he has to create value for customers as individuals.

3.Growth Manager The CMO is responsible for the market research and analysis. He has to familiarise himself with the trends and modern technology and market globalization in order to explore market opportunities and size them when they are beneficial for the company.

4.Leader and Cooperate advisor The CMO has to possess strong analytical skills and out of the box thinking in order to contribute to the development of a robust business strategy, vision that will ensure a good marketing policy and development in the company.

5.Marketing ROI The CMO has to be able to perform a Return on the investment (ROI) analysis and forecast and provide proofs of success or fail- ure in terms of numbers to the CEO and the board of directors.

Security Related Responsibilities

1.Value Creator The CMO has to use information security to promote the company's solid approach to information security and data privacy and develop or expand the brand name and reputation of the company.

2.Information flow keeper The CMO has to ensure that appropriate measures and controls are taken to protect information leakage about marketing events, procedures, services that could harm and affect the company.

3.Key Media Handling The CMO has to be prepared to handle the media appropriately and in advantage of the company's interests when a security breach occurs.

Recruiters officer name – address of company
phone number • *email address*

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Operations Officer
Reports to:	Board of Directors, CEO
Administrative Report to:	CEO
Additional Report to:	Board of Directors
Reporting to this position:	Program Directors and Business Manager
Scale of organisation:	Number of employees

Job Summary

Top executive responsible for a firm's overall operations and performance. He or she is the leader of the firm, serves as the main link between the board of directors (the board) and the firm's various parts or levels, and is responsible for the implementation of company's mission and vision as defined by the CEO and board of director's. The COOs primary task is to oversee the day-to-day operations of the company and assist the CEO in governance functions.

Accountabilities

Disciplinary Assignment:	Development of annual goals and objectives
Principal Duties:	Decision maker, Manager, Leader, Visionary and Business transformer and innovator.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 8 years experience in a senior management position. As chief operations officer, this individual demonstrates critical competencies in many broad categories: commitment to results, business innovation and transformation, leading change, and motivating.

Working Experience: 8 years in relative field.

Personal qualities: Strong communication skills, business development and project management expertise.

Management oriented Tasks & Responsibilities

1. Ensuring suitable operations management.
2. Optimizing operational processes.
3. Designing a framework to implement strategy into operations.
4. Managing the strategic assets of the company.
5. Driving key change and transformation initiatives.
6. Shaping the future of the business.

Security oriented Tasks & Responsibilities

1. The COO has to ensure that the staff of his department are following the tasks and acknowledge the responsibilities assign to them by the Information Security Policy of the company and report any suspicious activities to the security department.
2. The COO should ensure that the staff receives proper and continuous training and familiarise themselves with the security policy and procedures of the company.
3. The COO has to ensure that the operations department is capable and willing to provide technical assistance to the IT security Department.
4. The COO has to ensure that Security and Human Resources departments are informed before hiring third-party contractors.
5. The COO has to report to the Security Department a list of people where is specified the purpose and the time that a staff member will have access to critical systems.
6. The COO has to oversee, the creation and documentation of a user manual regarding information security procedures of the operational department.

Job Description

Company's name

Chain of Command Information

Position Title:	Chief Risk Officer
Reports to:	CEO
Administrative Report to:	CEO
Additional Report to:	Board of Directors
Reporting to this position:	Program Directors and Business Manager
Scale of organisation:	Number of employees

Job Summary

Chief Risk Officer (CRO) is the executive responsible for identifying, analysing and mitigating internal and external events that could threaten a company. The chief risk officer works to ensure that the company is compliant with government regulations and reviews factors that could negatively affect investments or a company's business units.

Accountabilities

Disciplinary Assignment:	Risk Management
Principal Duties:	Risk analysis, Enterprise Risk Management ERP, Strategy developer and advisor.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • ✉ *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 10 years experience in a senior management position. As chief risk officer, this individual demonstrates critical competencies in broad categories: Strategic risks, Environmental risks, Market risks, Credit risks, Operational risks, Compliance risks, IT risks.

Working Experience: 10 years in relative field.

Personal qualities: Strong communication skills, Excellent risk analysis skills, Organizational and project management expertise.

Management Related Responsibilities

1.Compliance The CRO has to identify the policies, standards and regulations with which the organization is required to comply.

2.Privacy The CRO has to identify and establish the privacy requirements for the information flows in the company according to government regulations and laws and company's policy.

3.Finance Risk The CRO has to evaluate financial risks that the company is exposed to such as credit, capital, investments, fraud and any other financial risks that may occur in a company's activities.

4.Market and Strategy Risk The CRO has to evaluate potential impacts of business activities and events initiated by market activities and company's overall strategy.

5.Operational Risks The CRO has to identify business process risks and analyse in what extent they may affect the business utilizing appropriate risk response measures.

Security Related Responsibilities

IT related Risks The CRO has to create a risk assessment on the IT threats and vulnerabilities and provide to the CISO the hierarchy of the information that needs to be protected.

2.Information Security The CRO has to provide the overall risk tolerance of the company to the CISO for him to develop controls that will mitigate the risks accordingly to the risk acceptance of the company.

3.Advisor The CRO has to participate in the disaster recovery and business continuity plans providing valuable insight regarding the risk-profile of the company.

4.Risk Coordinator The CRO is a coordinator of risk that receives valuable information from various departments regarding threats and risks and integrates them into a united framework providing back risk profiles and the overall risk tolerance of the company to them to act and align accordingly.

Recruiters officer name – address of company
phone number • ✉ *email address*

Job Description

Company's name

Chain of Command Information

Position Title:	IT security Auditor
Reports to:	CEO
Administrative Report to:	CEO
Additional Report to:	Board of Directors
Reporting to this position:	Supervisor, audit's staff
Scale of organisation:	Number of employees

Job Summary

IT Security Auditor is the person responsible for the Scrutiny of an organization's physical, financial and computer access control procedures and systems to determine its level of vulnerability to attacks or intrusions from unauthorized personnel or criminals.

Accountabilities

Disciplinary Assignment:	Information Security Audit.
Principal Duties:	Information Security Audit. Development of audit report, Vulnerability report, threats/risks report.

Physical Demands/Working Conditions

Any specific conditions such as stressful job, relocations etc.

Recruiters officer name – address of company
phone number • *email address*

Qualifications & Skills

Required:

Education: A Master's Degree is required with a minimum of 7 years experience in IT security audits. As IT security Auditor, this individual demonstrates critical competencies in broad categories: Information Security frameworks/standards, IT security audit, Vulnerability assessment and risk analysis, IT security architecture, IT security policies and procedures evaluation, Information Security legal compliance regulations.

Working Experience: 7 years in relative field.

Personal qualities: Deep understanding of the IT Security products, Experience with leading and documenting IT Security Audits and Risk Assessments, Understanding of IT Security policy and procedures and their enforcement, Strong problem solving skills, strong communications skills, strong collaborating skills.

Responsibilities

1. The verification of the effectiveness of the company's IT security.
2. Preparing the ground for the IT security audit process to kick off.
3. Evaluation of company's financial and IT systems identifying any possible frauds, mismanagement, misuse, dysfunction of resources, procedures and controls.
4. Evaluation of effectiveness, efficiency and most importantly compliance of company's security processes and procedures with global accepted best practices and government laws and regulations.
5. Propose solutions to resolve the potential issues that the audit findings might reveal.

Recruiters officer name – address of company
phone number • *email address*