IS Risk Practices From A CST Perspective: A Literature Review

Martin Lundgren
2014

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering
“The scientific man does not aim at an immediate result. He does not expect that his advanced ideas will be readily taken up. His work is like that of the planter—for the future. His duty is to lay the foundation for those who are to come, and point the way.” (Tesla, 1900, p. 211)
ABSTRACT

Aim; This review analyzes how information security risk practice literature differ in light of ideology and consequences on emancipation. Background; It is argued that information security (IS) has been dominated by functionalist and interpretive paradigms whereas the critical research stands undeveloped. To shed some light over this matter IS literature were analyzed from a Critical Social Theory (CST) perspective. Theory; In doing so, the framework developed by Thapa and Harnesk, based upon Haberma’s concept of four orientations in information systems development, illuminating the IS risk practice ideology as either Predictive & Controlled or Complex & Unpredicted and its consequence of the practice as Emancipatory or Non-Emancipatory, was undertaken. Method; A systematic literature review was conducted utilizing the suggested approach by Okoli and Schabram and the Framework developed by Ritchie and Spencer in conjunction with Webster and Watson. Result; A number of 52 articles, over a period of ten years and spread across 36 various outlets, were reviewed and synthesized, resulting in 26 articles recognized as instrumental, 19 as strategic, 7 as communicative and 0 as discursive. Conclusion; The majority of the literature was recognized as more functionalist and interpretive, although more recent literature seems to upbring a more critical approach. The different orientations’ IS risk practices tend to differ in scope and focus; from controlling and monitoring (instrumental), to co-operation and perspective (strategic), to understanding and expectation (communicative). Furthermore, emancipation seems to have practical impact as the different orientations suggest, in various forms, that IS risk practices could pose as an obstacle for the employees. This in turn seems indicate that there is no common understanding, structure, of IS risk practices ideological perspective and its consequence on emancipation.

Keywords: Critical Social Theory, Information Security, Risk Practice, Systematic Review
## INDEX

1 Introduction..................................................................................................................................................1  
  1.1 Background........................................................................................................................................1  
  1.2 Problem Description............................................................................................................................2  
  1.3 Scope & Limitation.................................................................................................................................2  
  1.4 Disposition.........................................................................................................................................3  
2 Theory..........................................................................................................................................................4  
  2.1 IS Rik Practices......................................................................................................................................4  
  2.2 A Critical Perspective...........................................................................................................................5  
3 Method..........................................................................................................................................................7  
  3.1 Search Strategy.......................................................................................................................................8  
  3.2 Practical Screening.................................................................................................................................8  
  3.3 Quality Appraisal....................................................................................................................................9  
  3.4 Data Extraction & Synthesis Of Studies.................................................................................................9  
  3.5 Writing The Review..............................................................................................................................11  
4 Literature Overview......................................................................................................................................12  
5 Result..........................................................................................................................................................13  
  5.1 Instrumental.........................................................................................................................................13  
  5.2 Strategic...............................................................................................................................................18  
  5.3 Communicative.....................................................................................................................................23  
  5.4 Discursive.............................................................................................................................................25  
6 Discussion....................................................................................................................................................26  
7 Conclusion...................................................................................................................................................30
1 INTRODUCTION

1.1 BACKGROUND

In this modern day and age organizations, governments and businesses etc. tend to be more computerized and the need for access and availability of data and information grows. In organizations, for example, the information system is not only there to reinforce organizational control, but is further capable of inspire criticism, to facilitate learning, and to raise the overall organizational competence (Lyytinen and Hirschheim, 1988). Indeed, nowadays some organizations cannot survive without direct access to certain information (Suh and Han, 2003). Information security (henceforth referred to as IS) thus comes as an unfortunate byproduct of this accelerated trend to keep these services operational while preserving confidentiality, integrity and availability.

However, common for IS practices tend to be the focus on ideologies which stress securing the asset and often dominated by functionalist and interpretive paradigms (Dhillon and Backhouse, 2001). Whereas the critical research in information systems security stands rather underdeveloped (Talib and Dhillon, 2010).

A central concept of critical research is the ideology (Stahl, 2007). The ideology can be defined as “representations of aspects of the world which can be shown to contribute to establishing, maintaining and changing social relations of power, domination and exploitation” (Stahl, 2007, p. 39). These, Stahl (2007) argues, are not necessarily based on bad faith, but something which is taken for granted, a shared conceptualization or construction of the social reality. It can however be argued that ideology limits the world view of the individual, and is as such a counter force to the main aim of critical research, that is to say, emancipation (Stahl, 2007).

Limiting the individuals’ world view, or in the case of IS their access or involvement, creates inequality. Not only by power, but also decision making and can thus lead to oppression, which in turn might render the individual alienated (Talib and Dhillon, 2010). Why, one might wonder, is this relevant to IS? As stated by Talib and Dhillon (2010), the critical research within systems security is not well explored. However, looking towards other fields and discipline which been using the critical security, such as politics and human research, we find some interesting thoughts and similarities. For example, in human security the traditional security thinking derives from military threats and strong counters (Booth, 1991). Human and critical security strives to reverse this traditional system of having a state responsible for security and its people supporting it. Instead, making the state support the people, while scrutinizing the state, questioning its cause and interest (Newman, 2010). For security, this becomes interesting as Booth (1991, p. 319) argued that “true (stable) security can only be achieved by people and groups if they do not deprive others of it”. From an IS perspective, maybe even more so, as an increase of individual emancipation can lead to better IS alignment with the organization and thus render higher protection of information (Talib and Dhillon, 2010), or in case of increased individual freedom and involvement, may render the end-user more eager to take part in the security practices (Siponen, 2000).

What we see is that there are a number of perspectives concerning IS risk practice based upon different approaches, practices and paradigms. The question of how IS risk practice literature reflect these matters from a critical perspective naturally arise from the discussion above – or rather, how risk practices differ in light of ideology and consequence on emancipation?
1.2 PROBLEM DESCRIPTION

As will be further explored in later chapters, there is a lack of knowledge from a critical perspective of IS risk practices, and so there is an importance to highlight the current literature and depict how and what has been addressed. IS is, as well as management, a fairly young field of research and needs as such literature reviews to back up its theoretical foundation, indeed, “review articles are critical to strengthening IS as a field of study” (Webster and Watson, 2002, p. 14). For this reason the following research question is posed to address this research gap and to situate IS risk practice within the critical research;

• How does information security risk practice literature differ in light of ideology and consequences on emancipation?

The contribution of this posed question is really two-folded. Firstly, the IS risk practice literature is studied in respect to the critical social theory. Of course, in no way will this deem different practices or approaches right or wrong, but instead contribute to a deeper understanding of the current knowledge in the field, and hopefully point out and inspire new research areas in need for further exploration. Secondly, highlighting these practices and differences may contribute to practical insight of the security concept and its relation to ideology and emancipation. From a practitioner’s perspective this may render helpful managerial insight, illuminating variables which may affect IS management outcomes. For example, if we look again toward the field of critical security for guidance, emancipation means not only absence of oppression, but also constraints which may stop individuals from performing tasks they otherwise would have chosen to perform (Booth, 1991). What if IS risk practices could pose as such a constraint?

1.3 SCOPE & LIMITATION

The aim of this thesis was to analyze the existing IS risk practice literature to highlight its differences on ideology and consequences on emancipation.

The environmental scope of this thesis situates itself quite naturally to that of an organization, where the subject of social interactions and oppression may be expected to be more evident. This limits however the scope to focus on a wider perspective (see section 2.1), and neglects as such pure technicalities, like interventions and implementations for example, which otherwise arguably speak in favor of the instrumental orientation (see section 2.2).

To study the IS risk practice ideology in perspective to its consequence on emancipation, a literature review to situate the existing literature within the critical field seemed fitting. However, due to a strict time limitation this literature review only covered peer-reviewed articles written in English and published between 2004 till 2014. All articles were gathered using the “Primo-library” search engine, utilizing a boolean search. The selected keyword, in relation to the restrictions composed, yielded 5 081 articles in total – though only 1 000 of these were targeted by the search strategy and practical screening (see section 3.1 and 3.2). This particular limitation was due to two reasons. Firstly, due to time, secondly, due to a steady increase in repeating articles.

As a result, a number of 52 articles, over a period of ten years and spread across 36 various outlets, were collected. The motive behind the selection, as discussed in section 3 and reflected in figure 3, was to get as wide a perspective as possible. Publications from different outlets and disciplines, as well as a timespan of ten years, seemed proper. It must as such also be noted that IS
literature was not exclusively selected, although making for the core literature, but also literature from other journals and disciplines found to discuss and handle IS and risks. However, when analyzing the many abstracts, much of the literature was found to be conceptual in its outlining (see figure 4). To get a more practical perspective, it was reasoned that technical reports (still within the inclusion criteria, see section 3.2) could shed some light upon the IS and risks practices, and were as such also included to the selection.

To guide the extraction and synthesis of the IS risk practice towards answering the research question, the CST framework developed by Thapa and Harnesk (2014) in conjunction with the framework analysis by Ritchie and Spencer (2002) seamed proper (see section 2.2 and 3.4).

1.4 DISPOSITION

Section two discusses the theoretical aspects of the subject, information security risk practices and the framework used. Section three explains the method of data gathering, what database and search criteria were used. In section four a brief literature overview of the articles gathered are displayed. Section five presents the result of the literature review. Section six is dedicated for a discussion concerning the result and the theory from section two, which leads us to section seven, where a conclusion regarding the problem description from chapter one will be drawn and propose further extensions.
2 Theory

As IS threats keeps evolving IS could arguably be said to be in a constant domain of change. The word change here is not as in changing something, but rather reflects the dynamic nature of an environment. One type of practice to identify and assess IS risks is by risk management. However, implementing and undertaking such practices (see section 2.1) are of course itself a target of change. There is a number of articles which advocate different practices for implementing IS risk practices (e.g. Bojanc and Jerman-Blažič, 2008; Chan, 2010; Williams, 2008) but these are often dominated by functionalist and interpretive paradigms (Dhillon and Backhouse, 2001). Whereas the critical research in information systems security stands rather underdeveloped (Talib and Dhillon, 2010).

To better understand and bind the critical research with the ideology of IS a definition of what IS risk practices means and how it is referred to in this study might be helpful.

2.1 IS RIK PRACTICES

The concept of IS risk practice can be defined in numerous ways. However, to better illustrate how it is referred to in this thesis the concept is defined by studying each word and its definition. Splitting these words apart, we find that the mere word risk (taken from Oxford Dictionaries), which derives from Italian *risco* meaning “danger”, can be described as “a situation involving exposure to danger”, or in regard to organizational IS as “the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization” (ISO/IEC 27005, 2008). The word practice can be described as (taken from Oxford Dictionaries) “the actual application or use of an idea, belief, or method, as opposed to theories relating to it”, or in regard to a social group experience Wenger (1998, p. 51) suggests that “practice is, first and foremost, a process by which we can experience the world and our encounters with it as meaningful”. IS is widely agreed to consist of the following three requirements (taken from Siponen and Oinas-Kukkonen, 2007, p. 62); information should not be modified by unauthorized subjects (integrity); information should be available to authorized subjects when required (availability); improper disclosure of information should be detected and prevented (confidentiality) [...] ensure that in trading or contracts one cannot afterwards deny an action (e.g., signing a contract) that one has carried out (non-repudiation).

Now, if we synthesize these definitions we get something like; a process of an idea, belief or method that is collectively experienced as meaningful regarding a situation or asset(s) integrity, availability, confidentiality and/or non-repudiation potential exposure to danger or threats. Meaningful here is referring to encounter the world as offering particular structures and opportunities (Dourish and Anderson, 2006).

IS risk practices can thus be seen as part- or the background of IS risk management, as IS risk management is concerned with the very process of not only identify these risks, but also to prioritize, assess and monitoring them (Spears and Barki, 2010).

In conclusion, risk practices will henceforth address not raw technical risks or practices so often found within this field. Instead, a much wider perspective is undertaken, inviting for the many concepts of risks, binding them as composed above. Thus including, but not limited to, these interventions to technical, social and even economic perspectives. This is fundamental as the scope of this thesis was not that of highlighting what works but rather what concepts and ideologies are at work?

---

1 http://www.oxforddictionaries.com/
2.2 A CRITICAL PERSPECTIVE

The problem with ideology is that it is often perceived as absolute truth and thus unchangeable. For example, the security literature often depict security as protection of a particular asset, explaining how a certain practice is expected to function, often benefiting some groups over some other groups, with little regard to other possible stakeholders (Stahl, 2007; Thapa and Harnesk, 2014). Thus, by implementing IS risk practices (as described in section 2.1 as a process of an idea, belief or method) the manager(s) ideology comes into play. This, however, as argued by Stahl (2007), may limit the world view of the individual which from a critical social theory (CST) comes into conflicts with the idea that emancipation is needed for the individual to realize his or her full potential. Indeed, the “critical social theory is a mode of reflection that looks critically at processes of social development from the point of view of the obstacles they pose for human flourishing” (Cook, 2004 see Granter, 2009, p. 31).

The research question posed aligns closely to what Stahl (2007) depict as the context of critical research; as the arena of addressing issues of ideology and emancipation. Therefore, the framework developed by Thapa and Harnesk (2014), which focus on the IS risk practices ideology and its consequence on emancipation of the individual seemed fitting to utilize. The framework highlights the CST aspect and is built upon Haberma’s work in distinguishing between four orientations in information systems development (ISD) change. The first two orientations, the instrumental and strategic, emphasize control. Whereas the communicative orientation looks towards creating shared meanings, sense-making, and the fourth, the discursive orientation, looks at clarifying or justifying claims through argumentation (Hirschheim et al., 1996).

As can be seen in figure 1, the orientations are recognized by the IS risk practices ideology as being either Predictive & Controlled, or Complex & Unpredicted. The different orientations and their consequence of emancipation are described below:

**Instrumental:** This orientation treats its domain as controlled and is focused on achieving given ends, something that has been socially predefined (Hirschheim et al., 1996). That is to say, the instrumental action is engaged when an actor applies technical rules from empirical knowledge or theoretical models, selecting and implementing means which promises result for a certain situation (Janson et al., 2001). This orientation is directed towards agents (human and non-human), seen as manipulative objects fit to serve the actors need (Lyytinen and Hirschheim, 1988). The concept is thus
success oriented, something which is done by deriving predictions on physical and behavioral models (Lyytinen and Hirschheim, 1988). The nature of this approach, in regard to risk practices, Thapa and Harnesk (2014) describes as being operated within a neutral and well-behaved environment, and that it treats the IS risks as a dependent variable which is explained as a function of independent variables. For example, risk practice selected and implemented will immediately and evenly be adopted across the organization (Thapa and Harnesk, 2014). However, Thapa and Harnesk (2014) further argues that due to the fact that the instrumental approach is so preoccupied with the predicted events it renders the approach insensitive towards changes in its procedure.

**Strategic:** This orientation is also relying on control in that the actor needs to affect agents/actors to achieve their goal. This in turn craves that each actor has an accurate picture of the relationships of facts (Janson et al., 2001). That is to say, the agents are by this orientation seen as an intelligent counteraction, which must be measured and taken into account for. For example, what may benefit one actor, might be noxious for another, thus forcing the actor to co-operation, as well as accommodation, in order to find the best strategy to pursue his or her goal (Lyytinen and Hirschheim, 1988). From a IS risk perspective, Thapa and Harnesk (2014) discusses the strategic dimension opens up for the reflection of coordination and co-operations between stakeholders and organizational functions. However, these opinions are rarely fully adopted into the risk practice as the ideal view of risk practice still impregnates risk management. Something which has been seen in other IS research, e.g. developing instruments for controlling, measuring and quantifying internal as well as external risk factors (Thapa and Harnesk, 2014). As such, Thapa and Harnesk argue, this orientation in terms of emancipation still treats employees as objects.

**Communicative:** For the communicative orientation, sense-making is central, meaning that no goals set by the actors are egocentric in the sense that the participants strive to use a cognitive process, language, to reach a common understanding. The essential difference between the coordinating mechanism found in both the instrumental and strategic orientations and the communicative orientation is that the latter is not motivated by individual profit, but instead focused on the common interpretation of the action situation (Janson et al., 2001). That is to say, finding and agreeing upon shared interpretations of a given action or event to e.g. enhance, progress, and or maintain meaning, ideas and plans (Hirschheim et al., 1996). This orientation from a IS risk perspective, Thapa and Harnesk (2014) discusses the characterization of sense-making from a number of sources as the cognitive process of commitment, capacity and expectation. This in turn is seen as critical for e.g. the individual compliance towards managerial regulations, as its effect can be seen as a result of the learning environment found in the organization (Thapa and Harnesk, 2014).

**Discursive:** As a result of a problematic, or in the case where a shared background cannot be taken for granted, communicative practice has taken place the discursive dimension takes shape. Initiated by doubt or ambiguity this orientation emphasizes communication and validity of claims as the target of communicative interest (Lyytinen and Hirschheim, 1988). For example, an actor could demand that another actor educe evidence which prove his or her claims as either true, right with respect to commonly agreed norms, or sincere (Janson et al., 2001). This however craves an environment free of oppression or domination, an “ideal” speech situation for each part to interact with minimalistic power imbalance (Janson et al., 2001). From an IS risk perspective the communicative challenges of risk ideology for example could be to spread its underlying rationality (Thapa and Harnesk, 2014). Furthermore, Thapa and Harnesk (2014) argue, the discursive orientation invites an arena of debates to shape the very risk practice, transforming it as socially conditioned.
3 Method

In contrast to the traditional literature review the systematic review utilizes a more rigorous approach in reviewing a specific subject, search question or topic area, where all the steps are predefined (Kitchenham, 2004). Okoli and Schabram (2010), in their guide to conduct systematic reviews within the field of information systems, describes this rigorousness as depending on the transparent and well defined search and selection strategy used. Okoli and Schabram (2010) refer to a compiled set of four important phases for a systematic literature review, all of which they argue, are essential for a rigorous review; Planning (Purpose of the literature review & Protocol and training); Selection (Searching for the literature & Practical screening); Extraction (Quality appraisal & Data extraction) and Execution (Synthesis of studies & Writing the review). These were, in consent with some of the guidelines suggested by Ritchie and Spencer (2002) and Webster and Watson (2002), the foundation of this chapter. Each phase were planned and structured before progressing any further; a predefined search protocol as stressed by Kitchenham (2004). Note, however, that phase one has been excluded as Purpose of the literature review is discussed in section 1.2 and 1.3. Protocol and training has also been excluded as its focus lies in bringing multiple researches to the same page, to ensure consistency, with equal expectations regarding the literature, its conduction and purpose. It is also worth mentioning that the Data extraction phase and Synthesis of studies has been merged due to methodological reasons (see section 3.4).

![Figure 2. A figure describing the research design; from purpose and theory input, to systematic output](image)

The decision behind utilizing Okoli and Schabram’s (2010) proposed steps in conducting this review was due to a number of reasons. First, Okoli and Schabram (2010) focus the outlining of a rigorous systematic review to information systems research. This is important as “information systems is a combination of social science, business, and computing science, whose research methods are different from those of the health sciences, from which the systematic review methodology has largely been developed” (Okoli and Schabram, 2010, p. 7). Furthermore, the fact that this review is within the field of information systems, and thus must balance articles in both qualitative and quantitative methodologies, will play a significant role when it comes to the collection of data, as will be discussed later. Secondly, Okoli and Schabram (2010) presents a clear set of phases in conducting the systematic review which were applied to produce a concept centric approach with additional input from both Ritchie and Spencer (2002) Framework of analysis and the concept-centric matrix as suggested by Webster and Watson (2002), while reducing risk of bias.
3.1 SEARCH STRATEGY

Derivation: As discussed in section 2.1, the IS Risk Practice can be seen as part of the management process and must be recognized as such. This becomes important when outlining the search strategy. David et al. (2003) argues that the systematic review draws upon “raw data” and is as such much conformed with the positivism, quantitative studies, and can more easily present articles relevance and quality while addressing the question of “what works”. Dixon-Woods et al. (2006) addresses this issue as well and concludes that the exclusion criteria regarding qualitative articles are not as clear and that there is no unison approach to this. In the making of Okoli and Schabram’s (2010) work, the authors highlights this as well and note that in all review-articles found, in the closely related management field, none followed the same method or structure. Whereas quantitative systematic review usually undertakes some form of inclusion criteria, for example the use of randomized controlled trial (RCT) to ensure that the articles meet a particular quality or standard (this will be further highlighted in relevance to section 3.3).

This, David et al. (2003) argue, influence the collection of articles which tends to be more qualitative, e.g. the field of management, where the “raw data” is seldom presented. Instead, articles within the field of management tends to present only part studies, satisfying the orientation of a particular journal and presenting only the findings (David et al., 2003). These articles are thus often text-based and rich in meaning. Furthermore Dixon-Woods et al. (2006) takes the same view, arguing that practical problems arise when trying to define “what works” questions for the more qualitative literature. Notably here is that due to its affect on the article collection (David et al., 2003; Dixon-Woods et al., 2006) the search should not be limited to a particular study design or journals (Dixon-Woods et al., 2006; Webster and Watson, 2002), see section 3.2.

Search strategy; Seen from the research question posed in section 1.2, and the reasons discussed above, this literature review recognized the need to explore “what are at work” rather than “what works”. As such, and to allow for a more holistic perspective, literature was collected throughout a period of ten years, 2004 till 2014. No limitation to a specific method found in the different articles was undertaken, as well as any limitation towards what field the study was carried out in. Only articles available online and in English were reviewed, using “Primo-library” as the initial source as it provides a wide array of journals and conference proceedings. The following keywords were used;

• "information security" AND risk* practice* OR manage*2

In addition, the articles of particular relevance, and referring to previous work, were used to conduct a backwards search, reviewing also these referred articles to broaden the perspective even further.

3.2 PRACTICAL SCREENING

Derivation: This phase specifies in short the inclusion and exclusion of the articles retrieved from the search. Note however that this phase does not include any exclusion based on quality – that will be explained in the next phase; quality appraisal. Instead, this phase focus on the following two

---
2 The citation looks for an exact match, AND and OR are boolean operators, and * allows for additional characters, e.g. risk* render hits for risk, risks, risked etc.
categories of practical criteria, as noted by Okoli and Schabram (2010, p. 21); according to whether the study’s content is applicable to the research question; and according to explicitly defined, albeit perhaps arbitrary, criteria chosen in order to restrict the total number of articles considered so that the literature review may be practically manageable. As such, the articles’ abstracts were carefully reviewed and only those articles which matched the following criteria were selected:

**Inclusion criteria;** 1) the articles must be written in English; 2) only articles published in peer-reviewed journals or conference proceedings; 3) only articles published within the time-frame of ten years, ranging from 2004 till 2014.

**Exclusion criteria;** 1) articles focusing on specific technical subjects with no reflection or inclusion of organizational or social perspective/concern (e.g. articles addressing only raw technicalities like intervention, implementation or benchmarking); 2) article not accessible online; 3) articles not peer-reviewed; 4) articles which did not meet the quality appraisal (see section 3.3); 5) study proposals and commentaries.

The selected articles were stored and subjected to detailed examination against these criteria again. For each detailed examination notes were composed motivating why (if) a particular article was excluded. For the articles kept, each articles “meta-information” (paper title, author names, research approach, method used) were stored into a concept-matrix as suggested by Webster and Watson (2002).

### 3.3 QUALITY APPRAISAL

This phase address the quality found within the articles collected, a type of methodological screening (Okoli and Schabram, 2010). The importance of this step is evident, but poses some difficulties as discussed in section 3.1, regarding qualitative and quantitative articles. Due to the epistemological differences in qualitative and quantitative methods the proposed quality appraisal was selected not to be too specific, addressing only the following items, as presented by Hart (1999, see Okoli and Schabram, 2010, p. 29) to be screened; what claims are being made, what evidence is provided to support these claims, if the evidence is warranted, and how it is backed. These are broad questions, and make the quality appraisal target for interpretation. However, drawing on the research question, which strives to explore the ideology and consequences on emancipation impregnating the literature (see section 1.2), I wished not to exclude relevant literature due to their quality – unless fundamentally flawed.

### 3.4 DATA EXTRACTION & SYNTHESIS OF STUDIES

**Derivation;** This literature review explores how information security risk practice literature differ in light of ideology and consequences on emancipation. As discussed above (see section 3.1) practical issues arise when considering “what are at work” as a more qualitative type of question rather than “what works”. This applies to the data extraction as well. As with all systematic literature review studies, the data extraction and synthesis must be predefined, specifying what to extract and what to analyze to reduce risk for bias (Kitchenham, 2004). However, due to qualitative methods and the nature of the research question, this becomes target for thematization through generalization and categorization. Many methods for data extraction and synthesis were considered, for example, Critical Interpretive Synthesis developed by Dixon-Woods et al. (2006), Narrative summary, Grounded Theory,
Hermeneutics and Meta-Ethnography. All good alternatives to extract and synthesize qualitative data. However, none of said methods allowed for the data extraction to be guided by an existing issue or framework – that is to say, without force-fitting data into a given framework, rendering the process difficult to repeat and not very transparent.

Instead, inspiration was taken from Noyes and Popay (2007, p. 230) which notes that “in qualitative research, theory is the vehicle through which arguments about explanation and generalizability can be developed”, although notes that one should be concerned to what extent the theory applies so as not to generalize beyond the research sample. As such, Noyes and Popay (2007) developed a thematic framework during their review. Indeed, a framework to guide the data extraction, and later on synthesis, was seen as critical to answer the research question while not generalizing beyond the research question. This also complies with what Ritchie and Spencer (2002) argue that in qualitative data analysis it is essential to undertake a method which allows for categorizing, theorizing and mapping. For this, Ritchie and Spencer (2002) have developed a framework named, confusingly enough, “Framework”. Although Ritchie and Spencer’s framework is a method for applied qualitative research and not specifically developed for literature reviews, Okoli and Schabram (2010) notes that depending on the research question, common methods for qualitative research are applicable to literature reviews as well.

To better comply with the theory as discussed in section 2.2, while prevailing focusing on answering the research question, the data extraction method saw fit to follow the systematic process proposed by Ritchie and Spencer (2002), as it allows for summarizing and classifying data into categories or domains predefined by an existing theoretical- or conceptual framework. Furthermore, it allows for analyzing data between themes, making it more than just a systematic thematic analysis. Ritchie and Spencer’s framework consist of the following phases (described below); familiarization, identifying a thematic framework, indexing, charting, and mapping & interpretation. In addition, the data extraction phase should also include details of the information source (David et al., 2003), something which is not covered by the proposed framework, but instead undertaken by the concept-matrix as described by Webster and Watson (2002) (see section 3.2).

1. **Familiarization**: during the familiarization phase, the articles were read and the process of conceptualization and abstraction began. Key concepts were noted down, together with ideas and different aspects, arguments and motivations for emerging themes.

2. **Identifying a thematic framework**: this phase is concerned with identifying a particular framework. A framework here is broken down into categories with including codes (the frameworks “concepts”, instead of wring the whole name, this is a form of indexing). The Framework method allows for new frameworks to emerge, but notes that if an existing framework is undertaken (as in this case), this phase may be excluded (Gale et al., 2013).

3. **Indexing**: in this phase data were extracted, with references, into a spreadsheet under a fitting category and code. The categories were extracted from the framework as discussed in section 2.2, but also a category for what type of IS risk practice had been utilized or reflected, as discussed in section 2.1.

4. **Charting**: the charting involved summarizing the extracted data into a spreadsheet matrix, “lifting” the data from its original context (Ritchie and Spencer, 2002). Of course keeping citation and references to quotes (as this matrix was designed by case-order, not theme, it seemed fitting to extend the already case-ordered concept matrix as seen in section 3.2).
5. **Mapping & Interpretation:** in the final phase differences, relationships and parables in the data and categories were explored. According to Ritchie and Spencer, what to analyze should be guided by the research question, and as such, concepts and associations were in focus. Ideas and concepts noted down from the familiarization phase were also used in analyzing the data.

**Data extraction:** As much of the articles’ meta-data had already been collected (see section 3.2) the data extraction process focused on illuminating and extracting data in accordance with section 2.2. A data extraction form was created and applied for all articles, following the framework as suggested by Ritchie and Spencer (2002). The resulting chart (as described above) was appended to the already existing concept-centric matrix (see section 3.2), resulting in a complete data extraction matrix.

**Data synthesis:** The resulting data extraction matrix was analyzed as described in the last phase of Ritchie and Spencer’s framework. Data were thus read vertically by concept, and synthesized so as to describe the common theme of each category and how these relate to the study, not only list the extractions. The framework helps as such also in pointing out themes and/or concepts which may go beyond that of the framework. Strong points of differences or overlaps between categories were noted down for the discussion (see section 6).

### 3.5 Writing the Review

To better highlight the synthesis result in light of the research question the result section were divided into two chapters. The first, section 4, presents a literature overview and depicts the collection scope, the number of articles found and in what particular orientation (as discussed in section 2.2). The second, section 5, presents the result of the synthesis. The latter were divided into the given orientations, illuminating its ideology, emancipation and risk practice. Each extraction synthesis were then merged into a logical flow, focusing more on depicting the many articles’ key concept for each orientation heading, rather than just listing the synthesis.
4 LITERATURE OVERVIEW

In total, 52 articles were reviewed. Of these 8 are journal articles within the field of information systems, 11 articles from security journals, 24 from various other fields handling IS and risks, and 9 technical reports. The articles were published in 36 various outlets.

The result of the data gathering, practical screening and inclusion/exclusion were applied as reflected in figure 3.

As illustrated in figure 4, conceptual papers were by far the most common. These were articles which did not present or indicated any research method, but reasoning and demonstrating their conclusions.

As seen in figure 5, illustrating the different orientations and their year of publication, the instrumental and strategic orientation were by far recognized by most articles. Moreover, this overview also depict the research attention among the different orientations. Agreeing, to some extent, that IS literature has been dominated by functionalist and interpretive paradigms.

What is more, the publications recognized as more critical, the communicative orientation, although few, seems to have been publicized in quick session, and rather “late” compared to the other orientations.

No articles were recognized by the discursive orientation.

Figure 3. A QUOROM flow diagram reflecting the research

Figure 4. Research methods

Figure 5. Illuminating the time of publication and orientation
5 Result

5.1 Instrumental

The instrumental orientation invites (as discussed in section 2.2) for a neutral and well-behaved environmental view in which to achieve given ends, treating IS risks as a dependent variable which is explained as a function of independent variables.

Risk management within the instrumental orientation is drawn towards success, and as such, to facilitate control. Atyam (2010) describes the business technological requirement of technology centric solution as either 1) “Protect the FORTRESS (business operations) and bolster the defenses with the required FACADES (technology solutions)” or 2) “Strengthen the FAÇADE (technology solutions) for any weakness in its effectiveness” (Atyam, 2010, p. 344). Atyam (2010) further argue that there is a great need to quantify the impact of the information security risks on the business process, to allow for business level insight at the management level. Such an approach “allows the organizations to understand and prioritize the security risk management activities that make the most sense for their organization to secure the business operations instead of trying to protect against every conceivable threat” (Atyam, 2010, p. 343). Vijayaraghavan et al., (2010) agrees with this and recognizes also a great need for a quantitative security strength approach as the many existing standards to “certify the strength of a security system are qualitative, lack consideration of the countermeasures and do not consider the impact of security breaches.” (Vijayaraghavan et al., 2010, p. 213). As such, Vijayaraghavan et al. (2010) propose a framework, called iMeasure Security (iMS), to analyze – or rather to quantify – the “security strength of an enterprise system by considering the countermeasures deployed in its network, analyzes the business impact of the security breaches, and provides insights as to how the level of security can be improved from current levels.” (Vijayaraghavan et al., 2010, p. 213).

Atyam (2010), Chan (2010), Imamverdiev and Derakshande (2011) and Lo and Chen (2012) agrees that utilizing practices of risk impacts and likelihood can aid in identify and understand risks. Lo and Chen (2012), for example, in their article present a type of hybrid procedure for evaluating risk levels for risk management. The process utilizes Decision Making Trial and Evaluation Laboratory (DEMATEL) to construct relationships among current security controls, and Analytic Network Process (ANP) to determine the likelihood of a risk. Lastly, it uses Fuzzy Linguistic Quantifiers-guide Maximum Entropy Order-Weighted averaging (FLQ-MEOWA) to aggregate impact vales assessed by experts. Ou Yang et al. (2013, p. 483) argues that by “understanding the performance gaps of the implemented controls to an assumed ideal performance level is important for assessing the effectiveness of the various risk controls, compromise-programming methods can be used to rank the risk-control areas or objectives”. Further, Ou Yang et al. (2013, p. 499) notes that there is often many uncertain influences and factors which affect risk management, for example “human beings determine the risk value, risk probability of occurrence of security breach, or the consequence of occurrence of security breach according to their experiences”. This, Ou Yang et al. (2013) notes, becomes subject for subjectivity, something that ANP can help overcome. As such, Ou Yang et al. (2013) propose an MCDM model in combination of VIKOR, DEMATEL and ANP to solve the problem of criteria and feedback often missing in the “check Phase” in an PDCA process of information security management. Imamverdiev and Derakshande (2011) discuss the information security risk management from a
Fuzzy OWA model perspective. Imamverdiev and Derakshande (2011) argue that the Fuzzy OWA model can be used for managerial decision-making to reach better countermeasures and reduce information security risks. The model proposed weights criteria based on information entropy by a given situation. Chan (2010) argue for the need of a checklist-type model, and propose a Bayesian index model for measuring enterprises’ information security, and note that “the likelihood ratio for each IS risk item can be referenced for decision making on IS protection measures” (Chan, 2010, p. 637). Huang et al. (2006) developed a balanced scorecard-framework to set up the performance index for information security management in organizations. This, they argue, may strengthen the linkage between performance indicators and progressive business strategy. The framework consist of four measures of perspectives; Financial, Customer, Internal business process and Learning & growth. From a security perspective these contribute to illuminate the “growth, profitability, and risk viewed from the perspective of the shareholder […] strategic priorities for various business processes that create customer and shareholder satisfaction […] preservation of confidentiality, integrity and availability for information asset to keep business value” (Huang et al., 2006, p. 243). The methods for measuring information security management performance, Huang et al. (2006) argue, are closely related to that of IT performance evaluation, as both schemes aim to unify information assets and safeguard information value. Important to realize is that information is an asset of value, and as such needs to be protected in order to minimize business damage and maximize ROI (Huang et al., 2006).

Smith et al. (2007) introduced a model to illuminate risks, trying to identify those processes and linkages that are vulnerable to IT related threats and its origin – ranging from organizational, network as well as environmental sources; “by isolating the point of origin for IT-specific threats, we are able to identify points of vulnerability within the system and thereby customize risk mitigation strategies.” (Smith et al., 2007, p. 2606). “By focusing on not only the type of threat but also its point of origin, we are able to allocate resources to more effectively combat threats that may span multiple risk sources” (Smith et al., 2007, p. 2606). Smith et al. (2007) further argue that the increase of communicative systems have removed the protective barriers around assets and processes and that it increases the sources of risks, and as such may exploit vulnerabilities which may affect the chain’s ability to satisfy a customer’s demand.

In contrast, Dai et al. (2012, p. 318) argue, that many “enterprises’ information security measures are simply device-level protection; this is just a pile of related security products, not a solution”. Security risk management is a very systemic and dynamic process, affected by many factors. As such Dai et al. (2012) model borrow from the plan–do–study–act (PDCA) cycle and is constructed in four steps; object establishment, risk assessment, monitor & audit and risk control. Dai et al. (2012) propose a dynamic risk management model for information security management within the IC manufacturing industry. Dai et al. (2012) argue that the very essence of security management is risk management, and that the goal of implementing any information security risk management is to discover and eliminate risks in time. Doherty and Fulford (2006) discuss the importance of having the strategic information systems plan (SISP) and the information security policy steadily aligned. As the organizational strategy and plan evolves so must the organizations’ information security policy as well. For example, “a strategic drive to increase the number of customers using an organisation’s website might not warrant any explicit changes to the organisation’s IS/IT provision, but it might have indirect implications for information security” (Doherty and Fulford, 2006, p. 58). The information security policy will as such act as a framework to ensure that systems are not only developed but also operated in a secure fashion.
Chaudhry et al. (2011) propose a conceptual framework based upon four major issues (pillars); security policy documentation, employee awareness, top management support, and access control. These Chaudhry et al. (2011, p. 587) argue are the “key drivers associated with establishing an enterprise information security system.” All of these pillars will together work as the best way to make enterprise information systems secure, “however removing any one of these columns can truly diminish the stability/security of the entire system” (Chaudhry et al., 2011, p. 595). Wangwe et al. (2012) discusses developing and implementing an information security framework in a resource poor country, in this particular case Tanzania, where there is a great need for cost effective and sustainable implementation. The framework builds upon three “pillars”, governance, operational and technical, all of which adapts a service oriented architecture. The pillars allow for solutions to be mapped between, forces involvement of technical operators and managers, and craves “awareness sessions between technical and management teams are held every six months to review activities in each team and determine where solutions need to be mapped to each other” (Wangwe et al., 2012, p. 126).

Jones (2009) on the other hand propose an alternative view of user awareness and discuss how information made more user friendly and more visible can provoke better security. Jones (2009) notes that information security really makes it harder for employees to act in a secure manner as the security procedures “are largely hidden from the user and have been made to achieve their function without visible signs of activity and are not visually checkable” (Jones, 2009, p. 213). Most, if not all, of the security is managed by the organization’s security and systems staff. The users most certainly have some understanding of the physical security, means which they maybe use at home to protect their personal assets. Unfortunately, Jones (2009, p. 214) notes, “people do not apply the same level of security protection to their ‘invisible assets’, the information that is of value to them that is stored and processed on computers.” And so this becomes an issue for awareness. To tackle the issue of compliance and awareness, Bhardwaj and Singh (2011), Hentea (2007), Knapp et al. (2009), Mazzariello et al. (2011), Ross (2008), Roy Sarkar (2010), Veiga and Eloff (2007) and Zeadally et al. (2012) all propose the advantage of automation tools to inspect and to detect non-compliance behavior and argue that automated processing can help maintain great compliance.

This, Ross (2008) argue allows for information security functions to enforce policy standards. However, easy access to the compliance rules, laws, policies, guidelines and regulations etc. must exist. To enforce compliance and better monitor the environment a “log of enforcement-related events is also needed. This is essentially a record of all known instances of non-compliance. The log must be supported with an organizing structure that differentiates the most serious from the trivial events.” (Ross, 2008, p. 8). Hentea (2007) describe the use of intelligent systems to help managers in their work to keep up with the growth of cyber-attacks, and propose architecture for an Intelligent System for Information security Management. This, Hentea (2007, p. 29) describes, aims at “improve security management processes such as monitoring, controlling, and decision making with an effect size that is higher than an expert in security by providing mechanisms to enhance the active construction of knowledge about threats, policies, procedures, and risks”. Hentea (2007) argue there is a need for this sort of tool as many of the current security routines rely on human interactions, patching and analyzing new vulnerabilities. This could instead be a task for a monitoring system, however, policies tends to change and as such there is a need for feedback functionality, by which network administrator or security staff can add new rules to the system (Hentea, 2007). In Veiga and Eloff (2007) collects a number of existing frameworks for information risk practice and management. From these they extracted the essence and built a new framework which may be used by organizations to better ensure
information security from a holistic perspective (Veiga and Eloff, 2007). However, it is “essential to measure and enforce compliance, and both technology and employee behavior should be monitored to ensure compliance with information security policies and to respond effectively and timely to incidents that are detected” (Veiga and Eloff, 2007, p. 370). The whole concept also utilizes metrics to measure the effectiveness of organizations risk practices. Mazzarrello et al. (2011) present the development of behavior models, tools and algorithms for detecting unwanted events within a VoIP infrastructure.

Knapp et al. (2009) discuss information security policy, and present a policy process based on responses from certified information security professionals. This model, Knapp et al. (2009) argue, reflects as such recommended practice and illustrates internal and external influences and its impact on the organizational process. The overall study performed by Knapp et al. (2009) suggests that the security process and governance program must be seen as an ongoing interrelated policy management activity. The policy must work as a planning and control context, to establish acceptable behavior, decisions and standards (Knapp et al., 2009). The repeatable process works by policy development, approval, awareness and training together with monitoring and policy enforcement etc. The framework also takes into account external views, such as economic and technological advances, as well as internal, such as policy monitoring and enforcement. Knapp et al. (2009, p. 501) further notes that information security can be seen as a cultural problem as well, which ought to be taken into account for, if for example “an organization’s culture breeds hostility toward a security policy that employees perceive to be unreasonable, the security staff may find it challenging to achieve compliance of the particular policy.”

Roy Sarkar (2010) also recognizes the cultural aspect in his article discussing the threat of insiders. Roy Sarkar (2010) argues that technical solutions do not fully suffice, “since insider threats are fundamentally a people issue” (Roy Sarkar, 2010, p. 112). As such, Roy Sarkar (2010) argues for a three-pronged approach; technological, behavioral and organizational. As a result, Roy Sarkar (2010) argues for the following basic baseline; Strict HR policies, Mandatory awareness training, Technical controls, Hardware controls, Network access controls and Auditing and monitoring as detecting controls. Although emphasizing the importance of monitoring employees, Roy Sarkar (2010) also notes that it could be counter-productive for some honest employees. Even though such a “monitoring strategy” may lower the moral of the employees Roy Sarkar (2010) argues that “it is vital that employees are made aware of the level of monitoring and the policies of the organisation. It creates an open working environment of trust and user productivity with adequate levels of security for employees to safely share information while accepting different cultures and business practices” (Roy Sarkar, 2010, p. 130). Zeadally et al. (2012, p. 191) agrees with this to some extent but stress the need for better automated tools in identifying the threats of insiders, and argue that there is yet to supply an “innovative, cost-effective, and automated tools that can efficiently (with the least number of false positives) distinguish normal activities from insider threat activities in real-time so that appropriate actions can be taken before any attacks occur.” This includes however also the undertaking of a more holistic approach, which also would allow for psychological and organizational aspects of the given problem (Zeadally et al., 2012).

Zhao and Johnson (2010) describe the issue of information access within organizations, and the potential threat of its misuse. While employees must have access to some data, Zhao and Johnson (2010) notes that there is also a need for managers to protect the same information against misuse, but at the same time allow for the employees access. As such Zhao and Johnson (2010) have developed a type of escalation scheme to flexibly manage the allowance to information. This in turn is based on
policy and user access level. The data access must as such also be monitored to detect any misuses, and the misuse penalized. As such Zhao and Johnson (2010) argue that this framework is different beyond any other simpler control as it can allow employees’ which recognizes the need for particular information to fetch it, “such an approach has been witnessed in several settings, including investment banking, where it is sometimes referred to as “override,” and health care, where it is called “break the glass”” (Zhao and Johnson, 2010, p. 82). In Zhao et al. (2010) this issue is further explored, and undertakes the experience of information security within medical platforms. Zhao et al. (2010) recognizes the complexity of the medical system and its environment, and argues that “because of the complexity of the application environment, a unified user security management plan should be adopted with a strict user-licensing mechanism. The public key infrastructure (PKI)-based technology should be applied to the business personnel to improve the system’s access control” (Zhao et al., 2010, p. 746). Zhao et al. (2010) further recognizes that security policy is the aggregation of all measures for protecting the medical information assets, and that countermeasure must be taken in response to different security threats. Security should be seen as a proactive defense technology, and should consist of rigorous systems, strict management and advance technology (Zhao et al., 2010).

Bhardwaj and Singh (2011) stress the need for integrating an automated examination system into the academic context, but highlight its security concerns. This includes classification of data, roles and responsibilities of stakeholders as well as a firewall based security module for automatic filtering. The idea is that top-most managers must specify the user roles, and expected outcome of the system. This is important as “their roles and responsibilities for system handling must be clearly defined so they can be held responsible in cases of security breach” (Bhardwaj and Singh, 2011, p. 159), but also due to the fact that the privileges of using certain data should depend on the stakeholders working-task, that is to say, “the principle of “least-privilege” needs to be adopted; that is, access to the data is given only to those users authorized to access the data, meaning there is no need for all university personnel to have full access to all types of data […] The whole purpose of data security is to allow those users to use information without loss of confidentiality and integrity” (Bhardwaj and Singh, 2011, p. 159).

Etsebeth (2011) discusses the many threats related to information security and its importance to organizations in order to protect their business assets; trade secrets, patents and “know-how”. The article describe three broad categories of cyber-information assets threats; “(i) interference with information and/or data - where an adversary compromises the confidentiality, integrity and availability (CIA) of corporate information assets; (ii) interception of information and/or data - where an adversary not only obtains unauthorised access to corporate information, but he/she is also able to delete, alter or modify it; and (iii) impersonation – where an adversary masquerades or impersonates an authorised user” (Etsebeth, 2011, p. 63). Etsebeth (2011, p. 62) further notes that “companies need to strike a balance between the protection of sensitive and confidential corporate information and the availability of such information to stakeholders”, and notes that efficient information security infrastructure has, as of late, turned mandatory.

Mylonakis and Malioukis (2010) argue that the breaches of security can damage the organizations’ reputation and brand. Thus it is of importance that business leaders prioritize security high on their agenda, and to ensure that everything that can be done to prevent data breaches are done. Mylonakis and Malioukis (2010) lists some of the most common types of threats, such as; viruses and worms, fishing, key-loggers, hacking, botnet etc. etc. To mitigate these, Mylonakis and Malioukis (2010) also notes best-practice solutions, such as protecting the information from malicious code by installing and use real-time protection of anti-virus etc. To provide a firewall between the Internet and
the users, keep an updated and active software firewall. As well as patching, backup and physical access to networks and computers etc. etc. Mylonakis and Malioukis (2010, p. 7) concludes that “organizations that assume something will occur that will disrupt their ability to do business, and then plan for that eventuality before it happens will be well ahead of the curve in terms of their ability to survive the event and continue to service customers.” From an economical perspective van der Molen (2012) argues that lesser impacts of malware mean lower economic damages and thus more profit. Some of the highest causes of the infection of malware, van der Molen (2012) argue, are due to employees. The flexibility of the workstation can diminish the defense of the employees’ computers, and as such also spread into the organization. For example, “if employees work with business documents on infected PCs at home, this information could be disclosed.” (van der Molen, 2012, p. 272). However, van der Molen (2012) argues that organizations may model the spread of malware within a network by utilizing the Susceptible, Infected, Susceptible (SIS) model. This can in turn render a higher overview of the situation. Although van der Molen (2012) notes that not all malware can be expected to spread over the network, and as such propose organizations to “reduce the risk of malware infections by periodically resetting software on each computer” (van der Molen, 2012, p. 278).

5.2 STRATEGIC

This orientation also relies on control in that the actor needs to affect agents/actors to achieve their goals. That is to say, the agents are seen as an intelligent counteraction, which must be measured and taken into account for.

In trying to engage employees towards better information security Da Veiga and Eloff (2010) addresses the issue of culture and behavior. Their proposed framework undertakes such topics as attitudes, assumptions, beliefs, value and knowledge which different stakeholders utilize whenever using organization’s system. These procedures can either be classified as acceptable or unacceptable. Da Veiga and Eloff (2010) demonstrates the framework with a fictive company, and notes how to achieve better compliance by the posed policy by, for example, utilize necessary controls and have the employees sign the policy agreement to illustrate commitment. The ISCF framework can also be used as “the input to develop an assessment instrument for assessing the information security culture in an organisation” (Da Veiga and Eloff, 2010, p. 205). The result by such an examination may aid the validation of the culture component categories, and as such execute corrective action plans to mitigate and minimize these threats as posed by human behavior, and thus better protect the information assets.

Colwill (2009), Cox (2012), Dutta and Roy (2008), Knorst et al. (2011), Lambrinoudakis (2013), Qingxiong et al. (2009), Vance et al. (2012) and Williams (2008, 2013) also recognizes the alignment of organizational goal and user perspective/behavior. Knorst et al. (2011) propose a procedure which identifies the organization’s image, prioritize and identifies security practices. The process aims to secure the business requirements of confidentiality, integrity and availability by applying a framework which integrates the strategic, tactical an operation vision as well. This is done by utilizing BSC (for strategy), COBIT (for tactical) and IEC27002 (for operational). These are, in parallel, applied to another image-instrument, that of identifying the performance either related to mechanistic, psychic prisons, political systems, instruments of domination, organisms, cybernetics, or flux and transformation. Finally, a model of strategic prioritizing, based on compensatory fuzzy logic (Knorst et al., 2011). Qingxiong et al. (2009) developed a framework for a better holistic integration of the information security management plan. This framework was developed to integrate the assets of the organizational environment, to establish information security objectives, analyze its requirements,
develop security controls and train/evaluate these controls. Qingxiong et al. (2009) takes great height of the practical requirements of security, and addresses its issue as a sort of trade-off between security and ease of use. However, it should be noted that a majority of security problems are due to the fact that some implementations are designed for easy access (Qingxiong et al., 2009). In evaluating this process of information security management, a steering team is there to address and represent the major business unit, as well as the IT security team and legal department. This working group is there to better align the information systems security with that of the organizational directions and goal.

Williams (2013) discusses an e-health environment in Australia, and its natural demand of tight information security. As this new service arise, so does also new technology, which in turn craves new security attention. Williams (2013) notes that this also brings the attention towards individual responsibility of security, together with compliance, “whether or not information security is core to your role, individuals must become more aware of their responsibilities [...] larger organizations, such as hospitals, may have an IT department that has overall responsibility for this, it is important that managers and staff understand their responsibilities within their specific work area” (Williams, 2013, p. 36). The key point made by Williams (2013) is that security practices and compliance is an individual responsibility. Dutta and Roy (2008) also discuss technology and human factors in information security, and proposed model of system dynamics focusing on the interplay between technical and behavioral factors. However, Dutta and Roy (2008, p. 370) “takes a business value perspective and user reactions are triggered by erosion in business value caused by infosec incidents”. The focus of the model is to “captures delays associated with perception of security risk, the mechanics of user compliance and the mechanics of risk mitigation achieved by investments in security technology and user training” (Dutta and Roy, 2008, p. 349). Dutta and Roy (2008) further concludes from experiment that the compliance tend to fade in the absence of threats, and as such, sustained security and awareness as well as fire-drill alike training should be of high relevance. Dutta and Roy (2008) also note that an investment in new security technology can harm the effect of user awareness and compliance.

Lambrinoudakis (2013) propose an extension of existing security standard frameworks regarding information privacy compliance. Lambrinoudakis (2013) argue that there is often a concern regarding information privacy among the many security controls and solution. However, this is not correct, Lambrinoudakis (2013, p. 177) argue, “since the main security and privacy attributes are different; information security refers to information stored, processed and transmitted for completing the information system’s functions and purpose, while information privacy is the protection of the information’s subject identity”. Where the security “is commonly regarded from the viewpoint of the organization and information security preservation primarily protects the business goals and assets” (Lambrinoudakis, 2013, p. 185). As such, Lambrinoudakis (2013) argue that the traditional CIA triangle does not allow for the complete functions of privacy. For example, any security incident may pose organizational loss, but so can also privacy incidents argue Lambrinoudakis (2013). Thus, there is great need for “user-centric guidelines and criteria that should be developed in addition to the organizational-centric standards has been highlighted” (Lambrinoudakis, 2013, p. 186). As a result, Lambrinoudakis (2013, p. 188) argue, “it is required to elaborate and provide guidance on the development of web interfaces that assist the users to develop a privacy policy or establish a common ground between a user and the privacy features of an application. For that purpose, we relied on research done on human computer interaction in order to propose a set of user-centric usability criteria for information privacy”.

19
Cox (2012) describes different types of risky behavior among organizations’ employees, for example, the negligence of proper security compliance, even though the employee is well aware of it. As such, Cox (2012) developed a model focusing on bringing the “knowing-doing gap” into light. Thus it examines the information assurance understanding and security awareness, and can as such be used as a framework for better information security awareness training. The research in question focuses on “the intentional disregard of the information security policies and procedures for reasons other than malicious purposes: reasons such as convenience, disregard for the rules, or lack of understanding” (Cox, 2012, p. 1850). Cox (2012) notes there are many factors worthy of considering for security reasons, for example, social-engineering attacks, or the simple matter of an employee who does not fully understand the rules, or the rationale behind them. For example, “not choosing a strong password for securing personal information is an example of not understanding the reasoning behind the rules” (Cox, 2012, p. 1850). As such, human factors must be taken into account to motivate for policy compliance (Cox, 2012). Vance et al. (2012) also undertakes a discussion regarding employees’ failure to comply with information security procedures. Vance et al. (2012) note that there are a number of socio-cognitive behavioral approaches within this field, borrowing from a wide array of fields; criminology, psychology etc. However, these, as Vance et al. (2012, p. 190) argue, have not “resulted in examination of the influence of past compliance behavior on appraisals of information security threats and coping responses.” As such, Vance et al. (2012) address this gap by developing a model including habits – routines – with Protection Motivation Theory (PMT) to explain compliance. Vance et al. (2012) further tested this model and concluded that practitioners must ensure that employees’ recognize information security threats, stress the fact that the organization will most likely be targeted by some attack if the practices are not undertaken by the employed. Thus, it is of importance to make sure employees’ follow through with the compliance of security policies but also that these practices are not too complicated.

Colwill (2009) also address the issue of compliance and human factors and discuss the issues of insider threats. This in turn goes hand in hand of the information security routines, and the very nature of loyalty toward the organizational, cultural and economic social factors found within an organization. The insider threat, Colwill (2009) notes, differ from other threats as it faces legitimate access already established to the systems. The key question comes down to who to trust, and how to maintain that trust? Thus, organizations must impose an effective risk management, and it is important for organizations to “be able to provide evidence to their customers and stakeholders that appropriate risk processes (including a focus on insider threats) have been applied and that security compliance is being maintained” (Colwill, 2009, p. 195). Although, Colwill (2009) notes that technology can provide efficient monitoring, for example to detect malicious activity, but the real solution is that of the environment and human factors. As such, security controls must be agile and workable in perspective of the environment and user participation. Such controls and technology “should not be considered in isolation: if people do not co-operate with, and comprehend the reason for security controls, they may find cause and means to subvert or circumvent the technical restraints imposed on them, particularly if they impact on reward” (Colwill, 2009, p. 195). However, Williams (2008) notes that the insiders threats can be either malicious or unintentional, and that attackers “no longer require advanced technical knowledge and many attacks are unintentional, exploiting business process rather than technology” (Williams, 2008, p. 214). For this reason, business processes must be viewed from a holistic governance perspective. Raw technical implementations, Williams (2008) argue, cannot suffice in this matter, and organizations must instead undertake a view concerning both organizational,
technological and the people within the organization. As such, culture becomes an important component. However, Williams (2008) notes that too much trust may contribute to the complexity of insiders and notes that “whilst organisations must meet legal requirements, the ethical component of security in the medical environment is underpinned by individual behaviours contributing to information protection. In trustful environments where everyone does not take on the responsibility for information security, there is more opportunity for insider threats to go undetected and potential damage to be done” (Williams, 2008, p. 208). As such Williams (2008) proposed model invokes a balanced level of trust within the target environment, which allows for acceptable information security practices and the management of unacceptable ones.

Jones (2008, p. 220) concludes that the threat of a “malicious insider can only be successfully achieved if a holistic approach is taken to the issue of securing the assets and infrastructure.” This, Jones (2008) argues, becomes more and more difficult as the organizational trend of being even more agile and mobile increase. This not only craves that data and information is available and accessible when the information is needed but also monitoring what information is needed, when it is needed and by whom – trying to sort out abnormal behavior (Jones, 2008). The key, Jones (2008, p. 224) notes, is that if “the environments in which staff are working is friendly and inviting and the organisation has developed a reputation as a ‘good employer’, then staff are less likely to have a reason to cause it harm” and as such “detection and apprehension of malicious insiders is not simply a technical issue as the cause is fundamentally a people issue”. It thus becomes vital for organizations to re-evaluate the way in which they protect their information (Jones, 2008).

For example, Likar and Trček (2012) also recognize the complex nature in handling sensitive information, and as such introduce an info-innovative solution, a sort of complement to handle the complexity. This approach takes an ever changing approach in aiding information and innovation of security related threats. The approach applies the field of innovation management, and seeks to sort out creative individuals which, briefed with a short introduction of information security, can help identify and or recognize additional threats. This may also help in legal matters, but it is, as argued by Likar and Trček (2012, p. 26), “paramount that they are creative and represent different fields of expertise as well as representatives from different organisational units”, so that different level of experience and knowledge input may be taken into account. All these views are then subjected to a critical analysis by experts. The surviving threats developed into finding fitting solutions. This whole approach is recommended to be applied every six to twelve months according to Likar and Trček (2012). Building on the essences of Likar and Trček (2012), Trček and Likar (2014) argue that the startup of any new vulnerability is due to the following life cycle, which consists of birth, discovery, disclosure, publicity, scripting, correction and death. Where the main problem is the proactive defense of birth, which craves the attention of proactive risk management, which in turn only can only be “covered only by interdisciplinary work in the fields of security and innovation” (Trček and Likar, 2014, p. 65). Traditionally, when the statistics of newly born vulnerabilities were still low, Trček and Likar (2014) argue that well-established statistically based methods were sufficient to deal with these, but “the probability of newly born vulnerabilities increases, and such vulnerabilities cannot be addressed with the above techniques. There is one kind of a useful ‘crystal ball’ for this purpose that we are currently seeing; this is application of innovation techniques, among which brainstorming has the most successful track record” (Trček and Likar, 2014, p. 66).

Herath et al. (2010) agrees with this to some extent, and also recognize the need for multiple stakeholders’ perspective as well as business goals. Herath et al. (2010) propose a conceptual
framework for information security performance management using balanced scorecards. The framework builds upon four approaches; business value, stakeholder orientation, internal processes perspective and future readiness. Herath et al. (2010, p. 72) argue the importance for IT-security managers “to evaluate whether security investments are meeting organizational goals and objectives. They must take into account the business mission of the information systems. There is a need to set goals and develop performance measures for evaluating security processes and outcomes”. As such, great care must be taken by the security managers in consider as many different type of users and stakeholders’ as possible while providing IT-security services. Johnson and Johansson (2008) also address the issue of multiple stakeholder perspective. Johnson and Johansson (2008) describe a method for assessment of the level on information security within organization and business processes. This method was derived to give a percentage on how good information security and also provide an estimate of the credibility of the information security score. Johnson and Johansson (2008) recognize the problem of security assessments cost in collecting required data, and as such poses this method as minimize the efforts spent. For example, the method “draws on the knowledge of many employees to define the current state of security, identify risks to critical assets and set a security strategy” (Johnson and Johansson, 2008, p. 121).

The issue of cost is also addressed by Stewart (2012) who discusses the optimality spending on information security. Stewart (2012) notes that managers, faced with a capital budget decision, will try to maximize stakeholders value. Thus must consider and evaluate different spending’s, as it “affects the company, its business partners, and ultimately its customers” (Stewart, 2012, p. 312). In making a decision, Stewart (2012) argue there is a number of factors which influences the decision process, some by the very nature of information security, and others by psychological and economic aspects. For example, humans tend to react more emotionally to risks, which may affect their decisions. This in turn, Stewart (2012) notes, may cause managers to delimit environmental flexibility or freedom, and come in the way of the creative work. “The opportunity cost forgone is the productivity gain that the employees would [otherwise] receive” (Stewart, 2012, p. 314). For this reason, Stewart (2012) has developed a type of model which can be used to enable organizations to select a rational approach to information security. The model consists of two spending strategies, which both aim at addressing weaknesses in common justifications of spending on information security. The strategies imply a “minimal spend strategy”, to create a cognitive dissonance by the managers. This is important as Stewart (2012) recognize that “spending decisions either create or destroy shareholder value. As such, the security spending decision must be carefully considered” (Stewart, 2012, p. 325). As such, Stewart (2012) argue, that these strategies may help justify information security, and “if spending on security cannot be justified then it cannot be considered rational” (Stewart, 2012, p. 325).

Goel and Chen (2008) propose an approach to information security risk analysis. This approach builds upon the framework developed by Goel and Chen (2005), which can “illustrates how the organization can aggregate the risks of security breaches in an organization to help managers ascertain the importance of protecting such information” (Goel and Chen, 2008, p. 111). Goel and Chen (2008) argue that this risk-matrix approach can empower business decisions and guide these to be more rational. A tool for guidance rather than a tool for presenting solutions, to “help lead businesses to successful products and sustained profits” (Goel and Chen, 2008, p. 112). This is further demonstrated by Goel and Chen (2008) conducting a case study, inviting different stakeholders to take part. This resulted in different perspectives of security risks, vulnerabilities and its individual level of importance. This in turn introduced a number of different perspectives from different type of stakeholders. “The
environment is rapidly changing; new threats and vulnerabilities are constantly emerging and legislation is evolving, which makes managing security difficult. Most organizations operate in a reactive mode where they address security problems as they uncover them. Security, however, should be proactively integrated into business process conception or redesign, and not as a patch of controls that merely respond to security incidents” (Goel and Chen, 2008, p. 111).

Charitoudi (2013) propose a model based upon socio-technical systems, which places people and technical means in the context of the environment. The model “focuses on impact; on the implications events can have on the supply chain and business processes and not on risk estimation and the prediction of events” (Charitoudi, 2013, p. 41). Charitoudi (2013) model correlates the users by their given task role or responsibility, and what set of requirements and behavior can be expected from that affair. “The concept behind these functions is to allow us to express a set of necessary and sufficient conditions that must be achieved in order for a responsibility to be fulfilled” (Charitoudi, 2013, p. 35). On the other hand Farn et al. (2004, p. 512) concluded that the security information system “is like a chain. Its strength is affected by the weakest knot”. When dealing with these mechanisms of protecting assets against threats and vulnerabilities, risk management ought to be considered, and that “the human nature is not always good, and it is common for its guardians to intrude the security of the asset. Information security management not only is related to the ‘public security’, but also takes the organization levels, evil-disposed outsiders, and burglars inside the company into consideration” (Farn et al., 2004, p. 511).

5.3 COMMUNICATIVE

For the communicative orientation, sense-making as a cognitive process of commitment, capacity and expectation is central. Focusing on the common interpretation of the action situation.

Hilton (2009) propose an approach towards information security and stress that by “involving staff in thinking about how the organisation delivers it’s purpose, or thinking about their part in a multi-agency initiative, they will understand what their part is, can identify risks and, using their knowledge of the detailed work involved, can propose achievable controls” (Hilton, 2009, p. 127). The controls, Hilton (2009) argue, should be considered by managers, determining what they ought to achieve, but not how. The question of how to achieve these practices, Hilton (2009) argue, must be done by those who carry out the activity. “This involvement of staff should ensure the desired control is achievable and, more importantly, is sustained. Lasting change will be achieved, as individuals will change their perspectives and beliefs through open dialogue and conversation” (Hilton, 2009, p. 127). Hilton (2009, p. 127) quote “tell me and I’ll forget, show me and I’ll remember, involve me and I’ll understand.”

Albrechtsen and Hovden (2010), El-Gayar and Fritz (2010), Ozkan and Karabacak (2010) and Papadaki et al. (2008) all seems to agree with this quote on user participation in reaching a common understanding. El-Gayar and Fritz (2010) for example present a decision support system for information security planning. Their system addresses multiple perspectives within an organization, and have developed a web-based group decision making environment utilizing MCDM. The process seeks to address multiple stakeholders and judgments. As such, El-Gayar and Fritz (2010) allows users to set up security issues and assign its stakeholders. The stakeholders can then comment or add to these issues. The goal is to reach a common interpretation of the issue, and as such the users are anonymous. The issue can even be voted down or rejected altogether by the stakeholders. “As a technique for asset prioritization, risk assessment and control selection, this approach offers advantage over traditional techniques such as expected value or annualized loss expectancy, if the decision entails
prioritization on the basis of qualitative criteria, such as capabilities or properties/attributes of the alternatives in the selection decision which are value-based or otherwise subjective in nature. The ability to represent these criteria offers advantage over checklist-based and matrix-based approaches and the system can deal with conflicting priorities [...] and could be highly effective in forming a convenient summary of stakeholder opinions on an issue or problem being faced by the organization” (El-Gayar and Fritz, 2010, p. 53).

Koskosas et al. (2011, p. 53) found that “there is a chain reaction among these issues with a subsequent effect on the level of security goal setting”, and that trust within an organization resulted in higher level of cooperation and positive attitudes, which as a result, rendered better understanding of the group culture within. This in turn, Koskosas et al. (2011) found to have a relation towards improved communication of risks among the members of an IT-group – although this have less significance to a larger IT structures as its organization has a more rigid cultural environment which does not allow for individual intellect (Koskosas et al., 2011). Ozkan and Karabacak (2010) in their article present a case study on a collaborative risk method for information security management. The case study and method present focuses on common problems faced when implementing relating security ISO standards. The method undertakes a Plan-Do-Check-Act process and where applied in different public organizations. One key point which Ozkan and Karabacak (2010, p. 569) stress is that “there are two types of risk analysis methods; quantitative risk analysis methods contain mathematical instruments to evaluate risk, qualitative risk analysis methods do not contain any mathematical instruments”. Ozkan and Karabacak (2010) concludes that public organizations are better off with simpler methods than those presented by the qualitative security literature, and notes that the “foremost requirement to ensure information security management in public organizations is staff involvement. It cannot be assured by a third party company or a consulting firm; rather it is a continual process” (Ozkan and Karabacak, 2010, p. 569). As such, the risk analysis process, that is to say “the security requirements of organization, the cost of countermeasures, the budget of organization and the usability and the operability of the countermeasure – these were determined collaboratively with the involvement of employees of the organization” (Ozkan and Karabacak, 2010, p. 571). This method, in particular, Ozkan and Karabacak (2010, p. 572) argue “would be useful for public organizations in countries where effective information security management legislation has not yet been enacted like Turkey”.

Albrechtsen and Hovden (2010) argue that common, mainstream, information security measures “are typically top-down, and seek to bring about changes at the Intervention study individual level by means of an expert-based approach directed at a large population, e.g. training through formal presentations, e-mail messages, leaflets and posters” (Albrechtsen and Hovden, 2010, p. 432). Albrechtsen and Hovden (2010) demonstrate however that “the effects of employee participation on organisational development and change are known within several research traditions, but this knowledge is not reflected in mainstream standards and guidelines for information security [...] Participation is likely to create advantageous information security conditions, such as improved ownership and motivation among workers (Greenberg, 1975); improved quality of technological solutions (Adler and Winograd, 1992; Ehn, 1992); and reduced levels of risk (Elden, 1983; Shrader-Frechette, 1991). Moreover, it will satisfy the democratic rights of workers to influence their own working conditions (Elden, 1983; Greenberg, 1975)” (Albrechtsen and Hovden, 2010, p. 434). The collective reflections avoid as such any one-way communication lecturing, and aims thus at mutual understanding of routines, which is important for the very interaction within the organization (Albrechtsen and Hovden, 2010).
Papadaki et al. (2008) propose a systematic meta-process for developing or improving information security risk management (ISRM) methods. This draws upon the meta-methodology of TSI (Total Systems Intervention), Performing, Criticizing and Reviewing. Where Performing is the actual performance/practice of risk management process, Criticizing relates to evaluating the experiences from applying the methods (and participants comment on the success of the risk management and problems encountered), and Reviewing, where the identified problems are sought to find a fitting solution, and the participants decide on a method that is more appropriate. “In practice, only the first mode (practicing) has been the subject of research. The other two modes (criticizing and reviewing), although existing, are not explicitly acknowledged or addressed in a systematic way” (Papadaki et al., 2008, p. 338). Furthermore Papadaki et al. (2008) notes that “ISRM is not just a technical issue. On the contrary, it is an issue with multiple key dimensions (e.g. business, economic, culture, legal, politics, standards, technology) that need to be taken into consideration. Clearly the existence of many viewpoints ensures a holistic approach towards information security. The prerequisite for such an approach is to have people with different backgrounds participating in the network of practice for ISRM” (Papadaki et al., 2008, p. 339).

Hedström et al. (2011) discusses information security practice and policy management by a value-based compliance model. This, Hedström et al. (2011) argue, is a different approach than that of the ordinary control-based, compliance model which assumes most of the literature within this field. As such, Hedström et al. (2011) propose a theoretical model which assumes that many different rationalities and values can exist within an organization, creating potential value conflicts and thus affecting the compliance. The common practice today is to develop a set of rules, regulating expected use and behavior, and then let them understated how to follow these rules. Instead, Hedström et al. (2011, p. 381) argue that “management of information security and compliance should view users of information security measures as competent and rational actors, and see non-compliance as an action based on an underlying rationality which could form the basis for improving the information security management at the organization.” Thus Hedström et al. (2011) argues for the importance of breaking free from the control-based approach which views human and human behavior as controllable, and instead see compliance by what is said and done, to view humans as resources and not as problems.

5.4 DISCURSIVE

Initiated by doubt or ambiguity this orientation emphasizes communication and validity of claims as the target of communicative interest to illuminate underlying rationality. This, however, craves an ideal speech situation free of oppression or domination.

No articles were found to correspond to this particular orientation.
6 DISCUSSION

Based upon section 5, the following writing is dedicated to discuss some differences and parables found, and to suggest further extensions.

Overview; A number of 52 articles over a period of ten years (2004 till 2014) and spread across 36 various outlets were reviewed. The selection was motivated by selecting a wide perspective; ten years to depict current literature and themes, and literature from alternative journals and outlets than those purely focusing on IS was reasoned to contribute to this motive. Literature from different disciplines and journals, as well as technical reports to illuminate the practical end, were thus selected.

It was found that literature, recognized by the different orientations, tend to differ in scope and focus; from controlling and monitoring (instrumental), to co-operation and perspective (strategic), to understanding and expectation (communicative). Although limited, the reviewed literature suggests a type of “funnel” taking shape; steadily graduating from a static controllable to a complex socio-technical environment. Literature from these different orientations also suggests that emancipation does matter as IS risk practices could pose as an obstacle for the employees. Furthermore, no articles were found to undertake a discursive orientation and is, as such, as well as the idea that different orientations characteristics might contribute to one another, suggested as an area of further research.

Instrumental (26 articles); In a critical perspective, as discussed, some form of cognitive exchange must take place, shaping consensus. Something which the risk practices found in the instrumental orientation seems to lack. Instead, the instrumental orientation, as outlined in section 2.2, focus on achieving given ends. That is; applying technical rules from empirical knowledge or theoretical models, selecting and implementing means which promises result for a certain situation. This also seems to impregnate the literature associated with the instrumental orientation, the “measure and mark” solutions, which looks upon the environment as threats, cost and defenses/remedies. This is reflected throughout the various topics within the reviewed articles, and seems to be the most common, thus noteworthy, distinction for this orientation; monitoring compliance, measuring current threat-levels to assure cost effective decisions, while applauding statistics and likelihood in risk controls.

However, the employee is not absent from the instrumental orientation. For example, many of the articles did mention training and culture as an important factor. Although many of the articles stress technical means, like monitoring, to ensure employee compliance. This in turn raises some interesting questions regarding managerial proceedings to ensure compliance and its relation towards the individual and cultural aspects. Although some articles mention these aspects, they are rarely deeply discussed and mostly targeted by technical means. Generally floating on the managers and security staffs ideology of their own best-know-how, relying on physical or behavioral models to enforce security and compliance. Though some articles recognized that risk practices may come in conflict with the employees’ cultural or moral perspective and even contribute to counter-productivity. However, to tackle this, these articles seems to build on stressing the underlying rationality and importance of these practices to make the employees aware and able to adapt to these new routines. This, in turn, seems to agree with the discussion, from section 2.2, that the practices are adopted and spread evenly.

Strategic (19 articles); In the strategic orientation we evolve further up the funnel and start to see that the user has a potential role which must be taken into account. For example, some literature has pointed out that simply listing what and what not to do is not sufficient, instead one must look at the stakeholders’ behavior, roles and their need for different security approaches. As such, a number of
Frameworks and models are presented, inviting the idea that individuals are intelligent actors which cannot be treated as the same, but must be cooperated with to find the best fitting strategy. Thus concerning both alignment of organizational goals and user perspectives.

Although topics such as cost-effectiveness, security policy and risk controls are brought up, though not by the same quantity as within the instrumental orientation, the focus has been shifted towards more “agent-close” factors. For example, we find that the strategic orientation focus more on topics regarding awareness, culture and compliance. But also some new dimensions not found within the instrumental orientation, like behavior and perspective as well as innovation and creativity by the stakeholder. This in turn renders some interesting insights towards the practices found. For example, some articles stress that security practices, if not undertaking employees’ perspective, may pose as a constraint and thus come in the way of the employees’ creative work. Although this idea is found within some of the instrumental literature as well, the idea here is not to stress underlying rationality and importance, but seems instead to co-operate and take the actors’ perspective into account.

However, it is important to note that these practices, although undertaking great stakeholder perspective, does not address emancipation. This seems mainly to do with the still overhanging idea of control. Not in the sense of controlling the threats, which are seen as more complex than reflected by the literature in the instrumental orientation, but controlling the achievements and the very practice of how. Managers may welcome ideas, but in the end these are still employed or dismissed by the manager or security staff. The enforcement of practice thus still lingers in this orientation, circumventing agent consensus, as managers and security staff still seem to doctrines the IS practices.

Communicative (7 articles); In the communicative approach we find that there is a need to find and apply common sense and expectation. The literature points for a greater need to align the business initiatives with the process which in itself ought to be transparent – suggesting the importance of stakeholders agreeing upon shared capacity and expectation. Interestingly, through far from definitive, is that these articles seem to have been publicized in quick succession and tends to be rather “new” (see figure 5). This might suggest for a later theme to interact with the individuals’ perception of an environment or system. Of course, the instrumental orientation for example does discuss some individual focus like addressing the need of user training, which in itself must be measurable in its effect. The non-emancipatory orientations fail however to suggest that the lack of compliance and/or understanding might be due to a missing cognitive process, like a cultural aspect to share meaning of, for example, proposed policy routines. The articles that do undertake a communicative approach however, seems to stress the need for a multi-way communication, that is to say, not only give orders and rules, but to allow for reasoning, looking toward consensus by what is said and done.

As such, the area of awareness, culture and compliance is also a frequent topic within the communicative orientation, just as with the instrumental and strategic orientation. So is also the stakeholders’ perspective, as with the strategic orientation. However, the communicative orientation towards these areas differ, and focus has been shifted from controlling and monitoring (instrumental), to co-operation and perspective (strategic), to understanding and expectation (communicative). For example, the awareness, culture and compliance within the communicative orientation seems to recognize that there is a relation between practice and meaning. This means, from a critical perspective, that risk practices could arguably benefit to be viewed as offering structure and opportunity, inviting employees with different experience and knowledge to participate and to share meaning.

In addition, the communicative literature does introduce some new dimensions not found in either the instrumental nor strategic orientations. These topics concern employee communication (as in
cognitive process), user participation and common understanding/values. This, in turn, seems to shift the focus further from having the manager or security staff viewing the employees as a problem or object, towards viewing them as intelligent individuals, resources. For example, the managers or security staff, which otherwise seems to discourage any thinking which goes beyond the doctrines that governs the ideology, now looks towards shared meaning and understanding. As a result, the many practices found within this orientation focus on bringing the employees to participate. Of course, participation has been addressed to some extent by the strategic orientation as well. However, the difference seem to be the underlying meaning. The strategic orientation mentions participation as a mean to reach compliance and not have employees subverting controls. However, these controls are still dictated by the manager while its underlying reason remains undiscussed. As such, the cognitive process of reaching consensus is lost, and the employees’ perspective only taken into account so that practices does not become an obstacle – but not to reach a shared expectation or meaning.

**Discursive (0 articles);** Even though a number of articles have suggested complex and interesting socio-technical approaches with great deference towards the user, they have not reached the level of complexity and discursive underpinning which is this very orientation. It would however be interesting to find a case which fully undertakes a discursive orientation in its IS risk practice. Such an orientation is (as discussed in section 2.2) on the other hand difficult to achieve as it acquires an ideal speech situation with no power imbalance and free of oppression or dominance. The lack of such a case might, and is to some extent supported by the reviewed articles, be due to an existing hierarchy. For example, when a manager is about to choose a policy its suggested procedures may be discussed with the stakeholders to reach a common understanding, but the policies and its underlying rationality is still up to the managers best-know-how, and as such may lack in any full reasoning of evidence or rational motive of what may be missing, and could as such lead to ambiguity and a false sense of security.

It should however be noted that some of the articles found within the communicative orientation presented some features close to discursive. Both El-Gayar and Fritz (2010) and Papadaki et al. (2008) present some interesting features. For example, both utilize a web-based platform, allowing employees to submit, discuss and criticize IS practices. The idea of a web-based platform is interesting as it has the potential to facilitate both an arena of debate, to help shape the IS risk practice, and minimize any potential power imbalance by making each contribution anonymous. However, in the case of El-Gayar and Fritz, (2010), although anonymous, the power imbalance is not total as each “issue” is owned by a user, and it is up to that user to select what stakeholders have a say in the matter. In Papadaki et al. (2008), on the other hand, everyone may add, discuss and criticize, not anonymously however which may contribute to power imbalance. Furthermore, and this aligns to some extent with the idea as discussed above of an existing hierarchy, the risk practices in both cases are per-defined, ready to be commented on, and not to upbring the underlying evidence of meaning and interest.

However, interesting ideas of the potential quality of a discursive orientation arises, which of course only can be subject to speculation as of this writing, that if we are to undertake the same hypothesis as presented by Wenger (1998) (see section 2.1), which has also been suggested by the communicative orientation, there is a universal relationship between practice and meaning. If this is true, then one might expect interesting IS risk practices to be found in a discursive orientation.

**General comments & Further extensions;** While analyzing the material, as presented in section 5, it seems that the instrumental and strategic orientations reminds of its strict ideology, whereas the communicative, and presumably also discursive, orientation allows in a sense for more philosophy – seeking understanding and open for criticism. This fits well with the theory and
framework as discussed in section 2.2, where the emancipatory orientations encourage user participation, thinking, and ultimately (discursive) criticizing. While the non-emancipatory orientations risk practice agenda is set by the managers or security staff. This, from a critical perspective, discourage the cognitive advantage of the employee and pose as such as an obstacle for their full potential. Interestingly, this is something which literature from all orientations have suggested – although in various forms. This in turn seems to indicate that there is no common understanding, structure, of IS risk practices ideological perspective and its consequence on emancipation.

So, from what we’ve seen and discussed the different orientations separate their risk practices slightly, and their focus shifts to become more socio-technical, and their emphasis on predictable control dissolves. This makes some interesting points, not to mention from viewing these findings in relation to figure 5, illuminating the time of publications. This suggests that, as of late, research related to the more emancipatory orientation starts to emerge. However, what we have not seen, as of yet, is the discursive orientation. Though, if the progress from instrumental and strategic towards communicative is slow, and interpret as conclusive, it might suggest that the discursive, as a problematic form of communicative, will mature in mean time. As discussed above, this orientation may illuminate some interesting elements of risk practice in general, and is as such strongly suggested as a field of further exploration.

Furthermore, as an alternative to view each orientation as a separate approach it could be argued that none of these orientations are best viewed in isolation. The discussions regarding the different orientations have indeed brought up various features. Agreeing that IS is, as discussed in section 2.1, a process of an idea, belief or method that is collectively experienced as meaningful regarding a situation or asset(s) integrity, availability, confidentiality and/or non-repudiation potential exposure to danger or threats. This could also dictate different means of conceptualization. For example, even though a discursive orientation may contribute to develop a better shared ideal situation, where meaning and understanding is in focus – the question as of how to evaluate such an orientation still remains. How, for example, could such an approach be deemed meaningful from an administrative perspective? Or as with the instrumental approach, which may be easier to calculate for in its statistical and technical means in trying to control the many threats – but how to ensure loyalty towards the ideology? How, for example, could such an ideology be justified and meaningful from the employees’ perspective?

Now, these questions raises some interesting thoughts concerning IS risk practices in the first place. For example, if we address these concerns from the perspective as reflected in section 2, that IS threats keeps evolving and could thus arguably be said to be in a constant domain of change. Change as in reflecting the dynamic nature of an environment. Then, IS risk practices must not be viewed as static, but something which evolves – and rightfully so, as we implement, experience and learn over time. If this holds true, then the different orientations characteristics may naturally contribute to one another. How so? Arguably, and further illuminated by each orientations separate discussion, the different orientations fulfill various areas of concern regarding IS risk practices. Inviting the idea that risk practices could be better of invoking different, or even multiple, orientations to various degrees over time. What of it? The contribution is of course only target for speculation, but could arguably contribute to how we view and exercise risk practices by undertaking concerns, characteristics, stressed by various orientations, by a given situations. As such, it would be interesting to see if, and how, these different orientations characteristics discussed could contribute to one another. Thus evolving from the question of “what are at work”, as targeted in this thesis, beyond the traditional question of “what works”, and instead towards “could it work”, and is as such also recommended for further exploration.
7 Conclusion

The focus of this thesis has been to analyze how information security risk practice literature differ in light of ideology and consequences on emancipation. In doing so, information security (IS) risk practice literature were analyzed by categorizing them using the framework conducted by Thapa and Harnesk (2014) illuminating the IS risk practice ideology as either Predictive & Controlled or Complex & Unpredicted and its consequence of the practice as Emancipatory or Non-Emancipatory. The framework is based upon Haberma’s concept of four orientations in information systems development (ISD) change; instrumental, strategic, communicative and discursive (see section 2.2). A number of 52 articles, over a period of ten years and spread across 36 various outlets, were reviewed.

Dhillon and Backhouse (2001) mentions that the IS literature has been dominated by functionalist and interpretive paradigms, to some extent this review agrees with this, but indicates that more recent literature have taken some interest in the more critical approach, discussing conflicts over goals, roles and meaning through emancipation of the user. The result suggests there is literature supporting emancipation or non-emancipation, as well as viewing the environment as predictive & controlled or complex & unpredicted. These orientations’ IS risk practices tend to differ in scope and focus; from controlling and monitoring (instrumental), to co-operation and perspective (strategic), to understanding and expectation (communicative). Furthermore, emancipation seems to have practical impact as the different orientations suggest, in various forms, that IS risk practices could pose as an obstacle for the employee. This in turn seems to indicate that there is no common understanding, structure, of IS risk practices ideological perspective and its consequence on emancipation.

What have not been found in the literature however is a structure which supports both emancipation and a complex & unpredicted (discursive) environmental view and is, as such, recommended for further research. In addition, it would also be interesting to research if, and how, these different orientations characteristics could benefit from one another, rather than being viewed in isolation, and is as such also proposed for further research.


Tesla, N., 1900. The Problem of Increasing Human Energy - With special reference to the harnessing of the sun’s energy. Century Mag. 60, 175–211.


