[cover page]

Title:
Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors

Author:
Fredrik Björck

Contact information:
Department of Computer and Systems Sciences
Stockholm University / Royal Institute of Technology
Electrum 230, SE-164 40 KISTA, Sweden
Phone (office) +46.8.6747498, (celluar) +46.70.7777917
Fax +46.8.7039023 (“Attn.: Björck”)

Email: bjorck@dsv.su.se

Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors

Fredrik Björck

Abstract

This paper presents the findings of an empirical study of certification auditors' and information security consultants' experiences and insights concerning the implementation and certification of information security management systems. Using an action research strategy and a grounded theory research method, the study describes these particular experiences and insights primarily in terms of critical success factors vital to the implementation and certification processes. Two tentative theoretical frameworks, providing synthesized views of these factors, are put forth.

Keywords : Information security management system, information security policy, IT security

1 Introduction

Implementation and certification of ISMS (information security management systems) currently interests many researchers and practitioners. Especially 7799 – the British and now also international standard for ISMS (ISO 2000, BSI 1999) - have received a lot of attention in the information security research community lately:

Siponen (2001) criticises 7799, and other information security (management) standards, from the viewpoint of philosophy of science and argues that these standards are were developed based on personal observations that were not scientifically justified. In addition, Siponen argues, the standards in question claim to be universally valid, although they are not.

Eloff and S. Von Solms (1998, 2000a, 2000b) suggests that both IT product security (measured by for example Common Criteria) as well as procedural information security (measured against for example 7799) have to be taken into account when measuring the level of information security in an organisation.

S. Von Solms (2000) declares that information security must be managed on both a macro and a micro level. The macro level (information security at an inter-organizational level) should be managed with the help of, and measured against, an internationally accepted framework, such as the 7799 standard. The micro level (information security at the intra-organizational level) should be managed through a dynamic measurement system. Furthermore, he argues that an information security certification scheme, such as those set up for 7799, should play an important role in the future.

R. Von Solms (1999) makes a business case for the standard using a metaphor of driving a car:

> "Any motor vehicle on a public road requires a valid roadworthy certificate that will indicate that all technical safety and security mechanisms and features on the vehicle are present and functioning properly. The driver needs a driving licence that will indicate that he/she has learned how to drive the vehicle in a secure way by using the technical safety features correctly and effectively. Further, a third party, i.e. traffic officers, will continuously ensure that the vehicle is functioning technically well and also that the driver obeys all road usage regulations." (R. Von Solms, 1999)

He concludes that "…BS7799 can certainly provide the basis to ensure "safe driving on the information super highway" (R. Von Solms, 1999).

Labuschagne (draft, forthcoming) asserts that 7799 could rightfully be used as one of the cornerstones of web assurance in an electronic commerce context.

While many other authors have written about 7799, this is just to demonstrate that it receives a lot of attention. Although much has been written about the standard itself, very little has been written about the *practical application* of the standard. And so far, we have not found any published empirical studies on this subject – at least not related to the 7799 standard. Consequently, even though this study is somewhat limited in its scope and depth, it might still prove interesting for practitioner and academics.

The research question of this study is:

> *What are the critical success factors needed for successful implementation and certification of information security management systems?*

This answer is sought after via an action research strategy and a grounded theory method.

2 Research strategy and method

2.1 Research Strategy

An *action research* strategy is essentially defined by four characteristics; it deals with a (i) *practical* research problem in a (ii) *participatory* style. In addition, the pursuit of (iii) *change*, though a (iv) *cyclical research and feedback process,* is considered an integral part of research (Denscombe, 1998, p. 57). Even though we clearly follow this strategy, as will be clarified and justified here, the study was not really consciously designed or labelled as action research from the onset. In effect, the strategy was determined by the context in which the research took place. A brief examination of the four defining characteristics of an action research strategy clarifies this issue:

> *Practical*. The study was carried out within the context the Swedish Standards Institutes' 7799 project, which aim was to translate the BS7799 standard (BSI 1999) into Swedish, and make it an official Swedish standard (SIS 1999). Since this aim was reached in June 1999, the focus of the project was shifted towards generating and sharing experiences and insights about ISMS implementation and certification. For this, a "pilot certification workgroup" was formed, aiming to guide a few organisations all the way from start to 7799-certification (Sweden has a similar certification scheme as the British one based on part 2 of the standard). We were invited to join this group as researchers, because there was a clear need for the experiences and insights to be documented and shared among the group members and

in the Swedish information security- and business communities at large. Evidently, there was a practical problem: How do we go about implementing and certifying these management systems with little or no previous experience about 7799?

Participation. The pilot certification work group is unique in that it brings together certification auditors, information security consultants, government agencies, organisations interested in certification and researchers (us). All of these parties have been working together with the aim to generate and share the knowledge created. The respondents – the practitioners - have shared their own experiences and insights; we have merely summarized them in this study. They needed the knowledge themselves, that is why they decided to participate. We have participated in the pilot certification work group during the course of two years.

Change. A common understanding of what is required for the successful implementation and certification of ISMS according to the 7799 standard was sought. Moreover, we were looking for a methodology of *how* this can be done. The parties wanted to change - or calibrate - their views on these issues so as to research this consensus.

Cyclical feedback. For this change, mentioned above, to take place the results were (and still are) fed back by means of presentations of what we have learned, and through written feedback reports. There are three target groups for this feedback; the practitioners in the project (and in the study), the other information security and certification practitioners in Sweden, and the information security community at large – research as well as practice. This paper is also a part in this cyclical feedback loop.

We have now demonstrated that the strategy (i) was determined by the context in which the research took place, (ii) it can be labelled action research, and that (iii) it is reasonable for the study.

However, there are no research strategies without disadvantages – this is also true for action research. The main scientific objection to this kind of research strategy is probably that if can affect the “representativeness of the findings and the extent to which generalizations can be made on the basis of the results” (Denscombe, 1998, p. 65). This is true also for this study, but the objection assumes that the action research project takes place in only one organisation (a “work-site approach”). This study is concerned with experiences and insights from many organisations and many different contexts, which may make the results more universal. Another objection against action research is that the researcher most likely cannot be totally detached and objective in relation to the subjects under study, since s/he is so immersed. This is of course totally against the positivistic ideas as pointed out by for example Susman and Evered (1978). Nevertheless, it is also a scientific advantage since it gives the researcher a closer and deeper view of what is studied. Being aware of these problems and we have tried to stay as neutral as possible in the process of asking questions and analysing and making conclusions from respondents’ answers.

2.2 Research method

While the high-level research strategy and context were that of *action research*, the more specific research method follows the ideas of *grounded theory* (Glaser & Strauss 1967, Strauss & Corbin 1994).

Two sets of questionnaires were developed and sent to the respondents. They were composed of open-ended questions, so as to not restrain the thinking of the respondents. Each form contained six questions, and they were slightly different for certification auditors and information security consultants. This paper only report the findings of one question, which was posed in exactly the same wording to both groups:

> *In your opinion, which are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)*

The questionnaires were written in Swedish, so this is a translation. Although the question does not explicitly refer to the standard as such and to the problems associated with the certification process, the respondents rightly read this into the question because of the context within which it was asked. That context is; that they were asked about their experiences and insights as members of the Swedish *7799* pilot *certification* group.

In total, there are 8 certification auditors and 18 information security consultants in the Swedish 7799 pilot certification group. All of these were asked to complete the questionnaire. The response rate for the certification auditors were 75% (`(6/8)*100`), and for the consultants 56% (`(10/18)*100`). We have not formally analysed why some decided not to answer the survey. However, we do know that most of the ones who have not answered are new members of the group. Being new, they are likely to have limited experience and insights about the exact question. This fact might explain why they did not answer.

The answers were ranging from single sentences to quite extensive explanations. The exact answers were imported into ATLAS/ti – a methodology support tool for qualitative analysis of data especially supporting a grounded theory methodology. The answers from the auditors and the consultants were analysed separately, and therefore they will be presented separately in this paper. The idea with this was to see if there were any differences in insights and experiences (and views) between these two groups.

Each answer was coded with a code describing its content. And then patterns were looked for in the data. A more specific description of the analysis is provided under each section below.

3 Certification auditors’ perspective on implementation and certification of ISMS

Once again, the question was stated as follows (translation from Swedish to English):

> In your opinion, which are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)

From the answers, we could distinguish six different success factors. Since the consensus was so profound, we chose to present the answers sorted after each factor- starting with the most important, or at least the most frequently mentioned factor. All the answers fell within these six categories.

The critical success factors for implementation and certification, from the perspective of the certification auditors were the following:

1) Management commitment
Support from the top management of the organization, and their commitment to and understanding of the problems of information security was seen as one of the most important success factors for an efficient implementation of ISMS. This factor was mentioned firstly by all of the respondents in this group (auditors), even though there were no fixed answer alternatives and despite the fact that the respondents were unaware of each other’s answers. The following quotations speak for themselves:

> ”Top management’s interest and commitment in its own ISMS project. …”
>
> “Top management’s commitment and an understanding that the management system for information security must cover the whole business.”
>
> “Top management’s commitment…”
>
> “Top management’s understanding and commitment, in deciding the security policy / security level and to participate actively in the risk analysis and the continuity planning.”
>
> “Top management’s commitment. …”
>
> ”Endorsement from the company’s / organization’s top management. …”

2) Well-structured project
Another important success factor which was identified was that the ISMS implementation project in the organization is well-planned and –structured. The respondents expressed it like this:

> “An organizational unit responsible for the totality and for the risk analysis which is the foundation for all activities. …”
>
> “… a well defined project with delimited sub-projects. …”

> “A well developed project plan and a correctly dimensioned project organization. …”

Taken together, there are many aspects concerning the organization of the ISMS development and implementation that are mentioned:

- that the responsibility for the project is defined,
- that it is clear who shall carry out the different steps in the project
- that goals, resources and the time plan for the project are developed and documented in a project description, and
- that the resources in the project are well balanced.

3) Holistic approach

The project members – and other employees – ability to see the “full picture” is stressed by many of the respondents as an important success factor. Sometimes, it seems like the certification auditors have a feeling that the IT-technical aspects are handled in a very detailed way, but at the price to the detriment of obtaining a holistic view. Therefore, they meant that a more holistic approach and thinking in the projects should lead to positive consequences and pave the way to a more successful implementation and possibly certification of ISMS. Two of the respondents put it this way:

> “…that the participants in the work with identifying the risks are representing the whole business, that is not only security but also other parts of the business.”
>
> “Understanding that the management system for information security must cover the whole enterprise.”

As can be seen from the quotations, it is mainly the connection between the information security and the organizations core activities (processes) that is seen as important – that the ISMS does take into account and that it covers the whole organization – so that the ISMS does not end at the security- or IT department.

4) Appreciating the need for information security

That the organizations understand the need for information security is another success factor that was identified:

> “…that the company becomes aware of a need to protect its own, its customers and other stakeholders information.”
>
> “…understanding that the management system for information security must cover the whole organization”
>
> “management’s understanding…”

Although this factor may seem trivial, it is mentioned many times by the respondents. They sometimes perceive a lack of appreciation of the importance of information security from parts of the organization.

5) Motivated employees

Some of the answers focused on the need to motivate employees:

```
”To motivate the employees to develop processes and procedures
within their own areas of responsibility. ...”

”...motivated project management /-participants. ...”
```

The answers focus on the motivation of individuals participating in the ISMS project, such as project participants, project managers, and those responsible for different areas in the organization. After the development of the ISMS, it will also have to be implemented, and at that stage the importance of this success factor grow – at that time, *all* employees in the whole organization will have to be motivated to adhere to the rules. Further, they should regularly use the technical solutions that the projects have developed and the management decided on – they need motivation.

6) Access to external competence

The final success factor identified by the questionnaires was the importance of being able to call for external competence when needed:

```
”...good reference persons (preferably certification
authorities from the beginning).”

” ... access to external specialist competence.”
```

This factor is concerned with both experts and advisors in IT- and information security, but also about opening the dialog between the organization and the certification authority at an early stage. This contact – organization vs. certification authority – must be seen as very important – at least if the organization is planning to seek certification of its ISMS after the implementation.

Summary

The certification auditors in the Swedish pilot certification group viewed these six factors as critical for the successful implementation and certification of ISMS:

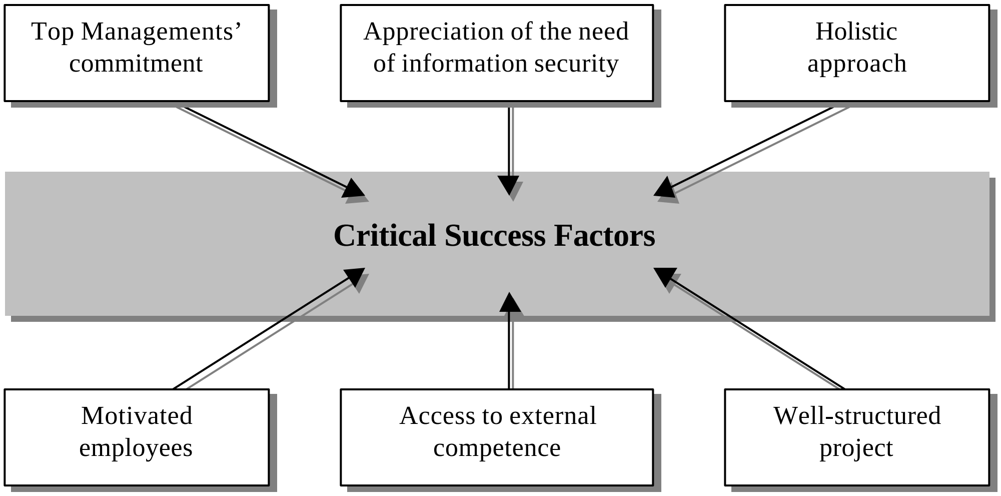

Top Managements' commitment
Appreciation of the need of information security
Holistic approach
Critical Success Factors
Motivated employees
Access to external competence
Well-structured project

Figure: Critical Success Factors for the implementation and certification of information security management systems, from the certification auditors' perspective.

4 Information security consultants' perspective on implementation and certification of ISMS

Also for this group, the question was stated as follows (translation from Swedish to English):

> In your opinion, which are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)

Also here, the answers were analyzed using a grounded theory method supported by a computerized data analysis tool (ATLAS/ti).

In total, there were 37 quotations from the consultants on this question. They were first analyzed and coded into 23 different categories, using no predetermined codes. This means that the essence of each quote can be represented by its code on this level. Afterwards, these 23 categories were further analyzed using the qualitative data analysis tool and we found that they fell into 6 more abstract categories.

Even though all the answers were in Swedish, we decided to code each quotation in English, so that it would be easier to present in this paper. However, the answers were not translated, but they are available in the Swedish report for those interested (draft, forthcoming).

It should be noted that there is no logic in the data analysis tool to help deciding on the categories of the data. The tool is only used to organize the analysis, and to keep track of and visualize the analysis result.

Here are all the codes used at the *first* level of analysis:

- ability to put policy into practice
- accurate analysis of preceding security situation
- active employee participation
- active project members
- appropriate project organization
- backing from top management
- balanced policy grounded in reality
- clear aim from top management
- customer organization participation
- documented business processes
- feasible implementation method
- identifiable business benefits
- implementation know-how for project leader
- insight and knowledge about security
- integration with existing management systems
- monetary resources
- project ability to influence IT development
- realistic cost estimation
- realistic time plans
- regular communication with stakeholders
- top management awareness

- top management involvement
- understanding the need for security

These codes were further analyzed and categorized into six more abstract categories. These six categories were:

- Project management capability
- Commanding capability
- Financial capability
- Analytic capability
- Communicative capability
- Executive capability

These capabilities form the foundation for a theoretical framework. Here is a short description of each of these capabilities.

Project management capability. A successful implementation project will need to have efficient project management capability. This means that for example active project members, an appropriate project organization and realistic time plans are needed.

Commanding capability. The commanding capability stems from the top management sponsorship of the project. It is this capability that gives the project the authority to decide on issues regarding information security. Without any real decision-making power, it is very hard, if not impossible to do reach the project goals. This capability is given by for example top management awareness and involvement in information security, identifiable business benefits and an understanding for the need of security, and a clear aim and backing from top management.

Financial capability. All information security projects need budgeted resources. A project with this capability is able to estimate costs realistically. It also has access to the resources needed to carry out the project.

Analytic capability. Projects with analytic capability can accurately analyse the preceding security situation, and therefore develop a well balanced ISMS which is also integrated with existing management systems (e.g. quality and environment management systems – iso900X and iso1400X). In short, this capability is needed to create a balanced policy grounded in reality.

Communicative capability. Many information security efforts stop at the security managers' desk. To avoid this, a communicative capability is needed. This capability is needed to enable regular communication with stakeholders and for active employee participation in the project.

Executive capability. Thinking about security and writing policies is one thing – implementing the ideas, rules, controls, and procedures is another. The executive capability means that the project can do things – that it can make things happen. One of the things that will need to be done is to put the policy into practice and this in turn often requires for example the ability to influence people in the IT department, in IT development and in other parts of the organization. A feasible implementation method and implementation know-how for the project leader are examples of parts that form this capability.

Summary
The information security consultants of the Swedish pilot certification group viewed these six capabilities as critical for the successful implementation and certification of ISMS:

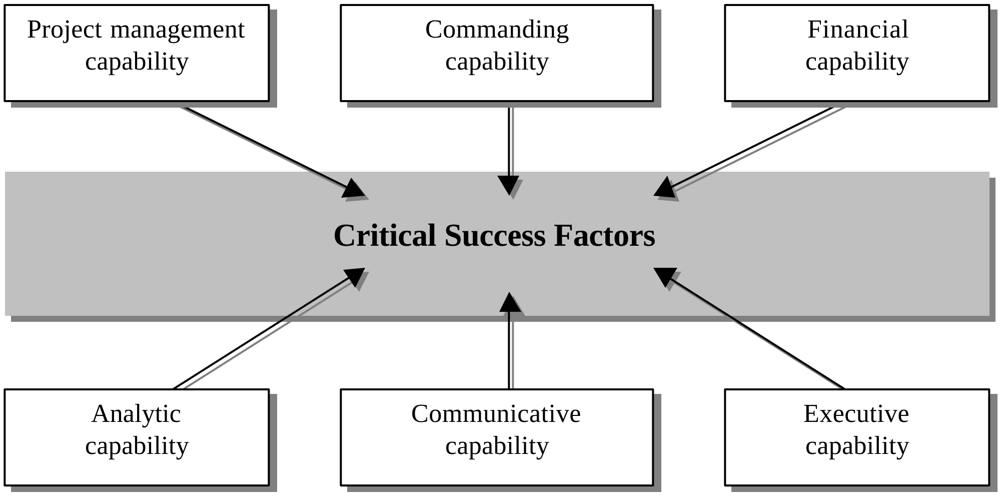


Figure: Critical Success Factors for the implementation and certification of information security management systems, from the information security consultants' perspective.

To demonstrate visually how this theoretical framework was developed, and how it is related with the data from the questionnaires, please refer to the network diagram in appendix 1.

5 Conclusions

Using an action research strategy and a grounded theory research method, this study has identified critical success factors for the implementation and certification of information security management systems. Even though we cannot statistically generalize these findings to a broader population, we believe that these results can be useful and valid. Especially for researchers and practitioners working with 7799 and similar management standards.

6 References

BSI (1999): *BS 7799-1:1999, Information security management. Code of practice for information security management* (This standard is now withdrawn and superseded by “*BS ISO/IEC 17799:2000, BS 7799-1:2000, Information technology. Code of practice for information security management*”), 1999, British Standards Institution: London.

Denscombe M (1998): *The Good Research Guide.* Open University Press: Buckingham.

Eloff M and S. Von Solms (1998): *Measuring the information security level in an organisation*, in Proceedings of the sixth working conference of IFIP WG 11.1 and 11.2, Budapest, 1998.

Eloff, M. and S. Von Solms (2000a): *Information Security: Process Evaluation and Product Evaluation*. In Qing, S., and J. Eloff, 2000: Information Security for Global Information Infrastructures (Proceedings of the IFIP TC11 16th annual working conference on information security during the World Computer Congress, Beijing, August 21-25 2000). Amsterdam: Kluwer Academic Publishers

Eloff, M. and S. Von Solms (2000b): *Information Security Management: An Approach to Combine Process Certification And Product Evaluation*. Journal of Computers and Security, Vol. 19, Issue 8, *Pages 698-709* Elsevier Science Ltd.

Glaser, B. and A. Strauss (1967): *The Discovery of Grounded Theory.* Chicago: Aldine.

ISO (2000): *ISO/IEC 17799:2000, Information technology -- Code of practice for information security management*, 2000, International Organization for Standardization (ISO), Geneva, Switzerland.

Labuschagne (draft, forthcoming): *Web Assurance: Information security management for e-commerce.* Draft available at http://csweb.rau.ac.za/deth/research/index.htm, Accessed 2001-03-28.

Siponen (2001): *On the scientific background of information security management standards: a critique and an agenda for further development*. The Second Annual Systems Security Engineering Conference (SSE), 28 February - 2 March, Orlando, Florida, USA.

SIS (1999): *SS 62 77 99: Ledningssystem för informationssäkerhet - Del 1: Riktlinjer för ledning av informationssäkerhet*, 1999, Swedish Standards Institute (SIS), Stockholm, Sweden. (Swedish translation of BSI, 1999)

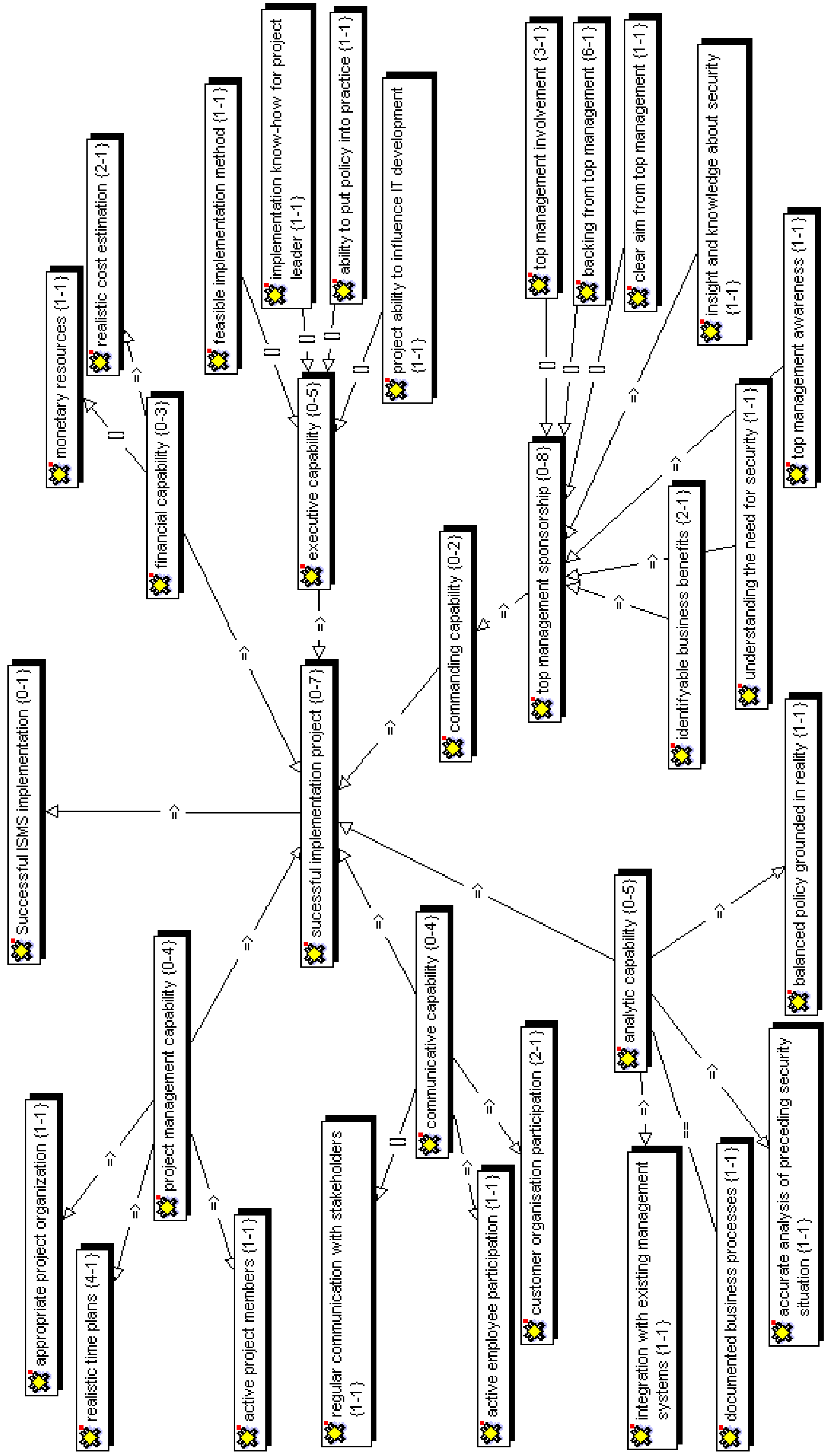
R von Solms (1999): *Information security management: why standards are important*. Information Management and Computer Security, Vol 7 Issue 1 Date 1999.

S von Solms (2000): *Information Security - The Third Wave?,* Computers & Security, Volume 19, Issue 7, 1 November 2000, Pages 615-620

Strauss, A. and J. Corbin (1994): *Grounded theory methodology – An Overview*. In Denzin and Lincoln, Handbook of Qualitative Research, Sage, Pages 273-285).

Susman G., and R. Evered (1978): *An assessment of the scientific merits of action research.* Administrative Science Quarterly, 23(4): 582-603.

Appendix 1: Information security consultants' view


Successful ISMS implementation {0-1}
sucessful implementation project {0-7}
financial capability {0-3}
monetary resources {1-1}
realistic cost estimation {2-1}
executive capability {0-5}
feasible implementation method {1-1}
implementation know-how for project leader {1-1}
ability to put policy into practice {1-1}
project ability to influence IT development {1-1}
commanding capability {0-2}
top management sponsorship {0-8}
top management involvement {3-1}
backing from top management {6-1}
clear aim from top management {1-1}
insight and knowledge about security {1-1}
top management awareness {1-1}
understanding the need for security {1-1}
identifyable business benefits {2-1}
analytic capability {0-5}
balanced policy grounded in reality {1-1}
accurate analysis of preceding security situation {1-1}
documented business processes {1-1}
integration with existing management systems {1-1}
communicative capability {0-4}
customer organisation participation {2-1}
active employee participation {1-1}
regular communication with stakeholders {1-1}
project management capability {0-4}
active project members {1-1}
realistic time plans {4-1}
appropriate project organization {1-1}