Paper #116

USING ENTERPRISE ARCHITECTURE FOR CIO DECISION-MAKING: ON THE IMPORTANCE OF THEORY

Pontus Johnson, Mathias Ekstedt, Enrique Silva, Leonel Plazaola

Dept. of Industrial Information and Control Systems
KTH, Royal Institute of Technology
SE-100 44 Stockholm, Sweden
{pontusj, mathiase, enriques, leonelp}@ics.kth.se

ABSTRACT

A company's Chief Information Officer (CIO) is responsible for the management and evolution of the enterprise information system. An approach suggested as an aid for the CIO's decision-making process is Enterprise Architecture, based on architectural models of both the enterprise information system and its context.

For architectural models to function as decision-making support, this paper argues that they must be amenable to architectural analysis. The purpose of this paper is to demonstrate the importance of *architectural theory* in the analysis of architectural models of the enterprise information system. *Architectural theory diagrams* are proposed as means for presenting and comparing architectural theories as well as for assessing the analytical value of architectural models.

INTRODUCTION

Enterprise Architecture is a model-based management and planning approach for the evolution of organization-wide information systems; it is an approach that has been proposed mainly as a response to the ever-increasing significance and complexity of business-supporting information systems (DoD 2003) (TOG 2003) (Zachman 1987) (Spewak 1993). Since the problem of enterprise information system management and planning is also the main task of a company's Chief Information Officer (CIO) function, this paper is based on the notion that Enterprise Architectures should be consciously designed to aid the CIO decision-making process (Ekstedt et al. 2004a).

Most Enterprise Architecture frameworks propose a set of models to be developed (in this paper, no distinction will be made between the architectural concepts *model* and *view*), describing not only the information systems per se, but also the context in which they are located, including the business organization and the technical milieu (such as available technical standards). Although the importance of good modeling is high-lighted by the Enterprise Architecture discipline, the plethora of proposed models that are available to the CIO is overwhelming, and it is rarely evident when and why a particular model is to be preferred over others. The main reason for this confusion is that there normally is an unclear link between the contents and structure of a model on the one hand, and its purpose on the other.

A general purpose of models is to answer questions about the nature of the modeled entity. Therefore, it would, in the field of Enterprise Architecture, be desirable to be able to explain precisely what questions a

given architectural model is capable of answering. Today, this is rarely the case. To put it differently, this paper claims that in the Enterprise Architecture discipline, we often do not have a clear understanding of why we use the models we use (this statement is further argued for in the remaining parts of the paper).

One risk-minimizing approach to mitigating the problem of generating inadequate models is to generate many and large models. This is however an expensive undertaking, mainly in terms of the cost of searching for the information to be incorporated in and represented by the models (Ekstedt et al. 2004a).

The present paper proposes an approach, based on the concept of *architectural theory diagrams*. It takes its starting point in the purpose of architectural models, i.e. the CIO decision-making, thus tackling the above problems.

Outline. The next section delineates a general decision-making process for the CIO based on architectural analysis, thus introducing important concepts such as architectural model and theory. Architectural theory diagrams are introduced as a means for making architectural theory explicit. Two architectural theories of IT Security are presented and subsequently applied in analyses of example scenarios. The paper proceeds with defining quality criteria for architectural theories. The topic of theory evaluation and comparison is then elaborated on with respect to these criteria. Finally, architectural model generation is discussed and an architectural meta-model derived from one of the example theories is presented.

ANALYSIS OF ENTERPRISE ARCHITECTURES

In order to clarify the concept of architectural analysis, we briefly consider the process that the CIO needs to go through when making decisions concerning the future of the enterprise information system.

Formulate scenarios. Firstly, the CIO needs to consider what options are available with respect to the future structure of the enterprise information system. An intuitive way to do this is by conjuring up scenarios representing possible future states of the system. Typically, these *scenario models* are modifications of the *baseline* (or *as-is*) *model* of the enterprise architecture.

As an introduction to the example that will be used throughout this paper, we ask the reader to consider the two scenarios A and B in Figure 1.

Decide upon evaluation criteria. Evaluation criteria are needed to determine which of the scenarios is preferable. A requirement on good evaluation criteria is that they need to provide answers to questions that are pertinent to the CIO; the more important questions they answer, the better they are, ceteris paribus. Examples of relevant questions for the CIO include properties such as the level of IT security, availability, performance, and business support.

Hereafter, we will refer to evaluation criteria as *architectural theory* or simply *theory*. In order to prevent confusion, we note that theory is used here in a broad sense. The evaluation criteria may range form simple rules of thumb to more strict and precise presumptions. On the level of abstraction of enterprise architecting, however, indicative theories stating relations with ballpark figures, are prevailing.

Analyze scenarios. Analysis is the application of architectural theory (evaluation criteria) on scenarios for evaluation purposes.

To continue with the example, the reader may ponder whether he or she finds that scenario A or B in Figure 1 is to be preferred with respect to the property *IT security* (IT security analysis will be considered in the example used throughout this paper) and what architectural theory would justify this

preference. In other words, which scenario seems to feature the highest security level and what analysis procedure would lead to this result?

Select Scenario. Between the formulated scenarios, the CIO will, based on the architectural analysis, eventually choose one to be realized.

Summarizing, the decision making of the CIO can be viewed as a problem of scenario selection (given a *baseline model* depicting current state of affairs). Scenario selection is in turn based on architectural analysis. We note that the CIO faces a situation of comparative analysis in the decision-making process; variations of future states of the enterprise architecture are produced and compared. We call architectural models of prospective systems *scenario models*. To undertake architectural analysis, we need architectural theory. Some of the theory may be viewed as factual, state-of-the-world necessities while others are a matter of opinion or desires about what should be prioritized. The latter category we refer to as *requirements*. Finally, the ultimately chosen scenario is referred to as the *target model*.

ARCHITECTURE THEORY DIAGRAM

A central argument of this paper is that good architectural theory is required to generate good architectural models. In this section, we introduce a diagram for presentation of architectural theory. This *architecture theory diagram* illustrates important aspects of the evaluation criteria (theory) we wish to employ when analyzing an architectural model. There are three main raisons d'être for this diagram. Firstly, it can be used to compare competing theories to each other. By these comparisons, we will be in a position to choose the theory that best suits our purposes. Secondly, it will detail what information a good architectural model needs to contain. Thirdly, it makes the theory explicit, facilitating both critical examination and reuse of the theory.

In Figure 2 and Figure 3, two competing theories of the property *IT security* are presented as theory diagrams. Figure 2 is based on the article "A Practical Approach to Enterprise IT Security" by Liu et al., published in the IEEE magazine IT Professional (Liu et al. 2001), and Figure 3 is based on SEI/CERT's security assessment and planning approach OCTAVE (OCTAVE 2001). The theory diagrams present how the abstract property IT security can be assessed by means of more concrete properties such as the existence of intrusion detection systems and antivirus functionality.

The white boxes in the theory diagrams represent properties of the architecture, such as *IT security*, *authentication quality,* and *encryption quality*. The grey boxes represent measures, i.e. properties that are immediately measurable in the real world. Again, note that on the high level of abstraction of enterprise architecting, measures are normally of an indicative nature. Properties may be defined in terms of other properties; this is indicated by compositional relations. Properties may be related by causal relations, so that a change in one property *results* in a change in another property. Properties may also be related by correlation relations, indicating that changes in the associated properties normally *coincide*. The strength of relations is indicated by a nominal scale {low, medium, high}. This scale is deemed sufficiently precise for the present context, but may be replaced if needed. A better understanding of the architecture theory diagrams may be provided by the example analysis in the next section.

EXAMPLE ANALYSIS OF IT SECURITY

In this section, we briefly consider the performance of the two IT security theories on the scenarios in Figure 1. A simple analysis

procedure for applying one of the presented IT security theories on a scenario is as follows:

1. For each measure in the theory, retrieve the measure value from the scenario model. Parenthetically, this procedure highlights the tight link between theory and model.
2. Derive the value of hierarchically superior properties as a weighted average of the underlying properties' values, where the weights are given by the relation strengths. Repeat this step until the hierarchical top of the theory diagram is reached (i.e., the property "IT Security Level").

Table 1 presents the results of the application of the two competing IT security theories on the two example scenarios using the above analysis procedure. The analysis results have been converted into a nominal scale for presentation purposes.

Table 1: Results of example IT security analysis.

	LIU ET AL.	OCTAVE
SCENARIO A	Medium	Low
SCENARIO B	Low	Medium

We note that the two theories have differing opinions on which scenario features the highest IT security level. This is due to the fact that they emphasize different security properties. Firewalls are, for instance, of greater relative importance to Liu et al. than to OCTAVE. Other properties are only included in one of the theories, as in the case with backup functionality, which is only valued in OCTAVE. Since theories may generate differing results, it becomes important to make an informed selection between competing theories. The theory selection problem is further discussed below.

It is here appropriate to issue some caveats. The above presented analysis procedure, based on weighted averages, may for other theories – where the relations between properties are less straight-forward – be substituted by more complex calculations. Also, it is important to emphasize that the presented analysis is excessively formalized and not per se recommended as a general approach to architectural analysis on the enterprise level. In most cases, this kind of automated analysis results can serve only as a base for discussion, since enterprise information system management has yet to attain the status of a quantitative discipline.

Returning to the main points of this example, different architectural theories will result in different CIO decisions. By exposing and considering the architectural theories employed by the CIO, we may improve the rationality of the decision-making process. As a vehicle for this improvement, the Enterprise Architecture discipline may provide valuable guidance to the CIO by suggesting architectural models that are consistent with good architectural theories.

QUALITIES OF ARCHITECTURAL THEORIES

The previous section showed that architectural theories may contradict each other. It thus becomes important to consider the quality of architectural theories in order to select the most appropriate one for the purposes at hand.

Detailing the characteristics of good architectural theories, we find three qualities of particular interest in this context:

- **Relevance.** A good theory should answer the CIO function's most important questions. Consequently, a good theory cannot be chosen before the CIO knows its main concerns.
- **Credibility.** A good theory should generate credible results, i.e., the answers delivered by the theory must be true also in the real world.
- **Information search cost.** The measures (the grey boxes in the theory diagrams) should not be excessively expensive to collect. This cost is mainly derivable to the cost of searching for the information

required by the theory, information which can be scattered far and wide.

These three qualities are however often at odds with each other, so relevance and credibility frequently need to be traded off against information search cost.

THEORY COMPARISON

In this section, comparison of architectural theories will be considered. The comparison is divided into two points of view, the CIO's and the scientist's. These two stakeholders are both important for the overall quality of a theory but they are driven by different motives – namely pragmatism and correctness respectively – and their knowledge of the specific property under examination is assumed to differ. Recall that the theory diagram is suitable for this kind of comparison because it helps answering questions relating to the represented theory's relevance, credibility and information search cost.

The CIO point of view. The CIO is a practically oriented function responsible for a great number of concerns. It is therefore not reasonable to require that the CIO have well-founded opinions on specific details of all relevant theories. The general approach for the CIO should instead be to assess theories according to the three following criteria: a) credibility of theory-issuing party, b) information search cost, and c) general soundness.

The first criterion considers the credibility of the institution or person who is responsible for the theory. It may, for instance, be reasonable to put greater trust in a theory issued by a standardization organization than a vendor organization.

The second criterion is related to the resources required when searching for the information needed by the analysis. This criterion thus considers the practical ease with which the theory can be employed. There are several possible approaches to the estimation of this information search cost, it may e.g. be based on architectural models of the information structure of the enterprise (Ekstedt et al. 2004b).

The third criterion considers the general soundness of the theory, as estimated by the CIO. On the top-level, relevance of a theory is of course defined by the CIO function in the sense that the CIO determines whether the theory deals with important matters or not. However, since the CIO is not expected to possess in-depth knowledge of the theory at hand, the soundness assessment cannot be a detailed one. However, the approach the CIO would use is the same one as that used by the scientist considered below.

In summary, this paper suggests that the CIO function should focus on the questions presented in Table 2.

Table 2: Theory evaluation criteria for the CIO.

RELEVANCE
Does the theory address pertinent questions?
Cf. Theory evaluation criteria for the scientist.
CREDIBILITY
What is the credibility of the issuing party?
Cf. Theory evaluation criteria for the scientist.
INFORMATION SEARCH COST
Is the search cost for any measure too high?
Is the aggregate search cost for any property too high?

The scientist's point of view. The scientist is assumed to have well-informed opinions on the contents of the theory diagram and thus compares theories with respect to their details to a larger extent than the CIO.

With regard to relevance, we note that from a scientific point of view, the most desirable theory diagrams feature causal relations, followed by correlation relations and finally composition relations. This order of preference is based on the concept of falsifiability (Popper 1959). A compositional relation means that the theory postulates that a property is defined in terms of its constituent properties. It is not possible to falsify such a definition, only to have differing opinions on

the relevance of the resulting property. A correlation relation means that changes in one property coincide with changes in another property. This relation requires that both properties are independently measurable and it can be falsified by e.g. a statistical study. A causal relation means that a change in one property is the cause of a change in another property. For a causal relation, a statistical correlation is necessary, but also an underlying explanation. It thus requires an argument for *how* the one property affects the other. With regards to these three relations, the scientist may not only have opinions on the choice between the relations, but also on their weights.

Table 3: Theory evaluation criteria for the scientist.

RELEVANCE
Could any compositional relation be replaced by a correlation relation?
Is the weight of any relation too high or low?
CREDIBILITY
Could any correlation relation be replaced by a causal relation?
Is any causal or composition relation missing?
Is any measure or property missing?
INFORMATION SEARCH COST
Cf. Theory evaluation criteria for the CIO.

In addition to issues about the relations, the scientist may compare theory diagrams with respect to the actual properties. Does one theory contain important properties that another theory is missing?

Scientific methods should be used to answer the questions of interest to the scientist. It would thus be reasonable to expect that the scientific community would focus its efforts on answering the questions in Table 3.

AN IT SECURITY META-MODEL BASED ON LIU ET AL.

Given a good architectural theory, it is possible to generate good architectural models facilitating evaluation of enterprise information systems. Returning to the IT security example, so far the article has presented some theories and employed them as a base for analysis. In this section, an architectural meta-model is outlined based on the theory of Liu et al., describing the entities of an IT security model.

The model generation process is simple. Since the theory diagram describes what information is needed to make good decisions (at least good decisions according to Liu et al.), we simply need to make sure that this information (and preferably only this information) constitutes the contents of the model. Table 4 presents an outline of a meta-model consistent with the security theory of Liu et al.

Table 4: Outline of meta-model for IT security consistent with Liu et al.

ENTITY	ENTITY TYPE
Antivirus	Function
Audit	Function
Authentication	Function
Content Screening	Function
External Firewall	Function
Internal Firewall	Function
Intrusion Detection	Function
Misuse and Anomaly Detector	Function
Network Scanner	Function
System Scanner	Function
Access Control	Business Process
Computer Forensics	Business Process
Employee Security Education	Business Process
Incident Response	Business Process
Disaster Recovery Plan	Document
Security Policy	Document
Employee Security Policy and Incident Response Test Score	Actor attribute

There is, of course, a great benefit to deriving the architectural model from the theory, since this ensures that the model will be able to answer the desired questions. However, it is quite possible to do the reverse, i.e. to use theory diagrams to clarify what questions a model indeed can answer. Since there are already many generally accepted models available in literature, this exercise may be a useful one.

IT security is one example of a concern that needs theory. The CIO function must, however, in its undertaking acquire and employ a large number of different theories for different questions. An obvious risk is that an inconsistent set of models are developed. This pinpoints the need for harmonization of theories so that the same model could be used for answering different questions using different theories. A main motive for this is once again the search cost related to collecting theory measures and populating the models. This is further elaborated on in (Ekstedt et al. 2004a).

CONCLUSIONS

To further Enterprise Architecture as a solid support for CIO decision making, this paper argues that not only architectural models, but also architectural theory needs to be made explicit. Architectural models without explicit architectural theory are of limited value, since it is not possible to assess their potential as decision-making support. The paper presents *theory diagrams* as a convenient notation for presenting architectural theory. The arguments of the paper are illustrated with examples of IT security analysis.

REFERENCES

Alberts, J. A., et al., *OCTAVE^{SM} Catalog of Practices, Version 2.0*, CMU/SEI, October 2001.

DoD Architecture Framework Working Group, *DoD Architecture Framework Version 1.0*, Department of Defense, 2003.

Ekstedt, M., et al., "Consistent Enterprise Software System Architecture for the CIO: A Utility-Cost Based Approach." *Proceedings of HICSS-37,* 2004.

Ekstedt M. et al., "The Architectural Information View – A New Perspective for Enterprise Software System Management." *To be published, 2004.*

Eriksson, H-E. and M. Penker, *Modeling business with UML – Business Patterns at Work*, OMG Press, 2000.

Liu, S., et al., "A Practical Approach to Enterprise IT Security." *IEEE IT Professional*, September-October, 2001.

Popper, K., *The Logic of Scientific Discovery*, Hutchinson, 1959.

The Open Group, *The Open Group Architectural Framework Version 8*, The Open Group, 2002.

Spewak, S., *Enterprise Architecture Planning: Developing a Blueprint for Data, Applications, and Technology*, Wiley, 1993.

Zachman, J., "A Framework for Information Systems Architecture." *IBM Systems Journal,* Vol. 26, No 3, 1987.

BIOGRAPHY

The authors are researchers at the Department of Industrial Information and Control Systems at the Royal Institute of Technology in Stockholm, Sweden. Dr. Pontus Johnson is a senior researcher and Mathias Ekstedt, Enrique Silva, and Leonel Plazaola are all Ph. D. students.

Figure 1: Illustration of two simple example architectural scenarios, A and B. The meta-models are based on the Department of Defense Architectural Framework's (DoDAF 2003) product systems communication description (SV-2) and standard business process notations, e.g. as presented in (Eriksson and Penker 2000).

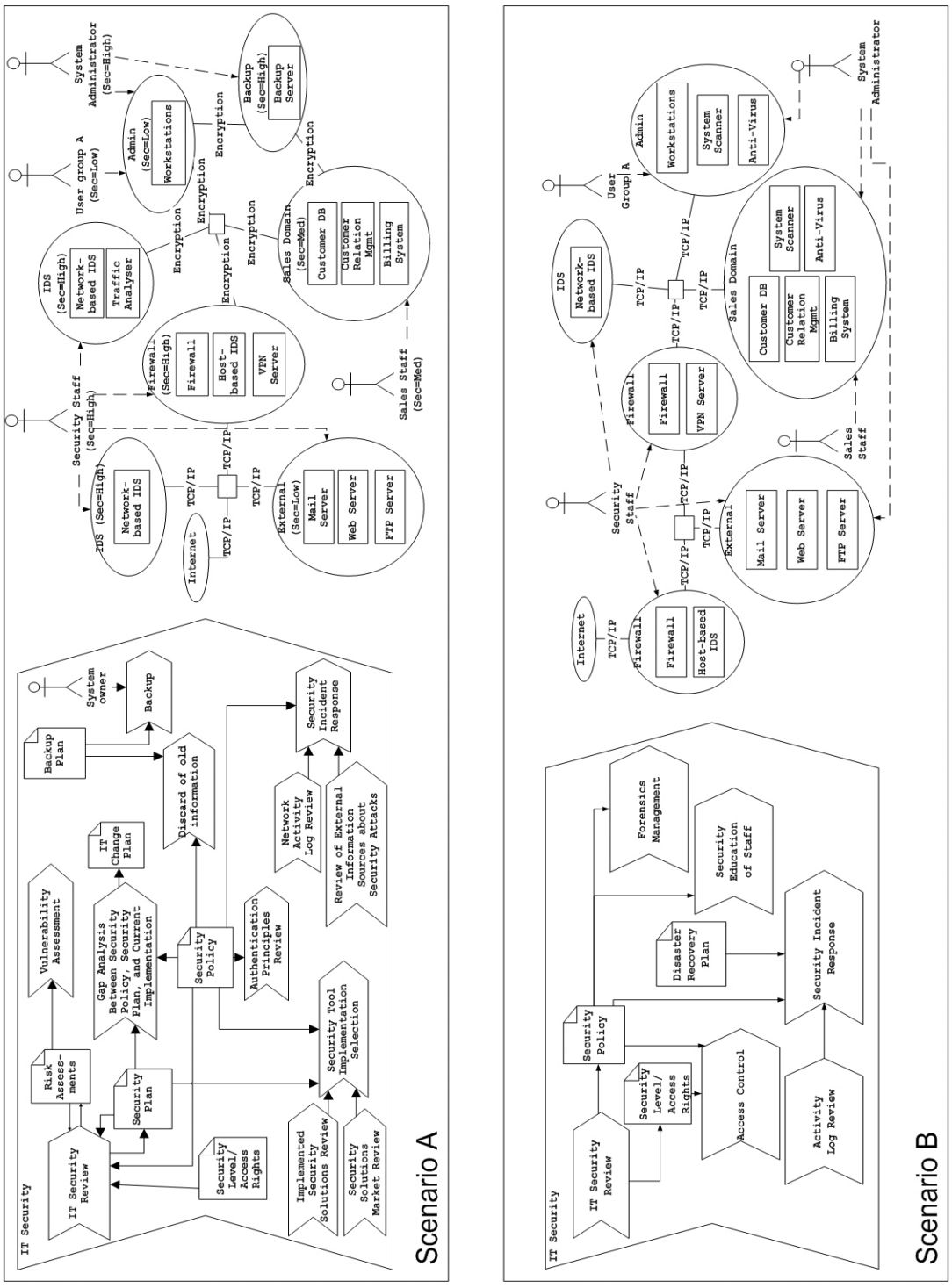

Figure 2: Theory diagram for IT security level, based on (Liu et al. 2003). All relations are assumed to be of "medium" weight since Liu et al. provide no other indications. Measures are intended to be as simple as possible.

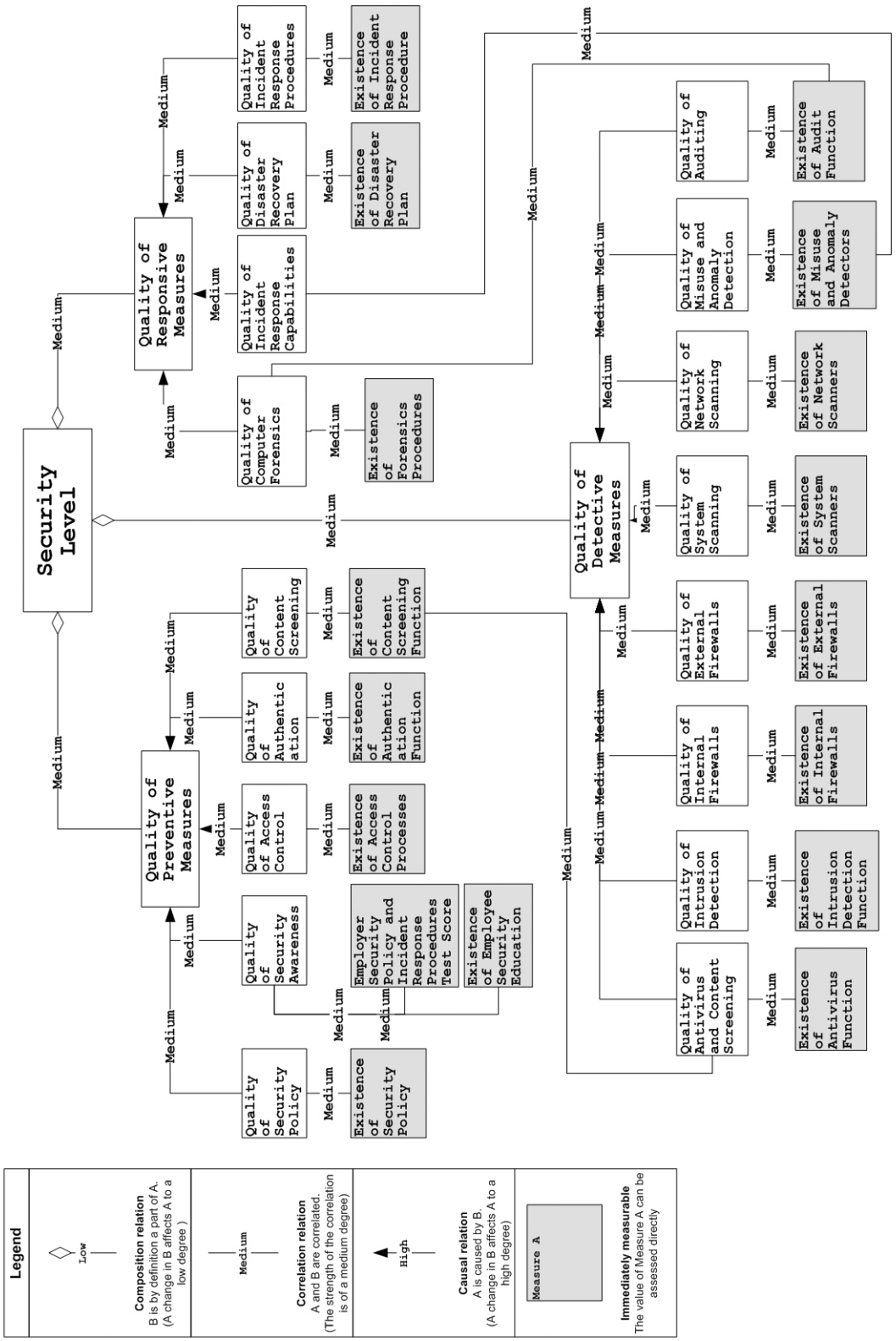

Figure 3: Theory diagram for IT security level, based on (OCTAVE 2003). All relations are assumed to be of "medium" weight since OCTAVE provides no other indications. Measures are intended to be as simple as possible. Measures are only shown for the property "Quality of system and network management" due to the limited space available in this paper. For legend, cf. Figure 2.